Technical Guide on Protecting Critical Energy Infrastructure against Terrorist Attacks

SEPTEMBER 2024

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

Global Programme on Countering Terrorist Threats against Vulnerable Targets

Implemented in partnership with:

UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE (CTED)

UNAOC
United Nations Alliance of Civilizations

unicri
United Nations
Interregional Crime and Justice
Research Institute

Technical Guide on Protecting Critical Energy Infrastructure against Terrorist Attacks

United Nations Global Programme on Countering Terrorist Threats against Vulnerable Targets

September 2024

Disclaimer

The opinions, findings, conclusions, and recommendations expressed herein do not necessarily reflect the views of the United Nations or any other national, regional, or international entities involved. This report is not intended to serve as a guidance document but instead take stock of current practices in place across the world. The practices described herein are to be perceived as relevant at the time of writing, are non-binding and do not override the purview of national authorities' guidance. This publication is intended to complement other relevant ongoing work by building upon available research and the experiences of countries. It also accounts for the work being undertaken by other international bodies.

The designations employed and material presented in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city, or area of its authorities, or concerning the delimitation of its frontiers or boundaries.

The contents of this publication may be quoted or reproduced, provided that the source of information is properly acknowledged. The United Nations Office of Counter-Terrorism (UNOCT) requests to receive a copy of any document in which this publication is used or quoted.

Acknowledgments

This Technical Guide has been made possible with the financial support from the Russian Federation and Turkmenistan, under the umbrella of the United Nations Global Programme on Countering Terrorist Threats against Vulnerable Targets[1].

Copyright

405 E 45th Street
New York, NY 10017

Email: OCT-info@un.org
Website: www.un.org/counterterrorism/

[1] United Nations Global Programme on Countering Terrorist Threats against Vulnerable Targets

Preface

Terrorists have increasingly been exploiting vulnerabilities in public and private utilities, including critical energy infrastructures (CEI). The interdependencies and interconnected nature of Critical Infrastructure (CI) located across borders raise additional concerns and require bilateral or regional responses.

While large-scale terrorist attacks against CI with significant cascading effects have not yet occurred, the threat posed by such a scenario remains persistent and requires countries to put in place adequate prevention, response and resilience measures.

This *Technical Guide on Protecting Critical Energy Infrastructure against Terrorist Attacks* was designed to provide public sector officials, practitioners, civil society, international and regional organizations, academia, the private sector and all relevant stakeholders with appropriate good practices, tools and case studies from across the world to support Member States' efforts to protect CEI.

The United Nations General Assembly and the Security Council have been paying close attention to this topic for several years. In the United Nations Global Counter-Terrorism Strategy (GCTS), under Pillar II on measures to combat and prevent terrorism, Member States resolved to "step up all efforts to improve the security and protection of particularly vulnerable targets, such as infrastructure and public places, as well as the response to terrorist attacks and other disasters, in particular in the area of civil protection, while recognizing that States may require assistance to this effect".

In addition to the more general calls to prevent this threat included in resolutions 1373 (2001) and 1566 (2004), the Security Council adopted resolution 2341 (2017), which was the first global instrument fully devoted to the importance of safeguarding CI from terrorist attacks. More specifically, in this resolution, the Council recalled that all Member States should establish terrorist acts as serious criminal offences in domestic laws and regulations and called upon them to ensure that they had established criminal responsibility for terrorist attacks intended to destroy or disable CI, as well as the planning of, training for, financing of and logistical support for such attacks.

In resolution 2396 (2017), the Security Council acknowledged that the Islamic State in Iraq and the Levant (ISIL), also known as Da'esh, had called on its supporters and affiliates, especially foreign terrorist fighters leaving armed conflict zones, to plan and carry out attacks on public places and utilities. In that resolution, the Council stressed the need for Member States to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, to share information and experience in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks against "soft" targets.

In 2018, the Counter-Terrorism Committee (CTC) adopted an addendum to the 2015 Madrid Guiding Principles, which highlights the importance of the protection of vulnerable targets, as called for in principles 50 and 51. In addition, Security Council resolution 2617 (2021) also includes specific provisions on the protection of CI and so-called "soft" targets as part of the new mandate of the Counter-Terrorism Committee Executive Directorate (CTED) and recognized the crucial importance of cooperation with the United Nations Office of Counter-Terrorism (UNOCT) in this area.

In June 2023, during the eighth review of GCTS, Member States agreed by consensus that the protection of vulnerable targets should be a priority in our common action against terrorism. General Assembly resolution 77/298 included two preambular and four operational paragraphs on this topic, condemning terrorist attacks against critical energy facilities and stressing the need to bring together all relevant stakeholders—Member States, international and regional organizations, the private sector, civil society and academia—to address effectively the unprecedented threat posed by terrorist attacks to CI and soft targets.

Over the past four years, Member States have been active in adapting their legal, institutional and operational frameworks to the protection of CEI. This Technical Guide will demonstrate to readers the speed at which the CEI protection landscape has been changing.

The United Nations Global Programme on Countering Terrorist Threats against Vulnerable Targets, jointly implemented by the United Nations Office of Counter-Terrorism (UNOCT), the Counter-Terrorism Committee Executive Directorate (CTED), the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Alliance of Civilizations (UNAOC), in collaboration with the International Criminal Police Organization (INTERPOL), has been supporting Member States since 2021 in building their capacities, developing connections between experts and identifying good practices for the protection of CI. This Technical Guide on Protecting Critical Energy Infrastructure Against Terrorist Attacks will be added to the repertoire of knowledge tools developed by the Programme over the past three years, including the five technical guides on the protection of public spaces/"soft" targets and the Compendium of Good Practices on the Protection of Critical Infrastructure.

I am certain that this Technical Guide, made possible thanks to the generous funding of the Russian Federation and Turkmenistan to the Global Programme, will become a seminal tool in this area, to the benefit of all Member States.

Vladimir Voronkov
Under-Secretary-General
United Nations Office of Counter-Terrorism

Contents

Boxes

Case Studies

Tools

Tables

Abbreviations

ADMM	Association of Southeast Asian Nations Defence Minister's Meeting
AI	Artificial Intelligence
ASEAN	Association of Southeast Asian Nations
BCK	Bayesian network – Consequence – Knowledge
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosives
CEI	Critical Energy Infrastructure
CEII	Critical Energy Infrastructure Information
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIP	Critical Infrastructure Protection
CIS	The Commonwealth of Independent States
CIS ATC	The Commonwealth of Independent States Anti-Terrorism Center
CSTO	Collective Security Treaty Organization
CTED	United Nations Counter-Terrorism Committee Executive Directorate
DDos	Distributed Denial of Service
DoS	Denial of Service
GCTS	United Nations Global Counter-Terrorism Strategy
ICT	Information and Communications Technology
IED	Improvised Explosive Device
INTERPOL	International Criminal Police Organization
ISIL (Da'esh)	Islamic State in Iraq and the Levant
LNG	Liquefied Natural Gas
OSCE	Organization for Security and Cooperation in Europe
PPPs	Public-Private Partnerships
PSIM	Physical Security Information Management
ROUV	Remotely Operated Underground Vehicle
SALW	Small Arms and Light Weapons
SCADA	Supervisory Control and Data Acquisition
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
UNCCT	United Nations Counter-Terrorism Centre of UNOCT
UNDRR	United Nations Office on Disaster Risk Reduction
UNIDIR	United Nations Institute for Disarmament Research
UNOCT	United Nations Office of Counter-Terrorism

1. Executive summary

Energy facilities are attractive targets for terrorist attacks due to several factors: considerable financial outlay and cascading effect, psychological influence, publicity and symbolism. The potential high impact of successful attacks can cause extensive economic, social and environmental damage. These attacks can disrupt the global economy, destabilize governments, and result in mass casualties. The psychological effect of such attacks can intimidate populations and undermine public confidence in the ability of states to ensure security. Furthermore, attacks on energy infrastructure attract significant media attention, amplifying the terrorist groups' visibility and perceived power. The feasibility of attacks on certain facilities, due to specific vulnerabilities, further entices terrorist organizations. Additionally, terrorists may exploit these attacks as a means of financing their operations, through ransom, theft, or extortion.

Modern terrorist attacks on CEI have evolved significantly, transitioning from symbolic acts to highly planned, coordinated operations that often combine physical attacks with the use of information and communication technology (ICT) for malicious purposes. The trend towards sophisticated attacks involves terrorists leveraging advanced technologies to maximize impact. Furthermore, coordinated attacks on multiple targets can create complex challenges for security and emergency response systems.

The vulnerabilities of CEI are multifaceted and stem from several inherent characteristics. CEI facilities, such as pipelines and oil refineries, are resource-intensive and geographically dispersed, making comprehensive security measures challenging and costly. The increasing digitalization of the energy sector introduces new information security risks, as the reliance on smart devices and Supervisory Control and Data Acquisition (SCADA) systems creates potential entry points for attacks using ICTs. The interdependencies between CEI and other critical sectors, such as transportation, communication and water supply, exacerbate the impact of attacks, potentially leading to cascading failures across multiple infrastructures.

The rapid evolution of Unmanned Aircraft Systems (UAS) and associated technologies have multiplied the potential threats to CEI. UAS offer terrorist groups distinct advantages, such as remote operation and the ability to bypass traditional security measures. UAS can be used for direct attacks, such as bombing facilities, or for reconnaissance, gathering critical information on the layout and vulnerabilities of the targeted infrastructure. The proliferation of UAS, combined with their decreasing cost and increasing capabilities, makes them an attractive and accessible tool for terrorists. The potential for UAS "swarm" attacks, where multiple UAS are used simultaneously to overwhelm defenses, further complicates the security landscape.

This Technical Guide includes detailed case studies, tools and good practices from numerous countries and international and regional organizations from around the world. These examples emphasize the importance of tailored national strategies, international cooperation, robust legal frameworks, effective inter-agency coordination and the role of public-private partnerships (PPPs) in enhancing security measures against terrorist-related attacks.

Effective protection of CEI requires a comprehensive risk management approach that includes regular vulnerability assessments, among these the continuous monitoring of terrorist threat scenarios. As a result, security measures in place will need to adapt to evolving challenges. Various methodologies and approaches

presented in this Guide facilitate the estimation of risks and the development of mitigation strategies. Identifying and securing critical elements within CEI facilities is essential for reducing vulnerabilities and enhancing resilience.

The Technical Guide delves into several key areas to provide a comprehensive understanding of the challenges that need to be taken into account and strategies that could be adopted to effectively safeguard these vital assets. The introduction sets the context, scope, objectives and methodology of the Guide, establishing a foundational understanding of the significance of protecting CEI and the approach taken to address this issue. The second part, "Understanding the Challenge," explores the motivations behind terrorist targeting of CEI, the general patterns and characteristics of such attacks and the evolving modus operandi of terrorist groups. It highlights the specific vulnerabilities of CEI, including the interdependencies with other critical sectors and the implications of cross-border interconnections, as well as the changing security landscape driven by emerging technologies and information security threats.

The third part, “National Approaches to Reducing Terrorist-Related Risks to Critical Energy Infrastructure”, examines legal frameworks, institutional mechanisms and operational readiness. The Guide emphasizes the importance of integrating CEI protection into national security priorities, establishing standards and protocols and considering human rights aspects. The fourth part, “International Efforts to Protect Critical Energy Infrastructure," highlights the importance of cross-border cooperation, international organizations and inter-agency coordination. It stresses the need for joint exercises, training and networking for effective information-sharing. The fifth part, "Renewable and Non-Traditional Energy Infrastructure Protection,” addresses the unique challenges posed by renewable and non-traditional energy infrastructures, underscoring the need for tailored protection measures for this emerging sector.

This Technical Guide underscores the need for a dynamic and flexible approach to protecting CEI. By integrating good practices, advanced risk management techniques and robust legal and operational frameworks, Member States can enhance the resilience and security of their energy infrastructures. The Guide emphasizes the importance of knowledge-sharing and collaboration among stakeholders to effectively address the evolving threat landscape. Ensuring the continuous functioning of CEI is critical for safeguarding societies and economies from the disruptive impacts of terrorist attacks, thereby maintaining the stability and prosperity of our communities.

Methodologically, this Guide has been developed through a thorough desk research and the inputs of the members of the United Nations Global Programme on Countering Terrorist Threats against Vulnerable Targets, the United Nations Global Network of Experts on Vulnerable Targets Protection,[2] and the United Nations Global Counter-Terrorism Coordination Compact Working Group on Emerging Threats and Critical Infrastructure Protection.

[2] The Network encompasses more than two hundred experts from 84 Member States, including from the public sector, academia, civil society, private sector, and international and regional organizations. For more information: Launch of the United Nations Network of Experts on the Protection of Vulnerable Targets Against Terrorist Attacks and Threat to vulnerable targets.

2. Introduction: context, scope, objectives and methodology

2.1 Context

Over the last decades, terrorists have increasingly demonstrated interest in attacking almost all vulnerable targets, including CEI, due to the potential impact of such attacks. Given the vital role of the energy sector in the functioning of modern societies, existing or apparent physical vulnerabilities of energy infrastructure make it a strategically attractive target for potential attackers. A terrorist attack that damages, disrupts, or destroys an energy infrastructure is likely to multiply its impact—including against a wide range of human rights—given the role such infrastructure frequently plays in maintaining or delivering vital societal functions.

While massive terrorist attacks against CEI involving significant cascading effects have not yet materialized, the threat is still very much present and calls on countries to set up adequate preventive, contingency and resilience plans. Considering that terrorists adapt their behaviour to changes in the security landscape and make use of new technologies, Member States' cooperation and exchange of experiences and good practices on how to effectively counter this threat is essential to ensure a successful, flexible and dynamic approach to target hardening.

In 2017, the United Nations Security Council adopted resolution 2341 (2017)[3] which is the first global instrument fully devoted to the importance of safeguarding CI from terrorist attacks. In that resolution, the Security Council notes, inter alia, "increasing cross-border critical infrastructure interdependencies between countries, such as used for, inter alia, generation, transmission and distribution of energy..." (preamble, S/RES/2341 (2017)). It also recalls Security Council resolution 1373 (2001),[4] which calls on all States to establish terrorist acts as serious criminal offences in domestic laws and regulations and to ensure, as Security Council resolution 2341 (2017) indicates, that they have established criminal responsibility for terrorist attacks intended to destroy or disable CI, as well as the planning of, training for, and financing of and logistical support for such attacks.

In its eighth review of the United Nations Global Counter-Terrorism Strategy (A/RES/77/298),[5] the General Assembly "strongly condemns all terrorist acts against critical infrastructure, including critical energy facilities …" (paragraph 72). In the same resolution, the General Assembly also calls on Member States to strengthen efforts to improve the security and protection of particularly vulnerable targets and encourages them to consider developing or further improving their strategies for reducing risks to CI from terrorist attacks (paragraph 74). Additionally, the resolution recognizes the importance of developing PPPs in this area and calls upon the Global Counter-Terrorism Coordination Compact entities, including UNOCT, to continue

3 S/RES/2341 (2017). Available at S/RES/2341(2017).
4 S/RES/1373 (2001). Available at S/RES/1373(2001).
5 A/RES/77/298. Available at A/RES/77/298.

providing capacity-building support to requesting Member States and to identify and share good practices to prevent terrorist attacks on particularly vulnerable targets.

Member States have also been paying close attention to the essential role of secure energy supplies for international security and development. The United Nations General Assembly adopted several resolutions under the agenda item on sustainable development, including resolution A/RES/78/149 adopted on 19 December 2023[6] on "The pivotal role of reliable and stable energy connectivity in ensuring sustainable development", initiated by Turkmenistan. In that resolution, the General Assembly proposes, inter alia, to hold an expert meeting in 2024 to discuss strategies and develop cooperation with a view to strengthening energy connectivity and supply. Resolution 78/149 was the third one adopted by the General Assembly recognizing the importance of a stable, efficient and reliable energy supply and of international cooperation in this regard (i.e., A/RES/63/210 adopted in 2008 and A/RES/67/263 adopted in 2013). In this context, the Government of Turkmenistan hosted a High-Level Conference on Reliable and Stable Transit of Energy and its Role in Ensuring Sustainable Development and International Cooperation in Ashgabat on 23 April 2009, which brought together Member States, international organizations and industry representatives.

Launched in 2021, the United Nations Global Programme on Countering Terrorist Threats against Vulnerable Targets (hereafter "Global Programme") responds to a call by Member States, including through the General Assembly (GCTS and 8th review resolution A/RES/77/298) and the Security Council (resolutions 2341 (2017) and 2396 (2017)[7]; and the Security Council Madrid Guiding Principles on Foreign Terrorist Fighters and their 2018 Addendum[8]), to support Member States to address priorities, gaps and challenges in protecting vulnerable targets, which include CI and public places ("soft" targets). In particular, the United Nations Security Council, in its resolution 2341 (2017), recognized the "growing importance of ensuring reliability and resilience of critical infrastructure and its protection from terrorist attacks for national security, public safety and the economy of the concerned States as well as well-being and welfare of their population" (preamble). In addition, the Security Council "encourages all States to make concerted and coordinated efforts, including through international cooperation, to raise awareness, to expand knowledge and understanding of the challenges posed by terrorist attacks, in order to improve preparedness for such attacks against critical infrastructure" (paragraph 2). Furthermore, the 2018 Addendum to the Madrid Guiding Principles (S/2018/1177) contains two specific recommendations (No. 50 and 51) on measures "to protect critical infrastructure and soft targets from terrorist attacks" and underlines the need to deliver effective and targeted capacity development, training and other necessary resources, and technical assistance.

The Global Programme seeks to strengthen Member States' capacity to prevent, protect, mitigate, investigate, respond to and recover from terrorist attacks against vulnerable targets at the national, regional and global levels. The Programme's mandate covers both CI and "soft" targets or public places, as well as their exposure to threats from terrorist use of UAS. UNOCT leads the Programme implementation in partnership with the CTED, the United Nations Alliance of Civilizations (UNAOC) and the United Nations Interregional Crime and Justice Research Institute (UNICRI), and in consultation with INTERPOL.

6 A/RES/78/149. Available at A/RES/78/149.
7 S/RES/2396 (2017). Available at S/RES/2396(2017).
8 S/2018/1177. Available at Security Council Guiding Principles on Foreign Terrorist Fighters.

The Global Programme has a strong focus on collecting and disseminating international good practices and development-of-knowledge products and tools as resource documents to enhance the protection of vulnerable targets against terrorist attacks. In 2023, UNOCT, CTED and INTERPOL launched the updated second edition of the Compendium of Good Practices on Critical Infrastructure Protection (CIP). Furthermore, in 2022, UNOCT published five specialized modules with a focus on "soft targets" (i.e. general vulnerable targets protection; urban centres, tourist venues, religious sites and UAS). In this context, this technical guide is developed to provide Member States with access to international good practices and tools on protecting energy sector infrastructure against terrorist attacks.[9]

2.2 Scope

United Nations Security Council resolution 2341 (2017) explicitly recognizes that "each State determines what constitutes its critical infrastructure" (preamble). Definitions of what constitutes CEI might significantly vary from country to country. It usually refers to a wide range of energy-producing and transmission facilities, such as pipelines, electric power grids, storage facilities, refineries, terminals, vessels, tankers, hydropower and nuclear power plants, among others.

For the purposes of this document, the definition of CEI comprises facilities that enable the production (floating oil rigs, compressor stations, liquefied natural gas (LNG) plants, refineries, etc.), storage (storage tanks, aboveground and underground natural gas storage facilities, etc.), transport and distribution (pipelines and fuel terminals, offshore loading system, oil and LNG tankers, etc.) and transmission of energy sources both within one state or across border. For example, oil and gas pipelines can be thousands of kilometers long, and are resource-intensive and difficult to completely secure at each section. In addition, the infrastructure may be dispersed geographically and across multiple jurisdictional boundaries. Even within a single state it may be owned, operated and used by different stakeholders.

Given the extensive experience of many Member States in protecting the infrastructure of the traditional energy sector and its high vulnerability to terrorist attacks, the study mainly addresses international practices of oil and gas infrastructure protection that could be applied to other energy sectors. The protection of renewable and non-traditional energy sectors will be addressed in the sixth chapter of this Technical Guide.

2.3 Objective

The Technical Guide contains international good practices, tools, approaches and reference materials on the protection of CI in the energy sector against terrorist attacks. It is not aimed at reaching an internationally accepted definition on CEI, but rather at sharing useful approaches and practices employed around the world to counter terrorist threats against CEI. Therefore, this document identifies case studies, good practices and tools to help policymakers, practitioners, researchers and other public and private actors to prevent or minimize the impact of terrorist attacks on energy infrastructure. The Guide is thus designed to be used as a practical tool.

[9] These knowledge tools are available at Threat to vulnerable targets.

The international experience, practices, tools and other relevant materials collected as a result of this study form a digital library on energy infrastructure protection and are available for Members of the UN Global Network of Experts on the Protection of Vulnerable Targets on UNOCT's Connect and Learn Platform.

2.4 Methodology

This Technical Guide has been developed through a thorough desk research of open-source information and the inputs of the members of the United Nations Global Programme on Countering Terrorist Threats against Vulnerable Targets, the United Nations Global Network of Experts on Vulnerable Targets Protection, the United Nations Global Counter-Terrorism Coordination Compact Working Group on Emerging Threats and Critical Infrastructure Protection, and UNOCT staff.

Moreover, the research made use of methodological tools such as surveys, tailored data collection tools and case studies that allow for in-depth analysis of specific topics. Tables are included to allow readers to easily locate measures adopted by different countries and help them shape those that would best fit their own institutional and national context. The Technical Guide includes international good practices on both legal and operational frameworks to prevent, mitigate or recover from terrorist attacks against energy facilities.

3. Understanding the challenge

3.1.1. Why Terrorists target critical energy facilities

Secure energy infrastructure is vital for modern societies. Disruptions in energy supply can have disastrous consequences such as economic losses, social disorder, environmental degradation and decreased quality of life, as well as a far-reaching impact on a wide range of human rights.

Critical energy facilities have been frequent targets of terrorist organizations for the last decades. A survey on gas pipeline incidents reveals that intentional acts are the most frequent cause of damage.[10] These facilities represent an attractive target for terrorists seeking to affect the global economy, disrupt supply chains or cause mass casualties.

From 1970–2018, there were almost 2,000 security incidents where energy infrastructure (in many cases gas or oil facilities) was the primary target.[11] According to a study based on the statistics of the Global Terrorism Database of the University of Maryland (USA), between 1970 and –2018, the financial costs of physical damage resulting from terrorist attacks on energy infrastructure were higher than in other sectors (approximately 234–552 thousand US dollars for each incident).[12] Moreover, successful attacks on energy facilities can result in energy shortages, following economic losses and environmental damage.

ISIL (Da'esh) and Al-Qaeda and their affiliates continue targeting oil and gas industry-related facilities. Incidents include, among other examples, a gas pipeline bombing outside Damascus, Syria in 2020 that led to power outages in and around the city;[13] and an armed attack against the town of Palma, close to the "Mozambique LNG" plant in 2021, which led to the evacuation of more than 2,500 people.[14]

ISIL (Da'esh) in Libya declared foreign oil facilities in the country a legitimate target, carrying out armed attacks against the Libyan National Oil Corporation headquarters in Tripoli and oil fields in the country in 2018,[15] as well as the Zillah oil facility in 2019, which caused the death of five people.[16] These incidents, along with attacks on pipelines in Yemen, the Sinai Peninsula and Iraq, demonstrate the ongoing threat to energy infrastructure by terrorist groups.

---

10 Donya Fakhravar, Nima Khakzad, Genserik Reniers, Valerio Cozzani, *Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network*, Process Safety and Environmental Protection, Volume 111, 2017, Pages 714-725, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2017.08.036.

11 Lee, Chia-yi. (2022). Why do terrorists target the energy industry? A review of kidnapping, violence and attacks against energy infrastructure. Energy Research & Social Science. 87. 102459. 10.1016/j.erss.2021.102459.

12 Lavrukhin, M. *Terrorism in the energy industry*. Energy policy / Energeticheskaya politika, Volume 179, 2023. Pages 24-37. https://doi.org/10.46920/2409-5516.2023_1179.24.

13 Available at https://www.reuters.com/article/us-syria-blast-electricity/explosion-on-syria-gas-pipeline-a-terrorist-attack-minister-idUSKBN25K062/.

14 Available at https://totalenergies.com/media/news/press-releases/mozambique-lng-totalenergies-response.

15 Available at https://www.aljazeera.com/news/2018/9/10/libya-national-oil-corporations-tripoli-offices-attacked.

16 Available at https://www.aa.com.tr/en/energy/energy-security/daesh-attacks-oil-facilities-in-libya/26031.

Box 1

Reasons why energy facilities attract terrorists

Relevant studies on terrorism targeting the energy sector reveal why CEI is an attractive target. Some of the reasons include:[17]

- High cost and cascading effects: A successful attack can lead to extensive and hard-to-quantify consequences. For example, Al-Qaeda's attack on an Algerian gas field in 2016 significantly affected the country's production;[18]
- Intimidation (psychological effect): Targeting energy infrastructure can have a profound psychological effect on those directly affected by it. These attacks could also be aimed at destabilizing a country or specific company by undermining their ability to ensure safety.[19] For instance, after a terrorist attack in Mozambique, the French oil company Total suspended operations due to safety concerns, jeopardizing a USD 20 billion investment in gas liquefaction facilities in the country.[20]
- Publicity and symbolism: Some attacks are not focused on causing sensitive damage, but on drawing attention to the terrorist group's activities. Also, some often contribute to recruitment efforts—for example, if such attacks benefit a specific location and improve the delivery of energy and public services to the community, more men and women may feel attracted to support the terrorist group.[21]
- Attack feasibility: The level of protection and a terrorist group's capabilities determine the feasibility of an attack. Relatively easy access can encourage terrorists to strike.
- Financing: Some studies indicate that attacks on energy facilities are considered an integral part of the strategy to fund further terrorist activities. Such an approach, for instance, is taken by terrorist groups like ISIL (Da'esh) in Iraq and Syria.[22] Terrorists may kidnap personnel and extort energy facilities for ransom, or hijack oil or LNG tankers. Terrorist groups may also finance and support attacks through other illegal activities such as theft of oil or gas from pipelines, extortion or selling raw materials.[23]

3.1.2. General patterns and characteristics of terrorist targeting of CEI

Over the past few decades, terrorist attacks on energy infrastructure have evolved in tactics and in modus operandi. Today, experts are alerting to the transition in terrorist attacks from symbolic ones to highly planned

17 Lee, Chia-yi. (2022). *Why do terrorists target the energy industry? A review of kidnapping, violence and attacks against energy infrastructure*. Energy Research & Social Science. 87. 102459. 10.1016/j.erss.2021.102459; Toft, Peter & Duero, Arash & Bi, Ar. (2010). Terrorist targeting and energy security. Energy Policy. 38. 4411-4421. 10.1016/j.enpol.2010.03.070.; James A. Piazza, *Oil and Terrorism: An Investigation of Mediators*, Public Choice 169 (2016): 251–68, https://doi.org/10.1007/s11127-016-0357-0.

18 Available at https://www.reuters.com/article/idUSKCN0WL0AM/.

19 Piazza James A., *Oil and Terrorism: An Investigation of Mediators*, Public Choice 169 (2016): 251–68, https://doi.org/10.1007/s11127-016-0357-0.

20 Available at https://www.reuters.com/world/africa/frances-total-declares-force-majeure-mozambique-lng-project-2021-04-26/.

21 This has been the case, for example, in regard to water-related infrastructures. See UNOCT-CTED *Compendium of Good Practices on Critical Infrastructure Protection*, p. 27.

22 Tichý, Lukáš. (2019). *Energy Infrastructure as a Target of Terrorist Attacks from the Islamic State in Iraq and Syria*. International Journal of Critical Infrastructure Protection. 25. 10.1016/j.ijcip.2019.01.003.

23 Ibid.

coordinated physical and virtual attacks—i.e. use of ICTs for malicious purposes.[24] In some cases, terrorist actions are even more sophisticated: attacks on physical facilities of energy infrastructure are accompanied by attacks against their control systems and/or other ICT-enabled technologies.

Despite the variety of terrorist attacks on critical energy facilities they may be classified by:

- Nature (physical or information): While a physical attack is aimed at destroying an infrastructure, weakening it or rendering it inoperative in full or partially, the use of ICTs for malicious purposes aims to shut down or limit access to technological systems that are crucial to the functioning of the energy infrastructure and/or to tamper with data.
- Origin (insider or external): Effectively protecting energy infrastructure from external attacks, which are the most common, requires stakeholders to take numerous actions. Insider threats occur when employees, suppliers or contractors who have access to sensitive information misuse their privileges to exploit vulnerabilities within the organization. These threats pose significant risks to the security of CEI and represent an important challenge. Despite the facility being well-protected from external attacks, insiders can still gain access to valuable information and cause significant damage.
- Context in which they occur (isolated or multiple targets): Attacks against energy facilities could be either an isolated act or part of a broader, more complex plan to harm energy infrastructure—e.g., different facilities or parts of infrastructure located in the same area. As noted, in recent years, terrorist groups have demonstrated their ability to plan and execute complex attacks simultaneously against multiple targets. With the growing stability of energy infrastructure, the frequency of these attacks may increase because terrorists need to disable multiple power lines simultaneously to carry out a blackout.[25]
- Level of planning (spontaneous/ad hoc or coordinated): Attacks could be one-time, non-systemic in nature or be a part of a sophisticated strategy that includes different planning stages and phases that could go from revealing the most vulnerable parts of the facility to exposing different areas simultaneously.
- Targeting (direct or indirect): While a direct attack is aimed at disrupting the functioning of the infrastructure through on-target impact, indirect attacks could provoke disruption as a result of attacks on other CI, resulting in a "cascading effect".

3.1.3. Terrorist attack modus operandi

The analysis of terrorist attacks demonstrates that recent attacks on CEI can be characterized by the following modus operandi:

- Armed assault. Such attacks may be undertaken to:
    - Capture facilities: terrorist groups could try to seize an energy infrastructure facility, which could in turn serve to finance terrorist activities.

[24] Wang L., Wang X., Zhao Q., Zhao Y. *Multi-objective policing emergency logistics scheduling on multi-location coordinated terrorist attacks*, 2017, Xitong Gongcheng Lilun yu Shijian/System Engineering Theory and Practice. 37, available at: https://www.researchgate.net/publication/322482361_Multi-objective_policing_emergency_logistics_scheduling_on_multi-location_coordinated_terrorist_attacks.

[25] Lilliestam, J. (2014): Vulnerability to terrorist attacks in European electricity decarbonisation scenarios: comparing renewable electricity imports to gas imports, Energy Policy 66, pp. 234-248, available at http://dx.doi.org/10.1016/j.enpol.2013.10.078.

- Take hostages: terrorists could kidnap personnel of energy facilities for ransom or to acquire insider information. A recent example of this modus operandi can be found in May 2023, when 50 terrorists attacked oil plant facilities of the MOL Pakistan Oil and Gas Company in Hangu district, Pakistan.[26]

- Compromising physical structures of critical energy facilities by:
  - Sabotage, mining, bombing: Energy facilities such as pipelines could be mined and destroyed remotely. For instance, most of ISIL (Da'esh) attacks on natural gas pipelines in the Sinai Peninsula (Egypt) were carried out by mining the facility.[27]
  - Arson: Energy supply, in particular oil and gas supply, involves storage and transportation of explosive liquids. These liquids are particularly vulnerable to open flame and arson and could cause massive damage.
- Attacks using ICTs: Attacks on energy infrastructure might focus, inter alia, on industrial control systems with the intent to destroy or limit the functionality of CI services.[28] These attacks may target a single service provider, but the impact can cascade and disrupt other interdependent infrastructure services. Attacks using ICT on energy infrastructure may be aimed at damaging industrial automation and control systems, tampering with systems or data, shutting down or limiting access to crucial systems or damaging physical equipment due to the disruption of a technological process.

3.2 CEI vulnerabilities

Although no massive terrorist attacks on energy infrastructure with significant cascading effects have occurred to date, this threat is significant enough to require Member States to adopt adequate, preventive measures and contingency plans based on existing legal frameworks. Indeed, past terrorist activities have exposed the inherent vulnerabilities of a number of energy facilities.

3.2.1. CEI specific vulnerability factors

CEI's specific vulnerabilities stem from several factors:

- Reliance on a wide range of resources, including water, telecommunications, data, finance and others, can create a situation where even a minor impact or short-term failure can render the entire facility and its associated industries inoperative. Such dependence has significant implications for populations, given the critical role this infrastructure often plays in maintaining and delivering vital societal functions. In turn, attacks can also have a far-reaching impact on a wide range of human rights, from the right to life and security of persons to the right to health and to a healthy environment, the right to education, as well as other aspects of the right to an adequate standard of living.
- The length and geographical dispersion of energy transportation facilities, such as oil and gas pipelines, pose significant challenges. These pipelines, which are integral to CEI, can extend for thousands of

[26] Available at https://www.reuters.com/world/asia-pacific/islamist-militants-kill-six-gas-oil-extraction-plant-pakistan-2023-05-23/.
[27] Available at https://www.aljazeera.com/economy/2020/2/3/gas-pipeline-in-egypts-sinai-attacked-israel-imports-unaffected; https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=202012240006.
[28] More detailed information and statistics can be found in the Kaspersky's reports on main incidents in the field of industrial information and communications technologies security in 2020, 2021, 2022, 2023, available at: https://ics-cert.kaspersky.com/publications/reports/.

kilometers, making comprehensive physical protection difficult and costly. Key characteristics of pipelines include their vast length, extension across several countries and relatively easy access. Additionally, the infrastructure often crosses multiple jurisdictional boundaries and international waters, complicating efforts to prevent terrorist attacks. Even within a single state, ownership and operation are often fragmented among various stakeholders, including government entities, private companies and local communities. This fragmentation can create operational, organizational and communication hurdles, hindering effective responses to potential terrorist threats.

- The intensive digitalization of the energy sector has created dependencies on the functioning of information and control systems. In many countries, the energy sector is a leader in digital transformation, utilizing the Internet of Things,[29] AI technologies and remote-control systems. Consequently, the extensive use of remote control and intelligent data processing has led to a high dependence on the stability and proper operation of the information systems supporting these processes. In this context, various vulnerabilities related to information and communications technology security, such as monitoring systems distortions and unauthorized access to control systems, have become increasingly relevant.
- The high dependence of energy infrastructure on other critical sectors, such as the proper functioning of supply chains and transportation systems, is essential for the timely and secure movement of employees, equipment, and other necessary resources. Additionally, water supply for cooling system and telecommunication systems are crucial for data storage, transmission and remote control of CEI.
- The complex, knowledge-intensive and technological processes involved in CEI operations create a high risk of insider threats. These threats can originate from employees, contractors, individuals or others with close affiliations to an energy facility with relevant knowledge and access to sensitive information, which could facilitate a successful attack. The combination of intricate operational processes and the potential for insiders to misuse their access underscores the critical need for robust security measures to protect against these internal threats.
- Facility-specific vulnerabilities (production, storage, transmission and distribution) add another layer of risk. The nature of the energy facility, including the presence of high-hazard structures such as gas compressor units, introduces additional vulnerabilities related to its specific functions. For instance, power grids, which are highly interconnected and often rely on central control, are more susceptible to attacks using ICTs than to physical attacks.
- Location-specific vulnerabilities:
    - Climate or weather conditions: Protection measures are not equally effective in areas with different climatic and weather conditions. This can create additional vulnerabilities. For example, UAS detection tools may not work properly in areas with predominantly foggy or rainy weather.[30]
    - High level of activity of local terrorist groups. In particular, CEI in areas with socioeconomic instability and high levels of terrorist recruitment may have a higher risk of being targeted.

[29] The Internet of Things is a system of interrelated computing devices that can collect and transfer data over a wireless network without human input.

[30] Luo K., Luo R, Zhou Y. et al (2021) *UAV detection based on rainy environment*, 2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), available at: https://ieeexplore.ieee.org/document/9482383.

- Easy access due to geographical position. For instance, experts have outlined that maritime areas are at a greater risk due to their typically lower level of control compared to on-land infrastructure.[31]

Table 1

Vulnerabilities of different types of oil/gas facilities

Oil and LNG tankers	Due to their size and relatively low speed, oil tankers are more vulnerable to physical attacks, including by UAS, than other ships. Additionally, oil tankers often follow predictable routes, and navigate narrow straits and checkpoints that restrict their manoeuvrability, making them easier targets for attackers. International regulations and security considerations typically limit oil tankers from carrying defensive weapons, which makes them more prone to terrorist hijackings.
Ground oil and gas pipelines	Oil and gas pipelines transport highly flammable substances at high pressure, making them vulnerable to rupture and fire if damaged by explosives. Due to their vast length and location across both densely populated and remote, sparsely inhabited areas, it is usually difficult to prevent or even identify attempts to plant bombs along pipelines. Terrorists often hide explosives near or under pipeline infrastructure. For example, ISIL (Da'esh) damaged a natural gas pipeline in 2020 in Egypt's Sinai Peninsula by detonating a bomb planted under the facility.[32]
Undersea oil and gas pipelines	Underwater facilities are difficult to protect through traditional means like patrols or surveillance. Their security is mainly controlled by computer systems that receive data/alerts from a variety of sensors, which can be disabled or manipulated.
Refineries, oil and gas plants	The complexity of technical processes carried out in oil and gas plants and refineries substantially increases the risk of sabotage by employees. Additionally, these facilities typically have a large number of personnel and receive external suppliers and contractors, creating additional challenges in preventing insider threats. The terrorist attack on the Tigentourine gas plant in Algeria in 2013 demonstrated that such facilities are vulnerable to direct attacks, especially when abetted by insider support, and can result in massive casualties.[33]
Port terminal	By their very nature, port terminals face inherent security challenges. They require accessibility by land and sea and are often situated in densely populated areas, creating a complex security environment. Due to the high intensity of processes and the workload at ports, entrance security is often a challenge, exposing ports to sabotage and other criminal activities. In many cases seaports host or are adjacent to oil or LNG storage facilities and refineries that entail additional vulnerabilities. Moreover, most seaport operators have increasingly integrated information systems that could suffer ICT-based attacks.
Offshore oil platform	Due to their remote location, oil platforms face significant security challenges. Their isolation makes it difficult to deploy additional security personnel or reinforcements rapidly in response to threats like arson or insider attacks.
Oil and LNG storage tanks	Storage facilities contain significant amounts of highly explosive materials. Storage tanks are therefore more vulnerable to explosives, including UAS attacks.

31 T. Prodan, *Maritime Terrorism and Resilience of Maritime Critical Infrastructure*, National Security and the Future, 1-2/18 (2017), p. 103. pp. 103-122.

32 Available at https://www.aljazeera.com/economy/2020/2/3/gas-pipeline-in-egypts-sinai-attacked-israel-imports-unaffected.

33 The *In Amenas Attack, Report of the Investigation into the Terrorist Attack on In Amenas*, Statoil, February 2013, available at: www.statoil.com/en/NewsAndMedia/News/2013/Downloads/In%20Amenas%20report.pdf.

Box 2

Insider threat to energy infrastructure

Terrorism in the form of an insider threat takes the form of unlawful activities by employees, contractors, individuals or others with close affiliations to an energy facility with relevant knowledge and access to sensitive information that could facilitate a successful attack against a CEI for terrorist purposes.[34] In this context, insider threats are a significant security concern for energy infrastructure, as a successful insider attack has the potential to damage assets and interrupt critical services that society depends upon.

The complex, knowledge-intensive and technological processes involved in CEI operations create a high risk of insider threats. The energy sector has significantly evolved over the past years, partly due to globalization and the increase in outsourcing processes. While insider threats often refer to employees or contractors of the facilities, in some cases, it also includes outsiders who may be able to gather sensitive information. Diversification of suppliers, short-term hiring and other factors sometimes reduce the ability of CEI operators to thoroughly vet personnel. In this situation, a system of pre-emptive measures and early warning is necessary.

Security measures to prevent insider attacks could include:

- Security services personnel exercises: Providing regular training exercises for security personnel to enhance their preparedness and response capabilities.
- Comprehensive employee screening and vetting: Implementing thorough background checks and vetting procedures for all prospective employees to mitigate insider threats.
- Psychological and behavioural insights: Considering the use of psychological assessments and monitoring of behaviour as potential tools to identify individuals who may pose a security threat.

Studies have particularly revealed that signs of suspicious behaviours can be identified prior to a terrorist act taking place, but that such behaviours are not normally reported.[35] Relevant stakeholders can address this vulnerability by providing specialized training to identify concerning behaviours that may indicate a risk of a terrorist act being planned or underway when analyzed alongside other risk considerations, and by establishing clear and confidential reporting channels. Concerning behaviours often include absenteeism, undue tardiness, dishonesty, conflicts with other employees, repeated instances of coming to the office outside of working hours or a rapid increase in wealth.[36]

34 Insider threats are a particular concern in a number of sectors aside CEI. For example, in aviation security. *See ICAO Insider Threat Toolkit*, available at https://www.icao.int/Security/Security-Culture/Pages/ICAO-Insider-Threat-Toolkit.aspx.

35 Bell, Alison & Rogers, Brooke & Pearce, Julia. (2018). The *Insider Threat: Behavioral indicators and factors influencing likelihood of intervention*. International Journal of Critical Infrastructure Protection. 24. 10.1016/j.ijcip.2018.12.001.Available at https://www.researchgate.net/publication/329419966.

36 Ibid.

3.2.2. Interdependence across CI sectors (transportation, communications, finance and public infrastructure)

CI across sectors comprises a complex, interconnected ecosystem and their interdependencies lead to additional vulnerabilities.

The ramifications of possible terrorist attacks are numerous since all sectors of the economy rely on energy to operate. Exploiting weaknesses in the grid's CI has thus the potential to initiate a "cascade effect" that may hinder or halt operations in other sectors, such as transport, finance and communication. Damage or destruction of that infrastructure could lead to disruption or interruption of services across sectors and sometimes across national borders.

Table 2

Interdependencies of CI with a focus on energy infrastructure

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

Source: DEFENDER D6.2: CEI Security Stakeholder Group Manifest, available at: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b7096f83&appId=PPGMS

3.2.3. Cross-border interdependencies

The ever-increasing complexity and interdependencies in the energy infrastructure not only have given rise to new risks and vulnerabilities, but may also exacerbate the severity and the extent of potential consequences that are not confined limited to the premises of individual energy facilities.

For example, the European Union has adopted the Trans-European Networks for Energy (TEN-E) policy that is focused on linking the energy infrastructure of EU countries to provide security of supply.[37] Such an integrated energy network could help to avoid or mitigate interruptions of service due to different causes, including terrorist attacks.

Another vivid example of cross-border CEI is the USA–Canada Keystone oil Pipeline. It runs from the Western Canadian Sedimentary Basin in Alberta to oil refineries in Illinois and Texas, USA, and to oil tank farms and an oil pipeline distribution centre in Oklahoma, USA.[38]

Modern energy infrastructure includes pipelines spanning thousands of kilometers that connect oil and gas plants with consumers. Cross-border energy infrastructure is likely to expand as energy deposits near traditional markets become depleted due to increasing demand. The African cross-border natural gas pipelines currently under construction are a good example of this (the Trans-Saharan gas pipeline and the Nigeria-Morocco gas pipeline among others).[39]

In the coming decades digital transformation will aim to make energy systems more connected, efficient, reliable and sustainable, including through Artificial Intelligence (AI).[40] Advances in digital technologies and services have accelerated the digital transformation of energy in recent years, particularly in electricity networks.[41]

At the same time, digitalization introduces significant additional risks, such as increased dependence on electrical energy supply. Today, all CI sectors depend on a stable supply of electricity. For example, the deep interdependence between electricity and communications systems underscores the need for enhanced resilience.[42]

Moreover, protecting critical electric energy infrastructure is essential for information security. While attacks using ICTs on energy infrastructure can cause physical damage, the reverse is also true: physical damage to electrical infrastructure can disrupt ICT-related systems.

37 Trans-European Networks for Energy, 2020, available at:https://energy.ec.europa.eu/topics/infrastructure/trans-european-networks-energy_en.
38 Keystone Pipeline System, available at https://www.tcenergy.com/operations/oil-and-liquids/keystone-pipeline-system/.
39 *Multi-Billion Dollar Opportunities in Cross-Border Cooperation for Oil and Natural Gas Projects in Southern Africa*, available at: https://energychamber.org/multi-billion-dollar-opportunities-in-cross-border-cooperation-for-oil-and-natural-gas-projects-in-southern-africa/.
40 *Digitalization of the energy system,* available at https://energy.ec.europa.eu/topics/energy-systems-integration/digitalisation-energy-system_en.
41 *Digitalisation*, International Energy Agency, available at https://www.iea.org/energy-system/decarbonisation-enablers/digitalisation.
42 *Digitalisation – Essential for Energy System Transformation. But What About Communications?*, 12 June 2023, available at https://www.techuk.org/resource/digitalisation-essential-for-energy-system-transformation-but-what-about-communications-guest-blog-by-grid-scientific-limited.html.

3.3 Changes in the security landscape

3.3.1. Use of new and emerging technologies by terrorists

There is an increasing trend of terrorists using new and emerging technologies both to carry out attacks and to provide support for terrorist activities (financing, propaganda, etc.). The technology landscape is evolving rapidly, making it challenging to keep up with technological advancements and their potential misuse by terrorists. This includes targeting facilities, networks, processes and other critical assets within the energy sector.

Experts have identified the following new technologies as potential means that terrorists could use to target energy infrastructure:

- Artificial intelligence and machine learning (particularly neural networks) might be used by terrorists for multiple purposes, i.e., from recognizing sites and people in video surveillance during the planning stages of an attack to selecting tools for hacking information and control CEI systems. Additional information can be found in the report *Algorithms and Terrorism: The Malicious use of artificial intelligence for terrorist purposes* published by UNICRI and the United Nations Counter-Terrorism Centre (UNCCT) of UNOCT (Global Counter Terrorism Programme on Cybersecurity and New Technologies).[43]
- Remotely operated systems, such as unmanned aircraft systems (UAS), uncrewed ground vehicles (UGV) or remotely operated underground vehicles (ROUV) have been increasingly used against energy infrastructure, including underground and underwater oil and gas pipelines.
- 3D printing technology, which, for example, is used to produce components of improvised explosive devices (IEDs) or to assemble UAS or ROUV.
- ICT such as:
    - Virtual private networks (VPNs) and proxy services, which can mask users' locations and disguise IP information.
    - The so-called "Dark Web," which offers a hidden and largely undetectable network for terrorist groups like ISIL (Da'esh) and their affiliates. This platform allows them to share sensitive information, plan attacks on CEI, and store training materials.[44] Additional information can be found in the report "Beneath the Surface: Terrorist and Violent Extremist use of the Dark Web and Cybercrime-as-a-Service for Cyber-Attack" published by UNICRI and UNOCT/UNCCT (Global Counter Terrorism Programme on Cybersecurity and New Technologies).[45]

More importantly, in recent years, terrorist attacks on energy infrastructure have become more sophisticated, often combining physical attacks with attacks using ICTs against control systems and other ICT-enabled technologies. A potential scenario includes a conventional bombing attack on the physical site of a CI

[43] UNOCT/UNCCT – UNICRI report *Algorithms and Terrorism: The Malicious use of artificial intelligence for terrorist purposes*, available at malicious-use-of-ai-uncct-unicri-report-hd.pdf.

[44] *Law enforcement capabilities framework for new technologies in countering terrorism*, UNOCT, UNCCT, INTERPOL, available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_law_enforecement_capabilities_web2.pdf.

[45] UNOCT/UNCCT – UNICRI report *Beneath the Surface: Terrorist and Violent Extremist use of the Dark Web and Cybercrime-as-a-Service for Cyber-Attack*, dw_beneath_the_surface_update.pdf (un.org).

combined with a distributed denial-of-service (DDoS) attack which temporarily disrupts the network traffic of the site. Such combined attacks can impair emergency response efforts, potentially increasing casualties and causing widespread public panic.

3.3.2. UAS-related terrorist attacks

The rapid evolution of UAS and their usage in terrorist attacks have significantly altered the security environment over the past decade. The remote operation capabilities of UAS, combined with their availability through commercial markets and ease of assembly, have made them a substantial threat. Successful large-scale UAS attacks on oil facilities in Saudi Arabia, such as those at Abqaiq-Khurais in 2019 and Jeddah in 2022, have highlighted the vulnerability of these kinds of facilities to such attacks across the world.[46]

The United Nations Security Council Counter-Terrorism Committee's Delhi Declaration[47] on countering the use of new and emerging technologies for terrorist purposes notes with "concern the increasing global misuse of unmanned aerial systems by terrorists to conduct attacks against, and incursions into critical infrastructure" (p.7). Furthermore, the non-binding guiding principles on threats posed by the use of UAS for terrorist purposes, known and referred to as the "Abu Dhabi Guiding Principles", were adopted in December 2023 and prepared in accordance with the Delhi Declaration, in which the Committee decided to develop a set of non-binding guiding principles to assist Member States in countering the threat posed by the use of new and emerging technologies for terrorist purposes.

Similarly, the United Nations Security Council, through resolution 2370 (2017),[48] moved to "strongly condemn the continued flow of weapons, including small arms and light weapons (SALW), military equipment, UAS and their components and IED components to and between ISIL (also known as Da'esh), Al-Qaida, their affiliates, and associated groups, illegal armed groups and criminals, and encourage) Member States to prevent and disrupt procurement networks for such weapons, systems and components". The Global Programme on Countering Terrorist Use of Weapons of UNOCT jointly with CTED and the United Nations Institute for Disarmament Research (UNIDIR) developed Technical Guidelines to facilitate the implementation of this resolution, comprehensively covering preventive and response measures to counter terrorist use of SALW, IEDs and UAS[49] and promoted its use in 43 countries.

The United Nations has actively developed tools to assist member states in combating this threat. The Global Counter-Terrorism Programme on Autonomous and Remotely Operated Systems (AROS Programme),[50] established in 2021, provides a vivid example of these efforts.[51] Through the AROS program, UNOCT and its implementing partners support Member States in developing frameworks that prioritize the protection of human rights, international humanitarian law and gender equality, while ensuring that counter-terrorism measures do not impede the legitimate use of UAS or hinder technological progress.

46 Available at https://apnews.com/article/d20f80188e3543bfb36d512df7777cd4.
47 United Nations Counter-Terrorism Committee Delhi Declaration. Available here.
48 S/RES/2370 (2017). Available at S/RES/2370(2017).
49 Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017) and related international standards and good practices on preventing terrorists from acquiring weapons, 2022, available at https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/cted_guidelines_2370.pdf.
50 https://www.un.org/counterterrorism/autonomous-and-remotely-operated-systems.
51 Available at https://www.un.org/counterterrorism/autonomous-and-remotely-operated-systems.

Furthermore, the United Nations Global Programme on Countering Terrorist Threats against Vulnerable Targets has published a technical guide titled *Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems*. This guide outlines best practices for safeguarding against terrorist attacks utilizing UAS. It highlights that "UAS offer terrorist groups a set of distinct advantages as part of their attack strategies, most crucially a greater potential to circumvent traditional physical protection measures based on multiple levels of security (e.g., in the form of hardened venue perimeters designed to stem vehicle-borne attacks, armed guards or visitor-screening barriers)".[52]

Additionally, in 2022 the United Nations Global Counter-Terrorism Coordination Compact Working Group on Border Management and Law Enforcement relating to Counter-Terrorism issued the *Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017) and related international standards and good practices on preventing terrorists from acquiring weapons* implemented by CTED, as the Chair of the Working Group, together with UNIDIR and UNOCT/UNCCT, in close cooperation and collaboration with members of the Working Group. The technical guidelines suggest an approach, which can support Member States in eliminating the supply of SALW and associated ammunition, IEDs and their components, and UAS and their components to terrorists.

The massive increase in the number of form factors, capabilities, ease of access and ease of operation of UAS at low cost could make them the weapon of choice for future terrorists.[53] The range and capabilities of UAS influence how they could be used in terrorist attacks on energy facilities.[54] Micro-UAV (Unmanned Aerial Vehicles) are used for close-proximity attacks directly targeting CEI. Conversely, medium-UAVs, with their long range, could cross dozens of kilometers before striking the facility.

So, UAS could be used by terrorists to attack CEI in following ways:

- Bombing energy facilities: Such attacks could take the form of suicide bombing of small UAVs (like First-Person View (FPV) drones) or dropping explosive devices from a UAV.
- reconnaissance of objects using photographic and video equipment, other technical means of observation and collection of information (such as the location of its critical elements and vulnerable areas, elements of physical protection and security forces, etc.).

Moreover, terrorists may use UAS to carry out attacks with the use of ICTs on non-UAS targets. Under this scenario, a UAV could be used as an "information weapon" to deliver malware against other systems such as critical information infrastructure. With the expansion of 5G technology as the new standard for broadband cellular networks, UAS's "communication payloads" may potentially become easier-to-use tools to disrupt

---

52 *Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS),* 2022, available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod5-unmanned_aircraft_systems_final-web.pdf

53 Thomas G. Pledger, *The Role of Drones in Future Terrorist Attacks*, available at: https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf.

54 UAS can be divided into four groups depending on UAV weight and, accordingly, battery charge and transport capabilities:
- Micro – the weight does not exceed 10 kg, they can stay in the air for no more than an hour
- Small – they weigh up to 50 kg and are capable of performing work for up to 5 hours without break
- Medium – the weight reaches one ton, with continuous operation time of up to 15 hours
- Heavy – they weigh more than a ton, they can operate for more than 24 hours, and some are capable of intercontinental flights.

private wireless communications.[55] UAS attacks could also be a part of a coordinated attack and be combined with attacks that use ICTs in-air target detection systems or surveillance systems of CEI.

Box 3
UAS "swarm attacks" on CEI

"Swarm" attacks are multiple UASs flying platforms integrated into a single networked system self-contained for communication, reconnaissance and weapons to strike an enemy target. So-called "swarm attacks" can enable terrorists to conduct multiple UAS-attacks nearly simultaneously, rapidly magnifying their overall effect.

These "swarms" could consist of low-tech drones, but they are aimed at overwhelming the defensive capabilities of CEI. One technology that could enable drone swarm efficiency is ad-hoc Bluetooth networks. These Bluetooth networks are low-power, local networks that self-organize and share information in real-time. The ability of "swarms" to self-organize and self-coordinate will continue to improve with computing power, which is simultaneously improving the ability of drones at targeting.[56]

3.3.3. Rapidly changing threat environment with growing threats of use of ICT for malicious purposes against CEI

As ICTs play an increasingly central role in the automation of energy production and energy transition, CEI becomes more vulnerable to terrorist attacks that use these technologies. Unlike physical attacks, in this kind of attack terrorists do not need physical access or proximity to an infrastructure facility. The Internet and broader ICT have equipped terrorists with new tools and capabilities, enabling them not only to recruit, finance and plan terrorist activities but also to execute attacks against CI, including energy facilities. Among other CI sectors, energy infrastructure suffers more than a third of all computer attacks.[57]

In the month of May 2023, Danish CEI was exposed to the most extensive attack with the use of ICTs in its history. More than 20 companies that operate parts of the Danish energy infrastructure were compromised in a coordinated attack. The result was that the attackers gained access to some of the companies' industrial control systems and several companies had to go into island mode operation.[58]

Attribution remains a significant challenge in the realm of attacks using ICTs. Determining the origin and responsible parties behind these attacks is exceptionally complex due to the ease of anonymization in the Internet. Notably, the potential consequences of attacks with the use of ICTs can be as severe as, or even more severe than, those of physical attacks, regardless of the motive. While terrorist groups may not explicitly

55 *Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS)*, 2022, available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod5-unmanned_aircraft_systems_final-web.pdf.

56 Thomas G. Pledger, *The Role of Drones in Future Terrorist Attacks*, available at: https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf.

57 *Energy sector faces 39% of critical infrastructure attacks*, Security, available at: https://www.securitymagazine.com/articles/99915-energy-sector-faces-39-of-critical-infrastructure-attacks.

58 *The attack against Danish, critical infrastructure,* 2023, available at: https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf.

claim responsibility for ICT-related attacks on CEI, the growing accessibility of ICT technologies has contributed to a growing and escalating threat landscape in this domain.

ICT-related attacks against CEI might include:

- Distributed Denial-of-Service (DDoS) attacks: These can impair network connections and essential resources, causing systems to fail and disrupting the operation of information and communication systems.
- Ransomware attacks: These can be facilitated through phishing. Ransomware affecting a network can block systems and disrupt the routine activities of CI operators, potentially impacting their operations. For example, in 2019, a massive ransomware attack targeted the Information Technology systems of Angola's National Fuel Society (Sonangol).[59] The attackers accessed data from over seven thousand computers, including sensitive and insider information about the company and its customers.
- Unauthorized use of remote maintenance access points: These access points, intentionally created as external entrances to information and communication networks, are often inadequately secured.

Moreover, energy infrastructure requires a sector-specific approach that goes beyond standard information security measures applied to information technology systems. This is due to the unique characteristics and additional vulnerabilities of information systems within the energy sector.

Table 3

OSCE table on vulnerabilities of energy infrastructure to attacks with the use of ICTs

Asset	Description of Possible Vulnerabilities and Attack Vectors
Software	Applications or system software may have accidentally or deliberately introduced flaws that can be exploited to subvert the purpose for which the software was designed.
Hardware	Vulnerabilities can be found in hardware, including microprocessors, microcontrollers, circuit boards, power supplies, peripherals such as printers or scanners, storage devices and communications equipment such as network cards. Tampering with such components may alter the intended functionality of the component or provide opportunities to introduce malware.
Seams between hardware and software	An example of such a seam might be the reprogrammable read-only memory of a computer (firmware) that can be improperly and clandestinely reprogrammed.
Communication channels	Communication channels between a system or network and the external world can be exploited by malicious actors in various ways. They can impersonate authorized users, jam the channels to deny access to legitimate users, or eavesdrop to gather classified or confidential information.
Configuration	Most systems provide a variety of configuration options that users can set based on their own trade-offs between security and convenience. Because convenience is often valued more than security, many systems are, in practice, configured insecurely.

[59] Available at https://businesselitesafrica.com/2019/06/07/sonangol-suffers-attempted-cyber-attack/?v=f9308c5d0596#:~:text=The%20National%20Fuel%20Society%20of,company%20explained%20in%20a%20statement.

Asset	Description of Possible Vulnerabilities and Attack Vectors
Users and operators	Authorized users and operators of a system or network can be tricked or blackmailed into doing the bidding of an adversary, or they may sell their services.
Service providers	Many computer installations rely on outside parties to provide computer-related services, such as maintenance or Internet service. A malicious actor may be able to persuade a service provider to take some special action on its behalf, such as installing attack software on a target computer.

Source: OSCE Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, available at https://www.osce.org/files/f/documents/4/b/103500.pdf.

The energy sector, particularly the electric and gas subsectors, exhibits a unique interdependence between physical infrastructure and information technology (IT) systems. This convergence creates vulnerabilities that malicious actors can exploit. These vulnerabilities encompass various risks, including the manipulation of operational technology (OT) systems to disrupt critical equipment operations. Given that CEI operators might rely on data from safety and transport monitoring systems — used to regulate the flow of electricity or gas — without additional manual validation, manipulation of OT systems could lead to dangerous overages, potentially damaging equipment.

The vulnerability landscape of the energy sector is further amplified by the threat of insider attacks involving the use of ICTs. Authorized personnel, including employees and contractors, pose a significant threat due to their access privileges to critical information systems. This access can be misused, either inadvertently or intentionally (e.g., in the case of radicalized individuals).[60]

[60] For more information: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities.

Box 4

Vulnerabilities related to the use of smart devices to operate CEI and SCADA-systems

SCADA is a computer-based system used by industries and CI to monitor and control sensitive processes and physical functions. Control systems can be used to monitor simple processes or to manage the more complex activities of an electric smart grid or nuclear power plant. Across different generations, SCADA has undergone significant evolution from a typically isolated environment to a highly interconnected network.

According to attacks with the use of ICTs, statistics, SCADA systems are targeted in more than 50 percent[61] of cases. It is generally recognized that smart devices and SCADA will allow entry to CEI, allowing practically anyone to gain access and interact with the infrastructure.

According to sophisticated research of SCADA vulnerabilities, common security attacks against SCADA are:

- A denial of service (DoS) attack floods a target entity with more traffic. By contrast, distributed denial of service (DDoS) is type of DoS in which multiple compromised computers simultaneously attack a target entity.
- Memory corruption attacks occur when the memory location is modified due to programming errors.
- Privilege escalation attacks occur when a threat actor obtains unauthorized access to a user account with administrative privileges to increase permissions.
- Privilege elevation attacks occur when a threat actor obtains direct unauthorized access to a SCADA system with privileges.
- Arbitrary and remote code execution is an attack resulting from related attacks and SCADA vulnerabilities, such as buffer overflow.
- Reconnaissance allows an attacker to gather information about a SCADA network's topology and data values, device functions or sensitive information stored on automation controllers.
- Reset-function-code attacks occur when unprotected SCADA communication protocols lack the proper authentication and authorization. An adversary may change the original state of a SCADA device by resetting the function code of that device to be in an inconsistent state, causing an outage of service.
- An SQL injection attack is a code injection attack that exposes data-driven applications.

Source: Manar Alanazi, Abdun Mahmood, Mohammad Jabed Morshed Chowdhury, SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues, Computers & Security, Volume 125, 2023, 103028, ISSN 0167-4048, DOI: https://doi.org/10.1016/j.cose.2022.103028 https://www.sciencedirect.com/science/article/pii/S0167404822004205.

[61] *Energy sector faces 39% of critical infrastructure attacks,* Security, available at https://www.securitymagazine.com/articles/99915-energy-sector-faces-39-of-critical-infrastructure-attacks.

4. National approaches to reducing terrorist-related risks to CEI: stakeholders' roles and good practices

Most countries have provided protection measures for their energy facilities, gradually adopting national strategies, regulations, and instructions covering both the national energy sector and certain subsectors.

4.1. Legal framework: National security framework, national legislation/regulation, requirements and standards in CEI protection

4.1.1. CEI protection in a national security framework

Over the last decade, many Member States have shifted their focus from primarily protecting critical entities to prioritizing their resilience. This approach aims to enhance the ability to mitigate the impact and duration of disruptive events from both physical and ICT domains. The emphasis has moved away from solely preventing attacks to focusing on the rapid restoration of operations, recognizing that achieving 100 percent security cannot be guaranteed.

According to the *Handbook for Implementing the Principles for Resilient Infrastructure* published by the United Nations Office on Disaster Risk Reduction (UNDRR), "Infrastructure resilience is the timely and efficient prevention, absorption, recovery, adaptation and transformation of national infrastructure's essential structures and functions, which have been exposed to current and potential future hazards".[62] Implementing resilience across all disruption phases should be done through collaborative risk and uncertainty management, multi-hazard assessment and methods that embrace the systemic nature of national infrastructure.

In practical terms, this means that CEI protection should involve pre-crisis measures that focus on robustness and the ability to withstand or resist stress. It also recognizes that disruptions to CI are sometimes inevitable and cannot be entirely avoided. Therefore, enhancing absorptive and adaptive capabilities, such as implementing redundancy and developing effective recovery strategies, is essential.[63]

62 *Handbook for Implementing the Principles for Resilient Infrastructure*, UNDRR, 2023, available at https://www.undrr.org/media/87213.

63 Christer Pursiainena, Eero Kytömaa, *From European critical infrastructure protection to the resilience of European critical entities: what does it mean?* Sustainable and Resilient Infrastructure, 2023, VOL. 8, Pages 85–101, https://doi.org/10.1080/23789689.2022.2128562 at: https://www.tandfonline.com/doi/epdf/10.1080/23789689.2022.2128562?needAccess=true.

4.1.2. CEI protection as a part of national security policy

Defining a set of measures aimed at protecting CEI against terrorist acts is a priority for most government authorities, especially special services and law enforcement agencies, as well as private stakeholders. The nexus between national security and CI protection is vital to the progress of any society, the protection of the right to life and its proper social and economic functioning.

At the same time, national approaches to prioritizing and coordinating protection measures can vary significantly. Authorities may decide whether to include protection of CEI in their national strategy, highlighting its vital role in national security, or develop a specific counter-terrorism strategy that includes energy sector protection among other sectors. Alternatively, the protection of CEI might be addressed within broader CIP policies.

In some countries, CEI protection may be covered by multiple documents, depending on the role and significance of the energy sector in the country's social and economic life. For example, in a:

- National security strategy and its priorities (see 4.1.3)
- Counter-terrorism strategy (see 4.1.4)
- CIP strategy (see 4.1.5)

4.1.3. CEI protection among national security priorities

Both the United Nations Security Council and the General Assembly have stated that any measures taken to prevent and combat terrorism must comply with Member States obligations under international law, in particular international human rights law, international refugee law and international humanitarian law, and have underscored that respect for human rights, fundamental freedoms and the rule of law are complementary and mutually reinforcing with effective counter-terrorism measures.[64] Consequently, any measures aimed at protecting CI against terrorist acts should be designed and implemented in line with international human rights law, international refugee law and international humanitarian law

As noted earlier, some Member States include the protection of CEI among their national security priorities to facilitate concerted and coordinated efforts. While this is not the primary method for organizing CEI protection at present, it is still employed by several countries, for example, Azerbaijan,[65] Brazil,[66] the Czech Republic,[67] and Russia[68] among other countries.

64 Global Counter-Terrorism Strategy (A/RES/77/298).
65 Azerbaijan National Security Strategy, available at: https://www.migration.gov.az/content/pdf/b5f3b29fd98276567dd7f0fd0ff2a58b.pdf.
66 Política Nacional de Defesa, available at: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf.
67 Security strategy of the Czech Republic, 2023, available at: https://mzv.gov.cz/file/5119429/MZV_BS_A4_brochure_WEB_ENG.pdf.
68 National Security Strategy of the Russian Federation, 2024, available at: http://www.kremlin.ru/acts/bank/47046.

- The increasing interdependence between CI sectors, coupled with the potential of cascading effects in the event of accidents or attacks, requires a broad approach to effectively coordinate prevention, response and recovery actions across sectors. This approach helps systematize and coordinate inter-agency efforts and avoid duplication of functions. A robust national security framework for CEI protection should:
    - Define the state bodies responsible for regulating CEI protection activities, including coordinating partnership with private sector.
    - Establish measurable strategic objectives, national programmes and timelines for achieving these goals.
    - Provide a foundation for effective prevention and incident management through the harmonization of tasks across different security policy areas.

At the same time, developing a sound national security framework does not necessarily reduce the need for energy sector-specific protection measures, especially if these measures have proven successful or align with binding international regulatory frameworks. Given the ongoing terrorist threats to CEI, it is essential to adopt a strategic approach that builds capacity and anticipates significant increases in both the volume and diversity of threats.

Case Study 1

Brazil national defense framework of CEI protection

The updated National Defense Policy and National Defense Strategy of Brazil includes as a national objective to protect strategic infrastructures, including energy facilities.[69]

According to these documents the first national defense objective is to "Guarantee sovereignty, heritage national and territorial integrity", which includes the necessity to secure among others the following sectors of Brazil's economy:

- Generation and distribution of electrical energy.
- Production and distribution of fuels.

Moreover, the eighth national defense objective, "Increase Brazil's influence at the concert nations and integration in international decision-making processes", also includes, as a secondary goal, the protection of the aforementioned sectors as part of national capacity-building efforts.

Source: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf.

4.1.4. Protecting CEI in a counter-terrorism policy framework

The inclusion of CEI protection in a counter-terrorism policy framework is more common than in a national security framework. National counter-terrorism strategies that include CEI protection as one of their priorities often establish a broad framework for preventing the commission of terrorist offenses and provide synergies

[69] Política Nacional de Defesa, available at: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf.

between intelligence and law enforcement agencies, but rarely define energy-sector specific counter-terrorism measures to address the particularities of the sector.

Case Study 2

Ghana's National Framework for Preventing and Countering Violent Extremism and Terrorism (NAFPCVET)

The document is based on a holistic approach and provides definitions of CIs, including energy facilities.

As part of Ghana's National counter-terrorism framework, critical energy facilities protection requires a well-defined, inter-agency approach for preventing and combating terrorist threats. The framework places greater focus on ensuring systematic co-ordination across ministries, departments and agencies and civil society organizations (CSO).

NAFPCVET clearly identifies state ministries and national agencies of Ghana that need to be involved in CEI protection and the types of national documents to be produced.

The protection of coastal oil facilities against terrorist attacks is a vivid example of inter-agency collaboration. While Ghana's Ministry of Energy is responsible for securing the nation's oil production, petroleum supplies and the distribution of oil and gas assets, maritime security agencies such as the Ghana Maritime Authority (GMA), the Ghana Navy and other maritime security organizations must also be closely involved when critical oil and gas infrastructure falls within the maritime security domain. Moreover, the document mentions the importance of putting "in place a maritime security strategy to ensure adequate safeguarding of these (energy) national assets".[70]

Source: Ghana's National Framework for Preventing and Countering Terrorism and Violent Extremism, 29 January 2020, available at: https://www.peacecouncil.gov.gh/storage/2019/09/NAFPCVET-Document-29-Jan-2020.pdf.

4.1.5. CEI protection through specialized CIP policies

- The most common option for institutionalizing energy infrastructure protection is through specialized CIP policies. According to recent research, the sector that countries worldwide most frequently mention in their CIP strategies is the energy sector (96%).[71]
- CEI protection can be an integral part of a state's CIP strategy or policy. Such a strategy or policy should:
    - Outline a methodology for identifying specific energy sector facilities as critical.
    - Describe additional regulations tailored to the unique features of the energy sector, such as special information-sharing standards or security provision requirements.
    - Ensure high-quality emergency response and recovery plans for both existing and newly constructed facilities.

[70] Ghana's *National Framework for Preventing and Countering Terrorism and Violent Extremism*, 29 January 2020, available at: https://www.peacecouncil.gov.gh/storage/2019/09/NAFPCVET-Document-29-Jan-2020.pdf.

[71] Valentin Weber, Maria Pericàs Riera, Emma Laumann, *Mapping the World's Critical Infrastructure Sectors*, 2023, available at: https://dgap.org/en/research/publications/mapping-worlds-critical-infrastructure-sectors.

4.1.6. Defining CEI stakeholders

To ensure an inclusive approach and stakeholder engagement in CEI protection, Member States need to adopt clear rules for defining and categorizing stakeholders who share the responsibility to protect CEI from terrorist attacks.

Table 4
Stakeholder roles in CEI protection policy

Government	Government refers to public sector policymakers who develop and initiate changes to the national strategy/policy of CEI protection, elaborate legal frameworks on CEI protection at the national level and allocate necessary funding for counter-terrorism activities.
Energy sector regulators	Energy sector regulators implement CEI protection policy as defined by government, elaborate requirements for security protocols, risk management, contingency and emergency planning and instructions on counter-terrorism measures to be implemented on energy facilities. Usually, regulators define the criteria for classifying energy facilities as critical.
CEI owners	Energy infrastructure owners adopt and raise protection standards, elaborate facility-specific counter-terrorism plans and request CEI operators to assess potential terrorist threats.
CEI contractors	Contractors are required to conduct their work in agreement with national standards and regulations. They develop and implement tools to comply with energy sector regulators security requirements and standards.
CEI operators	CEI operators manage, maintain and recover infrastructure according to the standards, codes and regulations agreed by government and energy sector regulators using the technologies and solutions provided by contractors. Operators collect data on threats and vulnerabilities to improve risk management. In terms of PPPs, owners and operators share their knowledge and experiences protecting energy facilities.

It is important to acknowledge the role of civil society, including trade unions, local communities and expert and scholarly organizations, in addressing security issues in the energy sector. While civil society organizations may not have the same level of responsibility as other stakeholders, they can contribute to public decision-making at both state and operational levels. They represent the interests and values of their members on ethical, cultural and religious issues and can develop responsible practices that enhance the protection of energy infrastructure.

4.1.7. Criteria for classifying certain energy facilities as critical

Another important issue concerns the criteria for classifying certain energy facilities as critical, as this entails implementing additional security measures to them. Member States use different criteria to define their CEI. In many cases, national definitions include one or both of the following elements: they highlight the purpose

of the energy infrastructure, linking its criticality to the performance of essential social and economic functions, and they emphasize the effects of disruption or destruction, describing criticality in terms of the estimated consequences of service interruption.

Table 5

National approaches to defining CEI/facilities

Argentina[72]	CEI includes dams, substations, electrical fluid lines, fuel storage plants, oil pipelines, gas pipelines.
Belgium[73]	The Energy sector includes the following sub-sectors of CI: 1. Electricity, consisting of infrastructure and installations enabling the production and transport of electricity, with a view to supplying electricity. 2. Petroleum, composed of petroleum production, refining, processing, storage and transportation by pipelines. 3. Gas, composed of gas production, refining, processing, storage, transportation by gas pipelines and terminals liquefied natural gas.
Brazil[74]	CEI consists of facilities that provide: • Generation and distribution of electrical energy • Production and distribution of fuels • Nuclear energy generation
Croatia[75]	Energy sector CI consists of production, including reservoirs and dams, transmission, storage, transport of energy and energy distribution systems
Czech Republic[76]	Czech CEI includes: • Electricity production facility • Electricity transmission system • Electricity distribution system • Gas transmission system (a high-pressure transit gas pipeline with a nominal diameter of at least 700 mm or a high-pressure national gas pipeline with a nominal diameter equal to 700 mm or smaller and a compressor station or a transfer station) • Gas distribution system (a high or medium pressure gas pipeline and a transfer and regulating station) • Gas storage (an underground gas storage tank with capacity of at least 50 million m3 of gas) • Oil and oil (petroleum) products transmission ○ Transit oil pipeline with a nominal diameter of at least 500 mm, including entry points

72 Subsecretaría de protección civil y abordaje integral de emergencias y catástrofes (1/2015), available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242082/norma.htm.

73 Act of 1 July 2011 on the security and protection of critical infrastructure, available at https://crisiscentrum.be/sites/default/files/documents/files/2021-03/PDFsam_15_2.pdf.

74 Estratégia Nacional de Defesa, available at: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf.

75 *Zakon o kritičnim infrastrukturama* NN 56/13, 114/22, 2022, available at https://www.zakon.hr/z/591/Zakon-o-kritičnim-infrastrukturama.

76 Czech Governmental Order No 432/20,10 Coll of 22 December 2010 on the Criteria for the Identification of a Critical Infrastructure Element, available at: https://www.govcert.cz/download/kii-vis/preklady/Order_432_2010_EN_v1.0_final.pdf.

	○ National oil pipeline with a nominal diameter of at least 200 mm, including entry points ○ Pumping station ○ Terminal equipment for oil transmission ○ The beginning and the end of oil pipeline doubling and branches – a pig launcher • Oil and oil (petroleum) products distribution system (a pipeline with a nominal diameter of at least 200 mm and a pumping station). • Oil and fuel storage and production (a storage facility or a set of storage facilities with capacity of at least 40,000 m3 and a refinery with capacity for atmospheric distillation of at least 500,000 tons per year). • Technical control centres in the energy sector are also defined as CI.
Germany[77]	Critical energy sector include: • Electricity supply: generation, transmission, distribution and trading • Gas supply: extraction, transport, distribution and trading • Fuel/heating oil supply: extraction, production, transport, distribution • District heating supply: generation and distribution
Ghana[78]	CEI includes jetties, storage tanks, refineries, LNG facility, hub transmission infrastructure, power plant, petrochemical plant, lube blending plant and transmission and storage infrastructure for land-locked countries
Kazakhstan[79]	Strategically important economic sectors facilities vulnerable to terrorism include energy facilities that meet the following criteria: • Gas distribution stations providing commercial gas to organizations engaged in the production of thermal energy and meeting the criteria of this subclause. • Energy-producing organizations producing electric (over 50 MW) and (or) thermal energy, boiler houses producing thermal energy in the centralized heat supply zone (over 100 Gcal) (state district power plant, hydroelectric power station, gas thermal power plant, thermal power plant and boiler houses). • Facilities where oil and (or) gas are processed, oil and (or) gas are stored in tanks, uranium is mined and processed. • Facilities operating in the chemical industry.
Romania[80]	The CI subsectors of the energy sector are: • Electricity, including nuclear-electric capacities and facilities for production, storage/ storage, distribution and transport networks. • Petroleum and petroleum derivatives: capacities and facilities for extraction/production, refining, treatment, storage / storage, distribution and transport via pipelines, terminals. • Natural gas and natural gas derivatives: capacities and facilities for extraction/production, refining, treatment, storage / storage, distribution and transport via pipelines, terminals. • Mineral resources.

77 KRITIS-Sektor definition Energie, https://www.openkritis.de/it-sicherheitsgesetz/sektor_energie.html.
78 Strategic Environmental Assessment on the Development of a Petroleum Hub in Ghana.
79 Resolution of the Government of Kazakhstan "on approval of the Rules and criteria for classifying objects as vulnerable to terrorism".
80 Order of the Minister of Economy, Commerce and Business Environment no. 1.178 of 6 June 2011 https://cncpic.mai.gov.ro/en/sectoare/energetic.

Russia[81]	CEI consists of energy sector facilities, whose disruption or cessation of functioning would lead to the loss of control of the economy of the Russian Federation, a subject of the Russian Federation or an administrative-territorial unit, an irreversible negative alteration (destruction) or a significant decrease in the safety or life of the population.
Slovenia[82]	Impairment of the energy system on the territory of the Republic of Slovenia which: • Takes more than seven days to rehabilitate. • A disruption of electricity supply for three days for over 100.000 people. • Interruption in the supply of petroleum products and natural gas for more than a week involving more than 100,000 people and costs of 10,000,000 euros per day.
Slovakia[83]	Critical energy facilities include nuclear power generation, electricity transmission, transportation and distribution of natural gas, transportation and processing of oil, heat generation and extraction of important raw materials.
Türkiye [84]	The entirety of the energy network, assets, systems and structures whose failure to fulfil their functions, in whole or in part, would adversely affect the sustainability of social order or the provision of public services.
UK[85]	National assets that are essential for the functioning of society, such as those associated with energy supply. The energy supply sector is made up of upstream oil and gas, downstream oil and gas and electricity.
USA[86]	Energy infrastructure includes electric power systems, natural gas and liquid fuels systems as they relate to the generation, transmission and distribution of electric power and emergency and standby power systems. Pipelines that transport natural gas and liquid fuels are discussed as part of transportation infrastructure because the engineering standards for pipeline safety and design are administered by the Pipeline and Hazardous Materials Safety Administration. A "critical" part of energy infrastructure means a system or asset of the bulk-power system (physical or virtual), the incapacity or destruction of which would negatively affect: • National security • Economic security • Public health or safety, or any combination of such matters.
Japan[87]	Energy sector of CI include: • Electric power supply services • Gas supply services • Petroleum industries

81 Federal law of the Russian Federation № 256 from 26 July 2011 "On security of energy infrastructure", available at: https://base.garant.ru/12188188/.
82 Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastructure državnega pomena v Republiki Sloveniji, 2012.
83 Slovak Act No. 45/2011 Coll. on critical infrastructure, available at: https://www.aspi.sk/products/lawText/1/73766/1/2.
84 Enerji sektöründe kullanilan endüstriyel kontrol sistemlerinde bilişim güvenliği yönetmeliği, 2017, available at: https://www.resmigazete.gov.tr/eskiler/2017/07/20170713-5.htm.
85 UK's Sector Security and Resilience Plans.
86 *Community Resilience Planning Guide for Buildings and Infrastructure System*, available at: https://crsreports.congress.gov/product/pdf/R/R47666.
87 Available at https://sg.nec.com/en_SG/pdf/brochures/PublicSafety/SocialValueCreationReport_en_Vol.1.pdf.

Case Study 3

Criteria for classifying energy facilities as critical in the Russian Federation

The Russian Ministry of Energy uses both qualitive and quantitative indicators to classify energy infrastructure facilities as critical. Additionally, energy facilities could be identified as critical at the federal (national), regional and administrative levels.

		Qualitative indicators	Quantitative indicators
1.	**Federal level**	Disruption of operations at these facilities would lead to economic instability or disruption of essential economic activity in two or more regions of the Russian Federation, potentially causing irreversible negative consequences or destruction.	Facilities where an incident could result in over 500 casualties (killed and/or injured).
		Disruption or suspension of operations at these facilities would lead to a decline in security in two or more regions of the Russian Federation.	Facilities where an emergency can cause environmental damage and material losses exceeding 1.2 billion roubles.
2.	**Regional level**	Disruption of operations at these facilities would lead to economic instability or disruption of essential economic activity within a region of the Russian Federation, potentially causing irreversible negative consequences or destruction.	Facilities where an incident could result in over 50 but does not exceed 500 casualties (killed and/or injured).
		Disruption or suspension of operations at these facilities would lead to a decline in security within a region of the Russian Federation.	Facilities where an emergency can cause environmental damage and material losses exceeding 12 million roubles, and up to 1.2 billion roubles.
3.	**Administrative (county) level**	Disruption or suspension of operations at these facilities would lead to the loss of economic control within an administrative centre (or county) of the Russian Federation and its irreversible impairment or destruction	Facilities where an incident could result in less than 50 casualties (killed and/or injured).
		Disruption or suspension of operations at these facilities would lead to a decline in security within an administrative centre (county) of the Russian Federation.	Facilities where an emergency could cause material losses of less than 12 million roubles, and where this emergency could not be classified as a local emergency.

Source: Decree of the Ministry of Energy of the Russian Federation No. 957, 15 September 2022, available at https://minjust.consultant.ru/files/33257.

Case Study 4

CEI stakeholders in Türkiye

According to Türkiye's State Law No. 4628, the regulators of CEI are:

- Electricity Market Department
- Natural Gas Market Department
- Petroleum Market Department
- Liquefied Petroleum Gases Market Department
- Tariffs Department
- Audit Department
- Expropriation Department
- Legal Department
- Information Technology Department
- Strategy Development Department
- Human Resources and Support Services Department
- Office of Press and Public Relations Counsellor
- Special Bureau for the Board
- Special Bureau for the President

The following organizations are defined as "Responsible Companies" (or CEI owners) and are considered responsible for CEI:

- Electricity transmission license holders.
- Electricity distribution licence holders.
- Electricity generation facility owners that have temporary acceptance and installed power of 100 MW or more.
- Natural gas transmission licence holders who undertake transmission via pipeline.
- Natural gas distribution licence holders who are obliged to establish a shipping control centre.
- Natural gas storage licence holders (LNG, underground storage).
- Crude oil transmission licence holders.
- Refinery licence holders.

Among other duties, these Responsible Companies are obliged to:

- Prepare a risk inventory to monitor the information process and ensure safety of industrial control systems used in CEI.
- Prepare a treatment plan clearly outlining risk mitigation actions.
- Provide the regulator with a system recognition form, outlining related processes, as well as work which has been performed for information security and source information.

Source: The Regulation on Information Security of Industrial Systems Used in the Energy Sector, 13 July 2017, available at https://www.resmigazete.gov.tr/eskiler/2017/07/20170713-5.htm.

4.1.8. Standards, protocols and regulations in the sphere of CEI protection. Examples of standard operating procedures around the world

Operators of complex tech-intensive energy facilities such as pipelines, refineries and storage tanks are obliged to develop and follow security protocols and specific rules in accordance with national and international legislation. General security requirements for energy facilities are usually developed by legislative bodies at the national level and take the form of national laws.

These laws should align with international requirements and guidelines relevant to that specific type of facility. For example, port LNG terminals protocols need to comply strictly with the requirements of the International Convention for the Safety of Life at Sea (IMO SOLAS)[88] and the International Ship and Port Facility Security Code (ISPS),[89] as well as measures to enhance maritime security and national requirements.

Many Member States elaborate requirements (standards) for the design, construction, operation and maintenance of different types of energy infrastructure to ensure a high level of security. Compliance with standards helps mitigate risks and contributes to the proper operation of energy infrastructure. For instance, in the USA where CEI connects or runs through a building, building codes and standards may apply to some components of infrastructure. For example, electrical facilities must follow building codes and standards, because these components are often part of the building structure.[90]

Since 2019, the People's Republic of China's Ministry of Public Security has standardized preventive measures for energy facilities protection and issued 12 industry-specific counter-terrorism security standards related to energy infrastructure that regulate oil and gas fields, refining and chemical industries, petroleum product and natural gas sales, engineering services, transport and oil and gas pipeline enterprises, as well as power grids, thermal power, hydropower, wind power, solar power and other enterprises.[91]

In many cases, security protocols and standards for CEI include:

- A methodology for determining the risk category of the facility, such as categorization rules. This procedure involves differentiating safety requirements for specific facilities based on the degree of potential hazards and the possible consequences of illegal acts or interventions.
- Rules and structure for the facility's security plan, which assist in developing security measures.
- A list of required equipment, both physical and informational, along with the appropriate financial resources to be allocated in the facility's budget.
- Criteria for security incidents that must be reported to the responsible national agency.

88 Available at International Convention for the Safety of Life at Sea (SOLAS), 1974.
89 Available at The International Ship and Port Facility (ISPS) Code.
90 *Infrastructure Codes, Standards, and Regulations: Frequently Asked Questions*, 2023, available at: https://sgp.fas.org/crs/misc/R47666.pdf.
91 As reported by the Shanghai Cooperation Organization Regional Anti-Terrorist Structure.

- Unique security requirements for each type of facility, if necessary. For example, elements of an energy facility, such as well pads in exploration, may require different protection measures compared to midstream transmission pipelines due to differences in location, dispersion and accessibility.

At the same time, imposing regulatory performance standards often fails to address inherent problems due to slow-moving bureaucratic processes. Traditional regulatory models are viewed by industrial experts as the antithesis of the innovation seen in the private sector and among those who build, operate and use ICT infrastructure.[92]

In many Member States security protocols are imposed not only on energy facilities but also on surrounding areas, defined as "security area/zone". Special rules typically apply to transportation and individuals entering or moving within these zones.

Case Study 5

Safety zones around critical oil facilities in Tanzania

According to paragraph 203 of the Tanzania Petroleum Act (2015), the Tanzanian Petroleum Upstream Regulatory Authority (PURA) is responsible for regulating security zones around critical oil facilities. Security zones can also be established before siting facilities or around abandoned or dumped facilities.

Oil facility operators are obliged to create such zones under PURA control. PURA determines the extent of these zones near oil storages, plants, refineries and pipelines and establishes additional security requirements for them such as rules of authorization of persons and transit accessibility. In case of accidents and emergencies, these security zones can be widened and the screening measures strengthened.

If security zones cross international borders, PURA must consult the Tanzanian Ministry of Energy.

Source: https://www.ewura.go.tz/wp-content/uploads/2020/04/The-Petroleum-Act-2015-1.pdf.

92 Melkunaite, Laura & Giroux, Jennifer. (2013). *Information Sharing for Critical Energy Infrastructure Protection: Finding value & overcoming challenges.* NATO Energy Security Centre of Excellence. URL: https://www.researchgate.net/publication/281584950_Information_Sharing_for_Critical_Energy_Infrastructure_Protection_Finding_value_overcoming_challenges.

Tool 1

Security certificate ("security passport") for critical energy facilities as a part of risk management in Azerbaijan, Kazakhstan and the Russian Federation

The "security passport" of energy infrastructure usually reflects the characteristics of the facilities, possible socioeconomic repercussions of unlawful interference (such as a terrorist attack), the category of the facility, the state of its physical protection system and fire safety. Moreover, the security passport of the critical energy facility contains measures to ensure security and counter-terrorism protection based on its specifics, location and scale.

In the Republic of Azerbaijan, the Facility Security Passport is the main document reflecting the data that satisfies the security criteria of the facility.[93] The owner or operator of the facility must submit a security declaration for approval by the competent executive authorities. Approval of the security declaration of the facility serves as a basis for the inclusion of the facility into the State Register.

In the Republic of Kazakhstan, the Facility Security Passport is an instrument for enhancing counter-terrorism security in facilities vulnerable to such threats.[94] It involves measures to prevent terrorist attacks according to the type of energy facility.

In the Russian Federation, the Security Passport of critical energy facilities is based on a two-pronged assessment: facility categorization derived from a risk evaluation and the sufficiency of implemented security measures. This encompasses engineering and technical controls, physical protection protocols and counter-terrorism measures, all aligned with government-mandated security requirements.[95]

Tool 2

CEI information

Critical energy infrastructure information (CEII) encompasses specific engineering, vulnerability or detailed design information about proposed or existing CI (physical or virtual) that:

- Relates to the production, generation, transmission or distribution of energy.
- Could be useful to a person planning an attack on CEI.
- Provides strategic information beyond the location of the CEI.

Typically, CEI regulators establish special rules and standards for handling sensitive information known as CEII. CEII operators can mitigate physical and information security risks by sharing vulnerability, threat, location or design information with government and industry. This information is important for energy planning and emergency response. However, there can also be exemptions. For example, in the USA, to prevent public disclosure of CEII, there is an exemption from mandatory disclosure under the Freedom of Information Act.[96]

93 Правовое обеспечение безопасности объектов топливно-энергетического комплекса: опыт СНГ, 2022, available at: https://gubkin.ru/faculty/faculty-of-complex-safety-of-the-fuel-and-energy-complex/kafedry-i-podrazdeleniya/knb/files/metod_materialy/prav_obespech_obj_tek.pdf.

94 Об утверждении типового паспорта антитеррористической защищенности объектов, уязвимых в террористическом отношении, 2023, available at https://adilet.zan.kz/rus/docs/V2300032950.

95 Framework on Security Passport of Critically Important Facilities Elaboration in the Russian Federation №2034, 10 November 2022, available at: https://base.garant.ru/405693779/.

96 Source: US Federal Energy Regulatory Commission: https://www.ferc.gov/ceii.

4.1.9. Taking into account human rights aspects in CEI protection

Terrorist attacks on CEI have a profound and direct impact on human rights. Considering the potential impact on populations, and given the roles such infrastructure plays in maintaining or delivering vital societal functions, attacks on CEI can result in devastating consequences for a wide range of human rights, including the enjoyment of the right to life (Article 3 of the Universal Declaration of Human Rights, and article 6 of the ICCPR), the security of person, the right to health and a healthy environment, the right to education, as well as other aspects of the right to an adequate standard of living.

The proper functioning of CEI is vital for delivering adequate services to populations and for promoting and protecting their human rights, as its disruption by a terrorist attack could cause catastrophic damage to local communities. For example, this can include large-scale injury, deaths and forced displacement, all of which negatively impact the right to health (Article 12 of the International Covenant on Economic, Social and Cultural Rights) and other human rights. Similarly, the disruption or destruction of oil and gas infrastructure can also have severe environmental impacts on communities, including water, air and other forms of pollution. Finally, it is important to recognize the differential impact of both terrorism and counter-terrorism measures on various segments of populations, namely women and girls, and men and boys.[97]

Furthermore, such attacks can destabilize governments, undermine civil society, jeopardize peace and security and threaten social and economic development, all of which significantly affect the enjoyment of human rights.

States' duty to safeguard human rights implies the obligation to take necessary and adequate measures to prevent, combat, and punish activities that endanger the rights of the persons within their jurisdiction, including terrorism. Respect for human rights and international law should therefore form the foundation of developing legal frameworks and policies to counter terrorist threats to CEI. According to Pillar IV of the United Nations Global Counter-Terrorism Strategy, measures to combat terrorism must comply with international law, in particular international human rights law, international humanitarian law and refugee law. Member States should be guided, among others, by the United Nations Global Counter-Terrorisms Strategy (GCTS) so as to ensure that respect for human rights is not competing but complementary and mutually reinforcing goals to combatting terrorism, while also taking into account gender and age dimensions.

The development and improvement of measures to ensure the protection of CEI against terrorist acts should not be achieved at the expense of excessively restricting individuals' rights or deteriorating working conditions. In the event of a terrorist attack against CI that reaches the level of a public emergency which threatens the life of the nation and existence of which was officially proclaimed, States may take measures releasing them from their obligations under international human rights law to the extent strictly required by

[97] See UN Women 2023 Report on Energy.

the demands of the situation and subject to certain conditions.[98] Adequate safeguards should be in place, including oversight to prevent abuse, and derogation measures should be lifted once a state of normalcy has been restored, in view of their exceptional and temporary nature. Outside of such public emergency situations, States can limit the exercise of certain rights provided that those limitations comply with the principles of legality, necessity, proportionality and non-discrimination. Member States are encouraged to conduct regular human rights impact assessments of measures taken in response to terrorist acts against CI in order to contribute to such measures being evidence-based and proportionate.

4.2. Institutional framework/mechanisms in countering terrorist threats to CEI

A prerequisite for effective coordination of CIP and to avoid duplication of functions is to ensure inclusive participation of all stakeholders, including both state and non-state actors. The latter include, in particular, private security companies, which usually directly protect sensitive infrastructure.

4.2.1. Whole-of-government (multi-agency) approach to CEI protection

Protecting CEI inevitably involves the participation of multiple government bodies and agencies across different levels of the administration, from national to local. The coordination of these efforts is thus fundamental and is typically outlined in the country's national security strategy or counter-terrorism policy.

The absence of coordination mechanisms can create significant challenges. For instance, multiple security agencies within a country often collect and analyze terrorism-related intelligence to assess threats to CEI. While this can foster positive competition and complementarity, it can also lead to duplication and fragmentation of efforts if there is no clear response framework. Furthermore, the lack of standardized procedures and differences in terminology can obstruct the ability to gain a comprehensive understanding and implement effective measures.

As the *OSCE Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection* indicates, public authorities can have different approaches to coordination. While some authorities "adhere to the power of market forces...others are strong believers in the government's legislative role". These differences can become a serious challenge, including when engaging with private sector stakeholders.[99]

A consistent whole-of-government (multi-agency) approach to CEI protection has proven to be a good practice, strengthening effective inter-agency coordination at the national level. This approach should also

[98] The International Covenant on Civil and Political Rights (adopted on 16 December 1966, entry into force 23 March 1976) stipulates in its article 4: "1. In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin. 2. No derogation from articles 6, 7, 8 (paragraphs I and 2), 11, 15, 16 and 18 may be made under this provision. 3. Any State Party to the present Covenant availing itself of the right of derogation shall immediately inform the other States Parties to the present Covenant, through the intermediary of the Secretary General of the United Nations, of the provisions from which it has derogated and of the reasons by which it was actuated. A further communication shall be ss, through the same intermediary, on the date on which it terminates such derogation".

[99] OSCE Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, Vienna, 2013, available at: www.osce.org/atu/103500?download=true.

prioritize effective coordination among all stakeholders, including ministries (such as those responsible for the energy sector, security, interior and defense), regional bodies and regulators collaborating at the strategic, tactical and operational levels.

4.2.2. Forms of inter-agency coordination to strengthen and maintain secure CEI

Some modalities of inter-agency coordination to strengthen and maintain secure CEI include:

- Horizontal coordination: Collaboration between agencies at the same level. For example, the ministries of transport and energy could jointly undertake CEI risk assessments as part of their horizontal collaboration.
- Vertical coordination: Interaction between different levels of government. For instance, a national-level security agency may issue general guidelines on CEI protection to local-level authorities. These guidelines would then serve as a basis for each authority to develop more specific security standards for their facilities.

To facilitate coordination between agencies involved in CEI protection, many Member States legally establish special governance mechanisms that allow government entities, energy infrastructure operators, and local authorities to share information. These mechanisms often include a combination of policy tools, ranging from regulation to incentive mechanisms, to support the implementation of measures protecting energy infrastructure against terrorism.

Case Study 6

Turkmenistan's inter-agency coordination approach to protect natural gas infrastructure against terrorist attacks

The Ministry of Internal Affairs of Turkmenistan, together with the Ministry of Defense and other relevant departments, is responsible for the protection of critical energy facilities, as well as operational investigative activities to identify and prevent illegal actions aimed at disrupting their functioning. As part of its efforts to protect CEI, the government has declared a principle of integrity for its main pipeline transport systems, as well as for transport systems that will be developed in the future. It also considers close inter-agency cooperation as essential to protect pipelines located in the interior and border regions of Turkmenistan.

Source: https://turkmenistan.gov.tm/ru/post/19819/garantii-nadezhnosti-i-bezopasnosti.

4.2.3. Law enforcement agencies and national security agencies cooperation in the context of energy infrastructure protection

In modern security environments, energy infrastructure protection against terrorist attacks is a complex, multidimensional task that requires the combined efforts of national security and law enforcement agencies. Since these bodies may use different approaches and methods, close collaboration and frequent interaction

are fundamental. The national legal framework should also enable these agencies to share relevant intelligence and information while respecting international law, including international human rights law.

Collaborative partnerships between law enforcement and national security agencies could be based on common tasks, clearly identified functions and a mutual commitment to provide necessary resources. This coordination could include:

- Joint and mutually reinforcing strategic and operational planning
- Joint risk and threat assessments
- Periodic information-sharing sessions
- Creating an institutional platform to exchange information in cases of emergency
- Joint exercises
- Joint operations, e.g., multi-agency surveillance

4.2.3.1. Inter-agency information-sharing

A well-established communication system often helps relevant agencies gain new perspectives on the terrorist threat to energy facilities. The information shared can be either situational (information about a specific event, facts) or analytical (assessments, forecasts, experience analysis) and, in the case of CEI, usually addresses three levels:[100]

- Strategic planning and investment to inform effective risk management decisions
- Situational awareness, for both routine operations and during crisis or incidents, including suspicious activity reporting, incident analysis and recommended protective actions
- Operational and tactical planning and execution

In this context, building the capacities of relevant agencies to adequately share information and take action based on that information is key. For example, in some Member States, counter-terrorism centres or specialized security bodies organize workshops where specialists from different ministries and agencies present good practices on how to share analytical information and specificities related to CEI protection—e.g., how to equip energy facilities with engineering and technical means and security systems; how to organize physical security, inspection techniques for visitors, vehicles and luggage; specific terrorist threats (organizational structure, modus operandi, tactics, etc.); how to respond to fire hazards, toxic and dangerous substances, measures to prevent and respond to emergency situations; how to identify explosive devices and how to respond (classification, procedures, security measures, etc.).

[100] Melkunaite L., Giroux J. (2013) *Information Sharing for Critical Energy Infrastructure Protection: Finding value & overcoming challenges*, available at: https://www.researchgate.net/publication/281584950_Information_Sharing_for_Critical_Energy_Infrastructure_Protection_Finding_value_overcoming_challenges.

Considering gender and age sensitivities in the planning, collection, analysis and dissemination of intelligence products provides another way of supporting identification of signs of instability that may have been overlooked and enables the development of a comprehensive grasp of social context and dynamics. This, in turn, helps to anticipate potential adverse consequences of intelligence collection and dissemination to the civil, political and human rights of those persons affected.

4.2.4. Institutional architecture to coordinate CEI protection

To ensure accountability, good practices highlight the importance of designating adequately resourced ministries or departments to coordinate CEI protection. In many countries, this typically involves a specialized unit within the Ministry of Interior, specialized teams within the Armed Forces or a dedicated agency for countering terrorist threats against CEI.

Case Study 7

Georgia, Strategic Pipelines Protection Department of the Ministry of Internal Affairs Georgia (SPPD)

SPPD is part of the Ministry of Internal Affairs of Georgia, tasked with protecting the Supsa Terminal, Baku-Tbilisi-Ceyhan oil pipeline and the Baku-Tbilisi-Erzurum South Caucasus gas pipeline, along with related infrastructure. The SPPD's functions include:

- Ensuring protection and security: Safeguarding the Supsa Terminal, Baku-Tbilisi-Ceyhan oil pipeline and Baku-Tbilisi-Erzurum South Caucasus gas pipeline, along with related infrastructure, through the implementation of comprehensive measures.
- Risk assessment and intelligence gathering: Evaluating risks, collecting and analyzing information related to the security of the protected facilities and providing relevant intelligence services.
- Enforcement measures: Coordinating and cooperating with other agencies to take appropriate actions against offenders to ensure the security of the protected facilities.
- Additional responsibilities: Carrying out other functions and tasks as defined by the "Law of Georgia on Police" and other relevant norms.

Source: https://police.ge/en/ministry/structure-and-offices/strategiuli-milsadenebis-datsvis-departamenti?sub=9658.

Case Study 8

Oil Police in Iraq

The Oil Police is a special security body established to protect CEI in Iraq in 2007. The Oil Police is part of the Ministry of Oil and serves to guard Iraq's oil fields mainly in Basra and Southern Iraq, encompassing 4,300 miles of gas and oil pipelines. The Oil Police forces are well-equipped and include mobile motorized units that are deployed around oil fields and power plants in Salaheddine and Kirkuk, as well as the al-Qayyarah and Najma oilfields near the city of Mosul.[101]

The Iraqi Oil Police is coordinating its activities with the Iraqi Federal Police and Joint Operations forces, technical groups of the Ministry of Oil and Civil Defense Corps to enforce protective measures.

The responsibilities of the Oil Police include:

- Protecting oil and gas infrastructure from armed attacks and sabotage
- Preventing the smuggling of oil and petroleum products abroad
- Countering other illegal acts, including theft of petroleum products as a result of tapping into an oil pipeline

4.2.5. Public-private cooperation

It is essential to engage all relevant stakeholders when developing policies for CEI protection against terrorist threats because many energy facilities are operated by the private sector. Given that the primary responsibility for safeguarding CEI assets and systems lies with their owners and operators, establishing effective PPPs is crucial for achieving adequate levels of protection.

Additionally, industries and their associated bodies hold invaluable expertise regarding the specific functionalities of CEI facilities. This expertise includes details such as interconnectivity with other infrastructure, inherent vulnerabilities and specific maintenance and repair requirements.

The ownership and operation of CEI can vary based on the legal framework, with potential operators including private companies, public entities or mixed public-private consortiums. Foreign companies may also be involved, especially in transit countries. These entities, due to their ownership or operational roles, are required to conduct thorough risk and threat assessments. These assessments should address both current and emerging threats and align with the security requirements, policies and recommendations set forth by government authorities and relevant industry associations.

Private entities engaged in PPPs must adhere to due diligence procedures as specified by the national legislation of the countries in which they operate.

[101] Understanding the security bureaucracy in Iraq: agencies and their tasks, July 2020, ORSAM Report, available at: https://orsam.org.tr/d_hbanaliz/understanding-the-security-bureaucracy-in-iraq-agencies-and-their-tasks.pdf.

4.2.6. Factors for enhancing PPPs in CEI protection

PPPs can vary widely in form, from informal collaborations to more formal arrangements. The level of formality often reflects the degree of control that public agencies wish to maintain, as well as the legal and cultural context. "Project-oriented" PPPs are often considered more effective than "process-oriented" ones due to clearly defined goals, timelines and budgets.[102]

However, several challenges can hinder the effectiveness of PPPs for CEI protection. These challenges include differences in expectations between the private and public sectors, a lack of trust between the cooperating parties and unclear task allocation. Experts frequently note significant disparities in organizational cultures and bureaucratic processes between public and private entities.

In contrast, good practices emphasize the importance of fostering an inclusive process. This process should involve a multifaceted approach that includes identifying and classifying threats to CEI; establishing robust communication and coordination mechanisms; promoting effective cooperation between public and private stakeholders; implementing agreed-upon protective measures coherently and specifying clear and unambiguous responsibilities for all participants within the PPP framework. By prioritizing these key elements, stakeholders can develop a robust and effective PPP model for CEI protection.

The mechanisms used to develop cooperation between the public and private sectors in CEI protection vary by country. While not an exhaustive list, common elements often include:

- Information-sharing, monitoring and best practices exchange (see 4.2.6.1)
- Joint risk management and coordination in emergency response plans elaboration (see 4.2.6.2)
- Cooperation in security regulations development (see 4.2.6.3)
- Joint training and security exercises (see 4.2.6.4)

4.2.6.1. Information-sharing, monitoring and best practices exchange in PPPs

Information-sharing is one of the most critical aspects of public-private cooperation for CEI protection. A collaborative approach should be encouraged to facilitate the sharing of data, knowledge and expertise among energy infrastructure stakeholders. The UNDRR's *Handbook for Implementing the Principles for Resilient Infrastructure* envisages that "organizations with common interdependencies should be able to share data in a standardized way and generate shared insights into how to handle common threats".[103] Such information exchange fosters a learning environment, allowing stakeholders to gain valuable insights from past security breaches and develop a unified response strategy against prevalent terrorist threats.

[102] Project -oriented PPPs are focused on a well-defined task within the energy infrastructure security framework. These partnerships are time-bound, characterized by urgency and address critical issues such as the development of specific rules of engagement for a particular challenge.

[103] *Handbook for Implementing the Principles for Resilient Infrastructure*, 2020, available at: https://www.undrr.org/media/87213/download?startDownload=20240612.

Empirical observations indicate that effective information-sharing between the public and private sectors in CEI protection relies on three pillars:

- Cultivating trust: Building trust among all stakeholders by leading agencies.
- Implementing safeguards: Ensuring the protection of sensitive information that is either encouraged or mandated for dissemination within CEI protection arrangements.
- Developing a legal framework: Creating an effective legal architecture to facilitate cooperation.

Another reason to strengthen PPPs and establish an appropriate framework of collaboration is that security departments within energy companies often find themselves directly involved in gathering information about potential illicit activities targeting energy facilities, or may be legally required to prepare and share data on security incidents to law enforcement or state security agencies.

Box 5

PPPs on information-sharing for energy infrastructure protection

For many countries, PPPs have become the key tool for creating an information-sharing framework on threats and vulnerabilities affecting national CEI and for coordinating actions between public and private stakeholders. In many cases, information exchange, joint exercises and joint risk assessments make it possible to overcome the diffusion of responsibility and coordinate work.

While both the private and public sectors support these partnerships, developing and implementing effective information-sharing mechanisms has proven difficult in practice due to cultural differences between the two communities. While some PPPs have been able to establish effective information-sharing relationships and coordination capabilities, others struggle to foster such partnerships due to concerns about inappropriate disclosure of information and other mismatches between private and public stakeholders' expectations and priorities.

For instance, lack of transparency and lack of information on the corporate side makes it very difficult, if not impossible, for policymakers to understand the root causes and possible cascading interdependencies between affected critical sectors and the impact on national security and the economy.

In context of information-sharing and monitoring, the roles of different stakeholders are usually as follows:

- **Government:**
  - Develop public policies for monitoring CEI and regulating information-sharing, particularly concerning sensitive information.
- **Regulators:**
  - Enforce government regulations related to energy infrastructure monitoring and sensing through compliance checks.
  - Organize workshops and consultations with the energy industry to determine requirements.

- **Owners:**
    - Request monitoring and sensing of critical assets in energy infrastructure and ensure operators develop skills in data collection and disruption prevention.
- **Operators:**
    - Implement monitoring systems, collect robust data, conduct analysis and adopt good practices indicated by regulators.

4.2.6.2. Joint risk management and coordination in emergency response plans elaboration

The risk management framework designed for PPPs in the context of CEI protection prioritizes widespread utility. To achieve this objective, the framework is designed with a high degree of flexibility, allowing each stakeholder to tailor their risk management strategies to address the specific threats within their area of responsibility. This adaptability ensures a comprehensive and nuanced approach to risk mitigation within the PPP framework.

A common approach is the establishment of dedicated, permanent working groups composed of representatives from a broad spectrum of stakeholders within the leading energy sector, including both industry participants and regulatory bodies. For example, the information security domain within oil and gas facilities presents a unique challenge related to threats from third parties.[104] Effective risk assessments in this context require close collaboration with private companies,[105] which could be achieved through a multi-stakeholder permanent working group.

To achieve optimal effectiveness in CEI protection, PPPs should encompass the entire risk management cycle. This includes involving private companies in monitoring and reviewing processes to provide an up-to-date overview of the threat landscape. Such a comprehensive approach extends PPPs beyond the preparatory phase to include crisis management and recovery efforts.

Additionally, PPPs are essential for developing an effective crisis management plan for incidents, including terrorist acts targeting energy infrastructure. These plans should involve both public and private stakeholders and focus on (1) protecting the civilian population and (2) ensuring business continuity.

4.2.6.3. Cooperation in the development of security regulations

The development of nationally mandated safety requirements and standards within the energy sector, mirroring other critical industries, necessitates a collaborative and inclusive approach. These cooperation efforts require the active participation of CEI owners, operators and suppliers. Such an approach is paramount for achieving an optimum balance between public security and the continued viability of the energy industry. Security standards should mitigate risks effectively without imposing undue burdens on industry profitability, hindering timely implementation or compromising the technical feasibility of these measures.

[104] Third-party risk is any risk brought into an organization by external parties in its supply chain.
[105] https://www3.weforum.org/docs/WEF_Advancing_Supply_Chain_Security_in_Oil_and_Gas_2021.pdf.

Under this inclusive approach, private sector stakeholders could suggest modifications to existing security standards or government guidelines—for example, on safety-zone pipelines—within the framework of a transparent and consensus-driven PPP process.

A good example is the Nigerian Upstream Petroleum Regulatory Commission. As a national energy infrastructure regulator, since 2021 it has been conducting special forums and seminars dedicated to encouraging cooperation in rulemaking for effective implementation and sustainable compliance by all stakeholders.[106]

4.2.6.4. Joint trainings and security exercises in PPPs

CEI protection exercises are inherently multifaceted, necessitating coordination and operational cooperation between private security services and their governmental counterparts, including law enforcement agencies. Given the transnational and transboundary nature of many CEI assets (often located near land or sea borders), this cooperative approach is particularly crucial. Engaging in joint exercises and training sessions fosters the development of invaluable expertise in implementing complementary security measures, ensuring a comprehensive and effective protection against terrorist threats.

For example, after a number of UAS-attacks on oil plants in Saudi Arabia, in 2021, the Saudi navy conducted comprehensive exercises with oil companies to thwart drone and missile attacks on "vital oil installations".[107]

Case Study 9

Indonesia PPPs in energy facility protection against terrorist attacks

The Indonesian Navy with the country's Elite forces, Indonesian National Armed Forces (TNI) and the National Police (Polri) has conducted a series of exercises with an Indonesian oil and gas company to enhance energy infrastructure protection against terrorist attacks.[108]

In November 2023, the Indonesian Navy's Elite Forces took part in a liberation simulation of the hijacked Sanga-Sanga oil products tanker in the waters of Balikpapan, East Kalimantan. In the simulation in the waters of Balikpapan, the Sanga-Sanga tanker, about to enter Balikpapan Bay, was attacked by 20 armed hijackers using two speedboats approaching from the left side of the ship's hull. There was also simulated terrorist activity near the offshore oil platform at Sepinggan.

The exercise to handle security disturbances at sea was carried out swiftly by deploying 274 personnel from the Denjaka anti-terror detachment, supported by various elements of the Indonesian Navy. The Indonesian Navy forces attacked the hijackers on the tanker and the offshore platform, successfully neutralizing all threats.

106 Available at https://leadership.ng/stakeholders-engagement-and-anticipated-oil-gas-industry-turnaround/.
107 Available at https://www.worldoil.com/news/2021/3/22/aramco-and-saudi-navy-start-exercises-to-thwart-drone-and-missile-attacks.
108 For example: https://www.pertamina.com/en/news-room/news-release/strengthening-security-of-national-vital-object-pertamina-indonesian-navy-conducts-emergency-drill.

Case Study 10

Canadian Resources Infrastructure Resilience Nexus (CRIRN)

The Canadian Resources Infrastructure Resilience Nexus (CRIRN) is a special project operated by the Energy Infrastructure Security Division of Ministry of Canada's Natural Resources (NRCan)—the lead federal department for CEI security. The NRCan is guided by the three strategic objectives of the National Strategy for Critical Infrastructure:

- Build partnerships to support and enhance CI resiliency
- Implement an all-hazards approach to risk management
- Advance the timely sharing and protection of information among partners and stakeholders

CRIRN is aimed at fostering PPP in CEI protection in Canada and helps to strengthen the links between technology, security and the energy sector stakeholders.[109] CRIRN occupies a unique position at the intersection of the Canadian CI, the security and intelligence community and research institutions. It leverages expertise and trusted relationships to provide energy sector owners and operators with knowledge and skills to transform information into action.

Source: https://natural-resources.canada.ca/sites/nrcan/files/science-and-data/science-research/cyber-security/eisd-booklet-en.pdf.

Case Study 11

PPPs in CEI protection in Algeria

In 2023, the Algerian government launched a counter-terrorism plan to protect oil and gas facilities from potential terrorist acts, with a strong emphasis on PPPs. This plan included hiring over 20,000 security personnel to safeguard CEI across the country. Additionally, USD 400 million were allocated for the development of security systems for oil and gas infrastructure. As a result, the largest Algerian oil and gas company adopted a new security strategy, working alongside authorities to protect the nation's vital energy facilities. To further discuss enhancing counter-terrorism capacity through PPPs, a special meeting was held in July 2023 with top managers from the Algerian oil and gas sector, the Ministry of Energy and Mines, and state security forces.

Source: https://english.aawsat.com/home/article/4102616/algeria-allocates-400-mln-protect-oil-facilities-against-terrorism.

[109] Energy infrastructure security division, available at: https://natural-resources.canada.ca/sites/nrcan/files/science-and-data/science-research/cyber-security/eisd-booklet-en.pdf.

Case Study 12

Public-private coordination and collaboration in offshore energy infrastructure protection in India

The safeguarding of offshore energy facilities necessitates a cohesive and multi-stakeholder approach. In India, this collaborative effort is spearheaded by the Offshore Security Coordination Committee (OSCC), established in 1978. Functioning as the apex body for offshore security oversight and evaluation, the OSCC convenes biannually under the chairmanship of the Director General of the Indian Coast Guard. Its membership encompasses representatives from a diverse range of stakeholders, including the Indian Navy, Air Force, Coast Guard, Intelligence Bureau, Ministry of External Affairs, Indian police forces and the Indian Oil and Natural Gas Company.

Further augmenting this framework is the "Flag Officer Defence Advisory Group and Adviser Offshore Security and Defence to the Government of India" (FODAG), established in 1983 and re-designated in 2002. As a member of the OSCC, FODAG serves as the nodal agency for interaction with ONGC and other oil exploration and production companies. Its primary function is to advise the Government of India on offshore security and defense matters pertaining to installations within India's maritime zones.

Regional Contingency Committees (RCCs) provide an additional layer of coordination. Chaired by the respective Chiefs of Staff of the Indian Navy's Western and Eastern Naval Commands, these committees also meet twice a year. Their composition mirrors the OSCC with the inclusion of representatives from private entities within the upstream oil and gas sector.

Beyond deterrent patrolling activities, a crucial aspect of India's offshore security strategy involves the regular conduct of contingency-based exercises. Culminating in a large-scale, biannual simulation known as Exercise PRASTHAN, these exercises provide a platform for rehearsing responses to a variety of potential threats. Scenarios practiced during Exercise PRASTHAN encompass anti-hijacking drills, bomb disposal procedures, fire emergencies, structural damage, oil spills, medical evacuations and assistance to disabled vessels. Notably, the 2023 iteration of the exercise involved participation from the Indian Navy, Air Force, Coast Guard, Indian oil and gas company's security forces, Directorate General of Shipping, Maharashtra Police, Customs, Fisheries Department, Mumbai Port Authority, JN Port Authority and other relevant state and central civilian agencies. This multi-agency participation ensures a comprehensive and realistic assessment of preparedness for various contingencies, ultimately strengthening established Standard Operating Procedures.

In 2023 the exercise was conducted on Greatdrill Chaaya platform. The exercise saw actions to counter contingencies such as fire outbreak on the oil platform, oil spill within designated area, flight emergencies, hazardous gas leak scenarios, assistance rendered to a disabled vessel in the offshore zone and medical evacuation of platform crew. The exercise provided a realistic setting to assess preparedness of all concerned to tackle these contingencies and strengthen standard operating procedures.

Source: https://maritimeindia.org/physical-protection-of-indias-critical-maritime-infrastructure-part-2-maritime-energy-sector/.

4.3. Operational framework and technical readiness in CEI protection

Over the past years, Member States have been very active in adapting their operational frameworks to the protection of CEI. In most cases, such frameworks include a structured set of guidelines, principles, and good practices that govern energy infrastructure protection activities of both public and private sector actors.

4.3.1. Risk management: threat, risk and vulnerabilities in energy infrastructure protection

The Security Council on 13 February 2017 through its resolution 2341 called upon Member States "to consider developing or further improving their strategies for reducing risks to CI from terrorist attacks, which should include, inter alia, assessing and raising awareness of the relevant risks, taking preparedness measures, including effective responses to such attacks, as well as promoting better interoperability in security and consequence management and facilitating effective interaction of all stakeholders involved" (paragraph 2).

Based on a structured approach to dealing with risk, all required aspects must be combined and described in a comprehensive framework intended to support organizations in managing risks effectively and efficiently. The content of the risk management framework will depend on the size and complexity of the organization/enterprise/facility, its risk exposure, legal requirements and the elements of risk management or management systems already implemented.

In general, risk management procedures related to CIP include:

- Risk assessment (see 4.3.2)
- Vulnerability assessment (see 4.3.4)
- Threat assessment (see 4.3.5)

Consequence assessment is also a critical component in this context. It involves evaluating the potential impacts of an attack on CEI, including economic, environmental and societal consequences. Although consequence assessment is essential for a comprehensive understanding of overall risk, it will not be addressed in detail in this Guide.

It is important to note that some methodologies incorporate threat, consequence and vulnerability assessments as integral parts of the overall risk assessment.

The overall goal of risk assessment methodologies is to provide a framework that, given national level and CEI sector specific priorities and requirements, makes it possible to allocate protection resources effectively in order to reduce vulnerability and minimize the consequences of attacks.

4.3.2. Risk assessment

Risk assessment is a fundamental step in ensuring effective CEI risk management, including risk control and risk reduction, and is essential for developing successful CEI protection strategies. While established methodologies exist, their application to CEI protection requires significant expertise and technical knowledge.

Cross-sectoral risk assessments are particularly important. These assessments cover the energy sector as well as interdependent sectors such as finance, information and transportation, revealing critical interdependencies and interconnections. Often paired with supply chain risk management practices, this approach facilitates consistent evaluation and ongoing updates of complex macro-level supply chain risks. It allows CEI owners, operators and state bodies to prioritize risk management efforts effectively.

Energy sector-specific risk assessments help identify CEI facilities, enabling the prioritization of resources, such as finances, personnel and information, for their protection. These assessments also inform decisions on mitigation measures and operational tactics, providing an accurate estimation of CEI vulnerability to terrorist threats. This is crucial for developing strategies to protect CEI from terrorist attacks and minimize potential losses.

Site-specific risk assessments focus on the unique vulnerabilities and threats associated with each individual CEI facility, offering a more detailed analysis.

Over the past decade, various methodologies have been developed to estimate risks and vulnerabilities in energy infrastructure protection. Examples include network theory, rating matrices and system dynamics methods.[110]

Additionally, different approaches to risk management have led to the development of widely used methodologies around the world. Notable examples include the International Organization for Standardization (ISO) standards on risk management, which provide comprehensive frameworks and guidelines for assessing and managing risks in various contexts, including CEI protection.[111]

[110] Yao, Xijun & Wei, Hsi-Hsien & Shohet, Igal & Skibniewski, Miroslaw. (2020). *Assessment of Terrorism Risk to Critical Infrastructures: The Case of a Power-Supply Substation*. Applied Sciences. 10. 7162. 10.3390/app10207162. https://www.researchgate.net/publication/346227204_Assessment_of_Terrorism_Risk_to_Critical_Infrastructures_The_Case_of_a_Power-Supply_Substation.

[111] More information available at https://www.iso.org/iso-31000-risk-management.html.

Tool 3

Example of a risk analysis method: the BCK model

The Bayesian network – Consequence – Knowledge (BCK) model, specifically designed to evaluate terrorist attack risks on Liquefied Natural Gas (LNG) storage tanks, proposed by researchers Rongchen Zhu, Xiaofeng Hu, Yiping Bai and Xin Li from People's Public Security University of China and China University of Mining & Technology (Rongchen Zhu et al., 2021), offers a comprehensive approach that incorporates the following key elements:

- Multidimensional Risk Factor Identification: The BCK model emphasizes the importance of identifying risk factors from a multifaceted perspective, considering potential cross-sectoral interdependencies that could exacerbate the impact of an attack.
- Graphical Model Construction and Conditional Dependency Analysis: The model utilizes graphical models, such as Bayesian networks, to visually represent the relationships between various variables and their conditional dependencies. This facilitates a more precise understanding of how different factors influence the likelihood and severity of an attack.
- Event Tree and Fuzzy Set Theory for Consequence Evaluation: Building upon the risk factor analysis, the BCK model employs event trees and fuzzy set theory to evaluate the potential consequences of a terrorist attack. Event trees provide a structured framework for exploring different attack scenarios and their corresponding outcomes. Fuzzy set theory allows for the incorporation of uncertainty and ambiguity to risk assessments.
- Knowledge Graph for Risk Knowledge Storage and Visualization: A key innovation of the BCK model is the application of a knowledge graph. This knowledge graph serves as a central repository for storing risk knowledge, including the identified nodes from the graphical models and the evaluated consequences of different attack scenarios. The knowledge graph not only facilitates the storage and retrieval of risk information but also offers a highly visual representation of various risk factors and their interrelationships.

Source: https://www.sciencedirect.com/science/article/abs/pii/S0925753521000370

4.3.3. Reviewing and monitoring risk indicators

CEI risk management should be grounded in risk indicators, which are usually categorized into different groups. Identified risks and their potential consequences can be categorized by both general criteria applicable to all CI (such as casualties and economic impact) and energy-specific criteria (such as ecological and social effects). The risk assessment process includes ranking CI and modelling interdependencies by identifying potential risk chains. Some approaches to risk management also describe the root causes of vulnerabilities related to capacity, competence and performance of CI.

For instance, the security risks associated with pipelines can be more critical than those of stationary oil plants or refineries. This is because pipelines extend thousands of kilometers through diverse areas, each with varying population densities, natural environments, assets and nearby vulnerable centres.[112]

Another important aspect is the interdependencies between energy facilities and other sectors, which can be categorized into types such as physical, informational, geographical and sometimes logical.[113]

Terrorist tactics and methods are constantly evolving and, similarly, the functioning of energy facilities is changing. For example, new equipment or control systems might reduce certain vulnerabilities but also introduce new ones.

In this regard, as part of risk management, it is important to:

- Regularly review indicators and threat scenarios
- Update the list of energy facilities classified as "critical" according to established criteria
- Reassess risk opportunities
- Revise and update the risk management documentation to reflect changes in the risk context and identify new risks

4.3.4. Vulnerability assessment

As previously mentioned, effective CEI protection based on a risk management approach must include vulnerability assessment as an integral component. Vulnerability can be analyzed by modelling how various infrastructure components respond to threats and assessing the overall risk to the infrastructure. This involves evaluating the consequences of an attack on each component, understanding the interactions between components and assessing the combined impact of both direct and indirect damage on the overall functionality of the infrastructure.[114]

Vulnerability assessments could include defining critical elements and establishing protection procedures. In the context of CEI, certain elements can be identified as critical to the functioning of the infrastructure and more vulnerable to direct physical attacks. This assessment can be part of a 'technological map' analysis, which involves evaluating the protections and interlocks designed to handle emergencies and identifying critical elements (or "soft spots") whose disruption would necessarily interrupt the technological process.

Critical elements of an energy infrastructure facility can include:

- Structural and technological components: These encompass the facility's main structures, administrative buildings, engineering structures and communication systems. For example, at a gas filling station, this

[112] Donya Fakhravar, Nima Khakzad, Genserik Reniers, Valerio Cozzani, *Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network*, Process Safety and Environmental Protection, Volume 111, 2017, Pages 714-725, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2017.08.036, available at: https://www.sciencedirect.com/science/article/abs/pii/S0957582017302914.

[113] According to relevant research of Petit F., Verner D., Brannengan D. et al. (2015), *Analysis of Critical Infrastructure Dependencies and Interdependencies*, logical dependency is attributable to human decisions and actions and is not the result of physical or cyber processes. Available at: https://publications.anl.gov/anlpubs/2015/06/111906.pdf.

[114] See above.

includes the production area with gas compressors, refilled cylinder storage, auxiliary areas with gas storage, garages and so forth.

- System elements: Components or devices within potentially dangerous installations.
- Storage areas: locations for weapons, ammunition and their components if they are located in the facility's premises.[115]
- Hazardous materials sites: Areas containing poisonous and/or flammable substances.
- Other vulnerable systems: Any other systems, elements, or communications identified as vulnerable to physical attacks following the vulnerability assessment.

The results of any vulnerability assessment should be used to develop and implement CEI mitigation and emergency response plans, in coordination with national or local plans and guidelines.

Box 6

Vulnerability assessment in risk management cycle

A vulnerability assessment, as part of risk assessment and overall risk management, is a comprehensive study that includes:

- Purpose and features: Examining the energy facility's purpose, functional characteristics, location, and scale.
- Protection measures: Evaluating the resources and measures for physical protection and security, including internal security protocols and access control procedures.
- Critical and vulnerable areas: Identifying critical elements, potentially dangerous zones and vulnerable areas within the facility.
- Terrorist threats: Assessing potential terrorist threats specific to the energy facility.
- Terrorist methods and consequences: Analyzing possible methods terrorists might use to carry out attacks and the anticipated consequences of such acts.
- Purpose and features: The energy facility's purpose, functional characteristics, location and scale.
- Protection measures: The available resources and measures for physical protection and security, including internal security protocols and access control procedures.
- Critical and vulnerable areas: Identification of critical elements, potentially dangerous zones and vulnerable areas within the facility.
- Terrorist threats: Potential terrorist threats specific to the energy facility.
- Terrorist methods and consequences: Possible methods terrorists might use to carry out attacks and the anticipated consequences of such acts.

[115] In many states the security services of critical energy facilities are armed with non-lethal (electric stunning devices, gas spray guns) or lethal weapons (pistols, automatic rifles, etc.).

Tool 4

Physical Security Information Management (PSIM)

PSIM is a 3D visualization tool to design physical protection systems on energy infrastructure. It is suitable for large-scale systems such as, for example, oil/gas infrastructure facilities, with a significant number of integrated physical, operational and information security subsystems. It may be used as a computer modelling tool to simulate potential attacks against stationary oil and gas facilities (plants, storages, refineries, etc.). This approach considers factors like the number and equipment of attackers, their gear and transportation. PSIM helps enhance operational measures and select cost-effective methods.

It is advisable to use modelling methods with a risk-based approach and consider all possible terrorist scenarios against the energy facility. Therefore, it is essential to analyze the facility's vulnerability in order to identify critical elements and vulnerable areas. Attacks on these areas could result in severe consequences for personnel, the facility, and the environment, potentially leading to its complete shutdown.

Source: PSIM tool «Iteration physical protection system», available at https://iter.ru/en/TERATION_PHYSICAL_PROTECTION_SYSTEM.pdf.

4.3.5. Threat assessment

The preparation of threat or attack scenarios should be part of the threat assessment process. For example, computer simulations of possible terrorist attacks on CI involve analyzing the capabilities of malicious actors such as terrorists, and their access to new technologies. Simulations can also identify the types of potential attacks and assess their level of sophistication. The threat assessment involves identifying various threat types, evaluating their potential impact on the facility and determining the most effective mitigation strategies based on current capabilities and resource needs.

In the realm of CEI protection, threat modelling is a key method for evaluating security risks comprehensively. This technique, based on risk assessment principles, helps identify potential vulnerabilities across various security scenarios that could be exploited by terrorists. By proactively employing threat modelling, stakeholders can mitigate the potential impact of attacks on personnel, physical facilities, and the surrounding environment.

However, it's important to recognize the inherent diversity within infrastructure categories. Facilities within the same category may have different functionalities and operational contexts, leading to variations in their vulnerability profiles. Therefore, a unified methodology for vulnerability analysis is essential. This methodology should be specifically tailored to address the unique scenarios posed by terrorist threats, ensuring a comprehensive and targeted defense against potential attacks.

Tool 5

Attack modelling aligned with identified risks

During the development of terrorist threat scenarios for CEI, a structured approach can be employed to model potential attacks. This approach can be broken down into the following stages.[116]

1. Motivation and Attack Type Identification: This stage involves determining the most likely motivations for terrorist attacks against CEI facilities and the type of attack most likely to be employed.
2. Target Identification: Based on the identified motivations, specific buildings or vulnerable elements within the CEI are identified as potential targets.
3. Reconnaissance Methods: This stage analyzes the methods terrorists might utilize to gather information about the target facility, such as security systems, technical equipment, communication channels, flammable material storage areas, etc.
4. Attack Methodology Exploration: Possible means and methods terrorists could employ to execute the attack are explored and analyzed.
5. Perpetrator Identification: This stage focuses on identifying potential participants in the attack, including both external actors and potential insiders.
6. Resource Assessment: The potential financial costs and resources required for the attack are estimated.
7. Preparation and Acquisition: This stage analyzes the methods used by terrorists to prepare for the attack, including participant training and acquisition or manufacturing of attack tools.
8. Covert Communication: Methods for establishing and maintaining covert communication between attackers are considered.
9. Temporal and Spatial Planning: This stage involves selecting the specific date, time, and location for the attack.
10. Escape and Evidence Elimination: Strategies for escape after the attack and the elimination of evidence related to planning and execution are explored.
11. Information Support: Methods for disseminating information in support of the attack's objectives are analyzed.

[116] Zhadikov R.S., Bekzhanov M.A. *Organization of a system of anti-terrorist protection of objects vulnerable to terrorism: Scientific and practical manual*. Almaty: Academy of the National Security Committee of the Republic of Kazakhstan, 2018. 104 pages.

4.3.6. Prevention and response measures for CEI protection

Prevention and response measures for CEI protection against terrorist attacks should be based on a comprehensive approach, and include certain measures and tools, proportionate to the risks identified, to:

- Ensure physical security of energy facilities (see 4.3.6.1)
- Ensure information security of energy facilities (see 4.3.6.3)
- Mitigate interconnections (see 4.3.6.4)
- Elaborate emergency response and contingency plans (see 4.3.6.5, 4.6.5.6, 4.3.6.7)

4.3.6.1. Physical security measures

Physical security measures should be selected based on previously conducted risk assessments and identified residual vulnerabilities. The specific measures applicable to a facility determine the range of equipment to be used. Physical security of CEI encompasses both perimeter security and indoor security. Perimeter security focuses on preventing unauthorized entry into the facility, while indoor security addresses what occurs within the facility's perimeter. Indoor security acts as a backup to perimeter defenses in the event of a successful breach and aims to prevent misconduct by CEI personnel.

Table 6
Physical security measures against terrorist attack on CEI

Measures	Equipment	Remarks
Perimeter security		
Delineation of CEI area perimeter	Fences, walls	CEI area shall be clearly marked to prevent accidental entry
Engineering protection	Fortified structures, blast walls, barbed wire	The CEI perimeter structures shall prevent easy unauthorized entry into the facility territory
Surveillance	CCTV cameras, intrusion sensors, security lighting, thermal detectors, laser fences	The employed equipment shall allow for 24-hour detection of unauthorized entry with immediate notification of the CEI central security post and police/national guard unit in charge of CEI backup protection
Entry control	Security gatehouse equipped with CCTV, barriers, access control system, X-Ray scanners, hand-held metal detectors, explosives trace detection, explosive detection dogs, etc.	A gatehouse shall provide for secure flow of personnel and vehicles

Measures	Equipment	Remarks
Indoor security		
Indoor patrolling	Armed foot guards or maritime patrol in case of offshore infrastructure[117]	Physical presence of patrolling guards within the perimeter allows rapid deployment to an incident
Surveillance	CCTV cameras, security lighting, UAS, volumetric detectors, etc.	Indoor equipment shall cover all areas and premises of the CEI facility. UAS may backup the CCTV cameras in case of their deliberate or accidental failure
Communication	Landline, mobile and radio communication devices, alarm buttons	All security staff shall be provided with at least two means of communication. The communication means used should duplicate each other in case any one of them is suppressed

The security measures will need to be updated if the security environment and risk assessment change. For example, if new roads leading to the CEI facility are built, they will have to be equipped with anti-ramming devices (barriers) to counter potential vehicle-borne terrorist attacks.

Moreover, Member States are increasingly implementing so-called “security-by-design” approaches as a tool to achieve physical security goals at the design and construction (or renovation) stages of buildings that host critical energy facilities.

New technologies are also helping to address significant challenges related to oil and gas pipelines. For example, distributed acoustic sensors (DAS) that use fibre-optic cables to detect ground seismic-acoustic vibrations at distances of several dozens of kilometers along the cable.[118]

[117] For example, in India physical security of offshore oil and gas infrastructure is ensured through continuous patrols by 1 armed patrol "Immediate Support Vessels" staffed by Naval personnel.

[118] For example, Houjia X, Yuantao L., Taotao Z., Fengyi L, et al, *An overview of the oil and gas pipeline safety in China*, Journal of Industrial Safety, 2024, available at: https://www.sciencedirect.com/science/article/pii/S2950276424000035. Also available at https://en.t8-sensor.ru/pipelines.

Case Study 13

Physical security measures on East African Crude Oil Pipeline Project (EACOP), Uganda

The Petroleum Authority of Uganda (PAU), in consultation with relevant Government security agencies, identified major security threats to the East African Crude Oil Pipeline Project currently under construction.[119] These threats include sabotage and terrorist attacks, as well as other emergency situations. A security strategy was therefore developed to address these challenges. A fibre-optic cable will be used to monitor intrusion along the entire length of the pipeline (1,443 km length). Additionally, other measures will be put in place at EACOP energy facilities in Uganda, such as:

- Deployment of a canine team and bomb squad.
- Deployment of access control security personnel and three walk-through metal detectors to screen individuals accessing the premises.
- Deployment of a fire truck and fire brigade team.
- Deployment of more than 50 security officers including day and night duty.
- Deployment of at least 10 traffic officers to guide movement of vehicles at the venues.
- Barricading off the perimeter of venues using warning tapes.

Source: Report on East African Crude Oil Pipeline Project environment and social impacts, Uganda, 2019, available at https://www.eia.nl/projectdocumenten/00009498.pdf.

4.3.6.2. UAS measures

Securing energy facilities against UAS attacks presents a complex challenge due to the difficulty of controlling the airspace around these facilities. The frequent proximity of energy infrastructure to transportation corridors further complicates this issue, as it allows terrorists to deploy UAS from a relatively close range.

In most cases, the standard procedure to counter UAS-attacks against CEI includes the following steps:

- Monitoring the airspace above the protected facility and the area surrounding the perimeter.
- Informing operators about detected targets.
- Using tools to detect UAS in case of suspicious activity.
- Identifying the type of UAS and distinguishing it from false targets such as birds.
- Issuing target designation for means of neutralizing a potential threat.
- Neutralizing the potential threat.

The combination of these factors necessitates the implementation of a complex surveillance system for the surrounding air and ground space. To ensure effective round-the-clock and all-weather control, the most reliable observation method is a combination of radar and radio equipment, supplemented by optical observation methods. Radar sensors are essential for pinpointing the location of the observed object and

[119] East African Crude Oil Pipeline Project, available at: https://eacop.com/overview.

determining a target designation to deter or neutralize the threat. There are different options for placing radar sensors, depending on the configuration of the protected facility and the required viewing area.

Increasingly, the private sector is developing UAS specifically designed to monitor oil and gas pipeline fields. For example, some of these UAS combine the advantages of aircraft and helicopter design (hybrid aerodynamic), include aerial monitoring (e.g. through remote laser scanner and a high-resolution video camera mounted on the UAS), and process data with self-learning systems.

Box 7

Methods to detect a UAS-attack against energy infrastructure

The main and most effective methods for UAS detection are:

- Radar detection in which radar provides UAS coordinates, movement parameters and characteristics by analyzing emitted and reflected radio waves.
- Radio detection systems scan for UAS signals and can be used to determine their location and trajectory.
- Optical detection uses highly developed optoelectronic sensors.
- Acoustic detection, which allows UAS to be detected with the help of ultra-sensitive noise microphones.

4.3.6.3. Measures to ensure information security of energy infrastructure

Measures to ensure the information security of energy infrastructure should include:

Hardware and Software Protection Means:

- This includes firewalls, antivirus programs, intrusion detection/prevention systems (IDS/IPS) and other security tools to protect against unauthorized access and ICT-related threats.

Information Security Policy Means:

- Establishing and enforcing rules and rights for access to resources and databases, typically based on the need-to-know principle. This involves role-based access control (RBAC) and regular audit to ensure compliance.

Separation of Information Systems:

- Also known as network segmentation, this involves dividing a network into smaller, isolated segments to prevent an outage or security breach in one segment from affecting the entire system.

Information Security Incident Analysis and Information-Sharing:

- Regular analysis of ICT-related incidents to understand and mitigate vulnerabilities. Sharing information about threats and vulnerabilities with other stakeholders (such as other energy companies, government agencies and information security organizations) is crucial for collective defense.

Implementing a System for Anonymous Tipoffs:

- Having a system for anonymous reporting can help identify internal threats from employees or insiders who might have malicious intent.

Digital Signature Verification and Comprehensive Authentication:

- Ensuring the authenticity and integrity of commands and communications through digital signatures and robust authentication methods (e.g., multi-factor authentication) is critical for preventing unauthorized actions.

Regular Security Training:

- Training for employees on information security awareness to recognize and respond to potential threats.

Regular Updates and Patching:

- Ensuring that all hardware and software are regularly updated and patched to protect against known vulnerabilities.

Incident Response Plan:

- Developing and maintaining a comprehensive incident response plan to quickly and effectively respond to security breaches.

Physical Security:

- Although the focus is on information security, physical security measures are also crucial to protect the infrastructure from physical attacks that could compromise information security.

Another effective organizational measure is to obligate CEI operators to promptly inform authorities about every information security incident. Many Member States have operational centres for information security incidents. However, given the vulnerability of the energy sector to ICT-based terrorist attacks, some countries have established specialized centres and Computer Security Incident Response Teams specifically for CEI operators. For example, in Australia, since 2021, electric grid operators must report every information security incident at their facilities, including ransomware, phishing and other similar threats.[120] Another example was reported by the Indonesian government in 2022, when it established a Computer Security Incident Database to accumulate ICT-related incidents in CI sectors, including energy.[121]

[120] Available at https://www.abc.net.au/news/2021-10-13/government-will-mandate-business-reporting-ransomware-attacks/100534890.
[121] Available at https://www.thejakartapost.com/paper/2023/08/09/cybersecurity-strategy-for-indonesias-critical-infrastructure-protection.html.

Some Member States have established Integrated Data Security Systems for CEI. For example, according to Brazil's National Critical Infrastructure Protection Policy, the Critical Infrastructure Security Data System contains computerized records of the security conditions of critical infrastructure, including energy facilities across the national territory. This system encompasses the collection, processing, storage, and retrieval of information.[122]

Tool 6

Laboratory for ICT-risk modelling in critical oil and gas facilities (Gubkin University)

The laboratory is based on the AMPIRE software and hardware complex and utilizes a "digital twin" of typical information processes in an oil and gas company to simulate various types of ICT-based attacks. These attacks can be conducted by company personnel during specialized training sessions, with some IT specialists acting as "attackers" and others as "defenders".

The training conducted in this laboratory aims to improve the following skills:

- Monitoring and detecting computer attacks targeting elements of the information systems of a virtual oil and gas company.
- Using specialized software to detect and analyze information security events, including malicious ICT activities.
- Conducting investigations to localize attack vectors and making changes to elements of the information system of a virtual enterprise to neutralize identified threats.

This laboratory is used by Gubkin University for training full-time students as well as company personnel undergoing professional development programs.

Source: https://en.gubkin.ru/news/university-life/the-training-laboratory-to-study-computer-attack-detention-was-established-at-gubkin-university/.

[122] Política Nacional de Segurança de Infraestruturas Críticas, DECRETO Nº 9.573, DE 22 DE NOVEMBRO DE 2018, available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm.

Case Study 14

EU Commission Recommendation 2019/553 on cybersecurity in the energy sector

According to EU Commission Recommendation 2019/553 energy network operators should:

a. Analyse the risks of connecting legacy and Internet of Things concepts and be aware of internal and external interfaces and their vulnerabilities.
b. Take suitable measures against malicious attacks originating from large numbers of maliciously controlled consumer devices or applications.
c. Establish an automated monitoring and analysis capability for security-related events in legacy and Internet of Things environments, such as unsuccessful attempts to log-in, door alarms for cabinet opening or other events.
d. Conduct on a regular basis specific information security risk analysis on all legacy installations, especially when connecting old and new technologies; since the legacy installations often represent a very large number of assets, risk analysis may be done by asset classes.
e. Update software and hardware of legacy and Internet of Things systems to the most recent version whenever adequate; in so doing, energy network operators should consider complementary measures such as system segregation or adding external security barriers where patching or updating would be adequate but is not possible, for instance unsupported products.
f. Formulate tenders with information security in mind, that is, require information about security features, demand compliance with existing information security standards, ensure continuous alerting, patching and mitigation proposals if vulnerabilities are discovered and clarify vendor liability in the event of computer attacks with the use of ICTs.
g. Collaborate with technology suppliers to replace legacy systems whenever beneficial for security reasons, but take into account critical system functionalities.

Source: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019H0553.

4.3.6.4. Measures to mitigate interconnectedness

As noted earlier in the Guide, the development of international and regional energy systems inevitably creates interdependencies that introduce additional vulnerabilities to energy infrastructure. To mitigate these interconnected vulnerabilities, the following measures could be considered:

- Increase awareness of interdependencies: Promote collaboration within and between different sectors through workshops, for example, and multi-sector meetings that address shared challenges across industries.[123]
- Integrate interdependencies into risk management frameworks: Incorporate the concept of interdependencies or cascading effects into risk management frameworks, such as threat scenarios. This approach encourages greater cooperation among stakeholders.

[123] For example, during the "Russian Energy Week" conference stakeholders from both fossil fuels and renewable energy sectors come together to discuss common issues. See https://rusenergyweek.com/en/about/about-rew/.

- Avoid single-source dependencies: Ensure the availability of alternatives and diversification to reduce reliance on a single source.
- Promote cross-sectoral exercises: Conduct cross-sectoral exercises to verify the effectiveness of incident response capabilities.

Moreover, energy infrastructure protection should consider dependencies not as static relationships but rather as dynamic and rapidly shifting. Raising awareness of mutual dependencies through inter-sectoral networking, such as risk scenarios discussions, can stimulate further cooperation among various stakeholders.

4.3.6.5. Mitigation and emergency response plans

Mitigation and emergency response measures are essential components of counter-terrorism protection for energy infrastructure and must comply with international obligations, including international human rights law and international humanitarian law.

Comprehensive emergency response plans are crucial and should detail procedures for handling incidents involving energy infrastructure. In many Member States, operators of critical energy infrastructure are required to anticipate, prevent and mitigate potentially dangerous conditions associated with their facilities. These emergency plans should outline emergency repair and recovery actions, set priorities, assign responsibilities, identify resources, and address coordination and communication during emergencies.

As previously mentioned in Section 4.3.2, CEI operators should use threat and risk assessment processes to identify potential incidents that would require an emergency response. The emergency plan should include the chain of command for responding to emergencies, a method for classifying incidents and an outline description of the incident management system. For instance, in Canada, operators are required to provide details on real-time monitoring of energy facilities, describe drills and exercises for testing procedures and outline measures to inform and instruct first responders, medical facilities, organizations and users about facility locations, potential emergencies and safety procedures.

Emergency plans should also establish rosters for emergency personnel, including on-call arrangements and rapid mobilization protocols. Additionally, these plans must be tailored to local and geographic contexts, considering factors such as neighboring area specifics and facility transport accessibility. They should also include tools and mechanisms for emergency communication with dependent facilities and sectors. A designated focal point, responsible for implementing and coordinating revisions of the emergency plan should be pre-trained and prepared for this role.

Active partnerships between the private sector and law enforcement authorities are vital for an effective response to attacks. For example, in Kazakhstan, security service heads are required to develop primary response algorithms to:

- Immediately inform law enforcement and national security agencies about terrorist threats.
- Timely report instances of theft or illegal acquisition of weapons or equipment that could be used to create IEDs.

Emergency plans should be integrated with those developed by relevant national authorities to avoid duplication of efforts and ensure that all needs are addressed. They should be updated according to the risk management and vulnerability assessment review procedures. Conducting emergency drills and crisis management exercises, involving both site operators and law enforcement, provides valuable opportunities to test procedures, identify coordination gaps, refine roles and update crisis management plans and protocols.

Early warning systems are integral to emergency response plans and are designed to promptly inform personnel and, when necessary, local communities. For example, an oil company in Kuwait uses electronic sirens with dual communication channels (main and redundant) across thirty gas wells. This risk-reducing measure is aimed at enhancing staff protection and ensuring timely alerts in case of emergencies.[124]

Regular training sessions and emergency response exercises, conducted in collaboration with local communities, are essential for preparing personnel to respond rapidly and effectively to emergencies. These training sessions also provide an opportunity to address community concerns and ensure that residents are well-informed about emergency response procedures.[125]

In response to emergencies, including potential terrorist attacks, most oil and gas companies establish operational centres to coordinate response activities and mitigate the impact of incidents. For instance, many companies deploy dedicated response centres that operate in conjunction with the company's central dispatch centre. This centralized approach ensures comprehensive coordination of all response actions and maintains full control over emergency operations until all remedial measures, such as environmental reclamation, are completed. Additionally, relevant emergency response agencies and regional or local authorities are notified and, if necessary, collaborate on evacuating nearby communities.

[124] Available at https://www.electronic-sirens.com/success-story-early-warning-system-kuwait-oil-company/.

[125] For example, https://dag-aif-ru.turbopages.org/turbo/dag.aif.ru/s/society/v_dagestane_na_neftegazovom_obekte_proshli_antiterroristicheskie_ucheniya.

4.3.6.6. Measures to mitigate environmental impact

Energy infrastructure recovery plans should include measures to mitigate environmental impact. For instance, pipeline operators typically develop spill response plans to minimize environmental damage in the event of a pipeline release due to an attack.

- A notable example is a major Russian oil and gas company that conducts regular recovery exercises—at least once a year—at oil wells in the Kara Sea, where the environment is particularly vulnerable to potential oil spills.[126] Such comprehensive exercises include oil spill clean-up, foaming and personnel evacuation.

Case Study 15

USA's Pipeline Security and Incident Recovery Protocol Plan

The objective of the Pipeline Security and Incident Recovery Protocol Plan is to establish a comprehensive interagency approach to counter risks and minimize consequences of emergencies involving pipeline infrastructure, specifically focusing on actions the U.S. Federal Government can take to assist pipeline protection, response and recovery.

The Plan presents a framework and protocols to support the recovery of pipeline infrastructure, as well as measures to prevent a security incident and enhance resiliency. The purpose of the Plan is to reduce the consequences of an attack, as well as minimize the operational impact of and time needed to recover from a disruption in the pipeline system infrastructure.

Source: https://www.tsa.gov/sites/default/files/pipeline_sec_incident_recvr_protocol_plan.pdf.

4.3.6.7. Contingency planning practices

In many Member States, CEI operators are required by law to develop a contingency plan as part of their emergency response preparedness. These plans are normally activated in the event of incidents involving personnel injuries, damage to facilities, or environmental pollution. By classifying the incident, it is possible to notify the maximum number of people in the shortest period, enabling them to take prompt and appropriate action. Generally, each type of incident requires a tailored response, involving specific instructions for different staff members, varying tasks and coordination with distinct organizational services.

Contingency plans provide clear instructions for personnel and security services, detailing the operation of critical systems during an emergency, including scenarios involving a terrorist attack on the facility. They also outline procedures for mobilizing personnel and equipment needed to manage emergencies effectively. For example, in the United Kingdom, energy operators are mandated to establish contingency arrangements and plans to address unexpected disruptions in energy supply.[127] Conducting tests is thus another typical requirement of these plans. The German Bundesnetzagentur (Federal Network Agency) for Electricity, Gas, Telecommunications, Post and Railway regularly stress tests the national energy system. These tests are

[126] For example, https://www.gazprom.ru/about/subsidiaries/news/2021/october/article540502/.

[127] UK's *Public summary of sector security and response plan*, 2018, available at https://assets.publishing.service.gov.uk/media/5c8a7845ed915d5c1456006a/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf

designed to prepare for potential electricity supply shortages and ensure that appropriate measures can be implemented in the event of an emergency.[128]

The contingency plan of an oil and gas company usually covers a broad range of scenarios, such as injuries necessitating evacuation and external medical assistance, hydrogen sulfide (H2S) poisoning (both individual and mass casualties), fatalities, personnel overboard incidents and serious injuries resulting from equipment failure. Additionally, these plans often specify criteria for classifying the severity of damage to the oil or gas facility and assessing potential environmental consequences, based on the type of spill and the nature of the discharged liquids.[129]

The plan should establish a central focal point within the company for coordinating response efforts, detail step-by-step actions for personnel, outline leadership succession and ensure clear communication channels for effective decision-making during emergencies.

Typically, contingency plans for energy infrastructure include:

- Rules and procedures for emergency notifications: Detailed guidelines for how to notify relevant parties in the event of an emergency.
- Immediate responsibilities of personnel: Clear distribution of tasks and coordination responsibilities among staff members.
- Alarm systems operation: Procedures for activating and managing alarm systems to alert personnel and external responders.
- Operation of backup systems: Instructions for ensuring that backup systems function correctly to maintain operations during an emergency.
- Evacuation instructions: Detailed plans for safely evacuating personnel from the facility.
- Measures to transition to a safe operating mode: Procedures for bringing the facility to a stable and secure operational state.
- Alternate emergency facilities: Identification of secondary locations or facilities that can be used in the event the primary facility is compromised.

[128] Available at https://www.bmwk.de/Redaktion/EN/Pressemitteilungen/2022/09/20220905-power-system-stress-test.html.
[129] For example, https://www.energean.com/media/1061/eisa-annex-13-contingency-plan.pdf.

5. International efforts to protect CEI

Due to the vast length of energy transportation infrastructure, cooperation between countries through whose territories cross-border CEI passes is crucial for effective security against terrorist attacks. The division of security responsibilities across multiple jurisdictions can increase vulnerabilities. Therefore, countries should work together to assess terrorist threats and develop comprehensive, human rights-compliant plans to mitigate them.

5.1. Cross-border energy infrastructure

5.1.1. Cross-border cascading effect

The globalization of the energy sector has reached an advanced stage and disruptions caused by terrorist attacks on storage facilities or pipelines can have widespread repercussions. Such disruptions can trigger chain reactions with severe consequences for other countries' energy sectors, as well as for societies and the environment.

A notable example of a cross-border cascading effect due to energy infrastructure disruption is the electricity blackout of the Central Asia power grid in January 2022.[130] As a result of a significant accident on the unified power grid of Central Asia, southern Kazakhstan, Uzbekistan and Kyrgyzstan experienced widespread power outages. Millions of people across Central Asia were left without electricity. The power loss led to the suspension of operations at airports and metro systems in Kazakhstan and Uzbekistan. Major mobile phone service providers in Kazakhstan, Kyrgyzstan and Uzbekistan reported loss of connection, while hospitals had to rely on generators to keep essential equipment operational.

Another example of cross-border energy infrastructure disruption happened in June 2024. A major power outage caused blackouts across the Balkan region. Power cuts started in Montenegro and then hit Bosnia and Herzegovina, parts of Croatia including the Dalmatia region, and northern Albania.[131]

These examples, together with the continuing growth of energy infrastructure integrity and interconnection at the global level highlight the importance of further developing international counter terrorism cooperation, including harmonization of legislation and judicial cooperation.

5.1.2. Need for cross-border cooperation in CEI protection

The transnational nature of terrorism necessitates enhanced cross-border cooperation for the protection of CEI. Many Member States have established legal and organizational frameworks for this purpose through bilateral and multilateral agreements, inter-governmental commissions and working groups. These collaborations are vital to international efforts aimed at countering terrorism targeting energy facilities.

[130] Available at https://www.reuters.com/world/asia-pacific/power-blackout-hits-kazakhstan-kyrgyzstan-uzbekistan-2022-01-25/#:~:text=ALMATY%2C%20Jan%2025%20(Reuters)%20-,use%20to%20cover%20unexpected%20shortages.

[131] Available at https://balkaninsight.com/2024/06/21/major-power-blackout-hits-albania-bosnia-croatia-montenegro/.

For example, as threats to offshore energy infrastructure grow, joint international initiatives are essential for safeguarding transport corridors used by oil and LNG tankers. This involves regular monitoring, sharing information about emerging threats and coordinating responses. Despite these efforts, CEI operators face significant challenges in protecting oil and LNG tankers and associated port infrastructure. Tankers navigating international waters must contend with the difficulty of patrolling extensive and hazardous travel routes, often with a limited number of defensive vessels.

5.1.3. Examples of international organizations working on energy infrastructure protection against terrorist attacks

It is important to note that there are no specialized international organizations exclusively dedicated to protecting oil and gas infrastructure from terrorist attacks. Generally, such activities fall under broader mandates of various organizations. For example:

- The United Nations Global Programme on Countering Terrorist Threats against Vulnerable Targets, as part of its mandate derived from the Global Counter-Terrorism Strategy, aims to support Member States in strengthening the protection of CI, including CEI. This programme is implemented by UNOCT, together with CTED, UNICR, UNAOC and in consultation with INTERPOL. Among its initiatives, the Programme provides capacity-building to beneficiary Member States; develops knowledge products such as technical guides with international good practices; connects experts worldwide through a dedicated Global Network on Vulnerable Targets Protection and helps Member States address emerging threats to vulnerable targets.
- The International Convention for the Safety of Life at Sea (SOLAS) of 1974, as amended, particularly Chapter XI-2, and the International Ship and Port Facility Security (ISPS) Code, along with the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention, including the 1988 and 2005 Protocols), provide comprehensive security-related requirements for governments, port authorities, and shipping companies. These regulations detail specific security measures for international shipping, port facilities, and fixed platforms on the continental shelf, including requirements for Ship Security Assessments and Plans, Port Facility Security Assessments and Plans, and the roles of security officers. As a result, national governments and terminal operators have taken steps such as enhancing physical security at port facilities and conducting offshore patrols, with compliance with ISPS Code requirements and improved security postures reported by tanker operators.
- Supporting the implementation of these regulations, the International Maritime Organization (IMO) plays a crucial role. As a United Nations specialized agency, the IMO assists Member States in developing and enhancing their national maritime security governance in line with SOLAS and the ISPS Code. This includes providing technical assistance for establishing National maritime security committees, risk registers and security strategies. The IMO also addresses the security of maritime-related energy infrastructure and elaborates on emergency response requirements for oil and LNG tankers in the event of terrorist and other unlawful acts.[132]

[132] Available at https://www.imo.org/en/OurWork/Security/Pages/FAQ.aspx#Should_IMO_should_be_worried_about_the

5.1.4. Examples of regional cooperation in energy infrastructure protection against terrorist attacks

Due to the need to protect cross-border energy infrastructure, regional organizations play a crucial role in facilitating cooperation among neighbouring countries. An illustrative example of such cooperation is the "*Recommendations on Countering Terrorism at the Energy Complex Facilities*," issued by the Collective Security Treaty Organization (CSTO) in December 2022 (see Annex 2).[133] This document provides a framework for Member States to enhance security measures against terrorist attacks targeting CEI. The Recommendations outline various anti-terrorism measures, including physical protection systems such as access control and security personnel, as well as robust information security protocols to protect infrastructure from ICT-related attacks. Additionally, the document emphasizes the importance of staff training in security procedures and public awareness campaigns to increase vigilance against potential threats.

Another notable example is the Trans-ASEAN Gas Pipeline, which enhances gas and LNG connectivity among Association of Southeast Asian Nations (ASEAN) through pipelines and regasification terminals. In 2021, ASEAN signed and adopted a Memorandum of Understanding for the Trans-ASEAN Gas Pipeline project, which includes provisions for implementing “appropriate measures to ensure the security and safety of the pipelines”.[134]

Given that outages in CEI can compromise energy supply availability, threaten regional stability and impact international energy prices, regional security organizations play an active role in cross-border CEI protection. Organizations such as the Regional Anti-Terrorist Structure of the Shanghai Cooperation Organization, the CIS Anti-Terrorist Center, ASEAN and the Organization for Security and Cooperation in Europe (OSCE) have developed a wide range of programs, courses and exercises for internationally coordinated prevention and crisis management.

For example, over the past decade, the OSCE has organized numerous events focused on protecting energy infrastructure from terrorist attacks. In 2020, the OSCE established the Virtual Centre for the Protection of Critical Energy Infrastructure. This platform facilitates collaboration among energy decision-makers, offering technical expertise, establishing norms and standards and promoting political engagement to ensure that CEI continues to support sustainable development.[135]

Another notable example of regional interstate coordination in CEI protection includes the CIS Anti-Terrorist Center’s Methodological Recommendations (2019). This document, already referenced here, exemplifies collaborative efforts to enhance the security of CEI.

[133] See pages 36-46: https://paodkb.org/uploads/publication/file/45/sbornik_5_december_2022.pdf.

[134] Memorandum of Understanding on the Trans-ASEAN gas pipeline project, 2021, available at https://asean.org/wp-content/uploads/2021/08/ASEAN-MoU-on-the-Trans-ASEAN-Gas-Pipeline.pdf-

[135] Ivo Walinga, *OSCE activities on Critical Energy Infrastructure Protection*, 2020, available at https://www.energycharter.org/fileadmin/DocumentsMedia/Forums/2-3_-_Critical_Infrastructure_Mr_Walinga.pdf.

Tool 7

Commonwealth of Independent States Anti-Terrorism Center (CIS ATC) 2019 Methodological recommendations for organizing interaction between security agencies, special services and law enforcement agencies of the CIS member states to ensure anti-terrorist protection of critical energy facilities

The Methodological Recommendations provide guidance for preparing and conducting both national and international anti-terrorism exercises focused on energy infrastructure. The document outlines indicators to monitor terrorist activities targeting energy and nuclear facilities. Beyond economic and demographic indicators, it includes comprehensive quantitative and qualitative parameters related to the preparedness of military, law enforcement and other specialized agencies for potential attacks on cross-regional energy infrastructure. Notably, the ATC CIS is tasked with monitoring indicators related to subregional energy supply protection, considering the cross-regional interdependence within the energy sector.

Source: Materials the governing staff of bodies security and special services of states — participants of the CIS: Collection of materials – M.: Publishing house "Print Torg", 2019. – 362 p.

Tool 8

OSCE Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace

This publication aims to provide a framework that encourages the formulation and implementation of appropriate policies and institutional management of information security related to CEI, based on a cooperative, integral (all-hazard) and risk-based approach and with an emphasis on achieving incident response preparedness, overall infrastructure resilience and energy reliability.

The Guide's goal is to assist countries with identifying and countering terrorist threats using ICTs, highlight methodological issues that need to be taken into account for the protection of non-nuclear CEI and offer suggestions for good practices to mitigate potential vulnerabilities. Furthermore, the Guide describes measures that may be adapted, extended and/or applied to other threats and other sectors. The publication includes worldwide practices on risk assessment, physical security, information security, contingency planning, PPPs, community engagement and international/cross-border cooperation on non-nuclear energy facility protection.

Source: https://www.osce.org/files/f/documents/4/b/103500.pdf.

Case Study 16

Asia-Pacific Economic Cooperation (APEC) Oil and Gas Security Exercises

Following the 10th APEC Energy Ministerial Meeting in St. Petersburg, Russia, in June 2012, member states tasked the Asia Pacific Energy Research Centre (APERC) with conducting regular Oil and Gas Security Exercises (OGSEs). These exercises aim to enhance regional collaboration by developing comprehensive response measures, including policies and institutional frameworks, to effectively address oil and gas supply disruptions and infrastructure damage.

Inaugurated in 2014, the OGSEs have been conducted in seven member countries, each featuring unique, carefully designed scenarios. For example, the 2019 OGSE in Chile simulated an explosion on the Concón-Maipú liquid products pipeline, resulting in a severe disruption of oil product supply, particularly affecting Santiago and its surrounding areas. These exercises have led to notable improvements in threat assessment procedures and the development of emergency response plans for both public and private stakeholders.

The most recent OGSE occurred in Thailand in September 2023. One scenario involved a major fire at the Thai Oil refinery, which required a coordinated emergency response from all stakeholders to maintain the functionality of energy-dependent economic sectors.

Source: https://aperc.or.jp/reports/ogsi.php.

5.2. International inter-agency coordination and cooperation

Given the cross-border nature of energy infrastructure, international cooperation is essential for its effective protection against terrorist threats. For instance, a pipeline that extends across multiple countries is subject to varying regulatory regimes, necessitating coordinated efforts among the involved nations to ensure comprehensive security.

5.2.1. Factors necessitating international cooperation in CEI protection

Potential scenarios demonstrating the need to integrate international cooperation into Member States' CIP strategies include:

- Shared infrastructure: When two or more countries host the same type of CI facilities, such as the Langeled underwater gas pipeline between Norway and the United Kingdom, or the Balticconnector underwater natural gas pipeline between Finland and Estonia.
- Dependence on foreign resources: When energy infrastructure in one country relies on products, services or technologies supplied by another country, as seen with the Baku-Tbilisi-Ceyhan pipeline.
- Cross-border impact: When issues or disruptions in an energy infrastructure located in one country affect neighbouring countries, particularly those sharing a border.

5.2.2. Forms and mechanisms of international cooperation on energy infrastructure protection

Forms and mechanisms of international cooperation to protect CEI vary significantly. Common forms of interstate cooperation aimed at preventing, detecting, and responding to terrorist acts against CEI include:

- Information-sharing and awareness measures: Facilitating the exchange of relevant information and raising awareness about potential threats.
- Collaboration in intelligence operations: Coordinating efforts to prevent, identify, and suppress terrorist activities within the energy sector.
- Joint measures against terrorism financing: Cooperating to prevent and address the financing, supply, and acquisition of weapons and ammunition used in terrorist acts.
- Harmonization of legal frameworks: Aligning national counter-terrorism laws and sharing regulatory information and practices related to counter-terrorism efforts.
- Exchange of expertise: Sharing knowledge and experience in preventing, identifying or addressing terrorist activities in the energy sector.
- Coordinated crisis communication: Enhancing communication and coordination during crises and emergency responses to terrorist attacks on cross-border energy infrastructure.
- Joint training and education programmes: Developing and participating in training programmes focused on the protection of CEI.

While these forms of international cooperation are not exclusively dedicated to CEI protection, they are crucial components of state responses to terrorist attacks on energy facilities.

Additionally, Member States often conduct joint patrols in border areas or maritime regions near oil platforms and pipelines. For example, Azerbaijan, Turkey and Georgia have coordinated efforts to safeguard the Baku-Tbilisi-Ceyhan pipeline. Similarly, Tanzania and Zambia have engaged in bilateral cooperation to enhance pipeline security against terrorism.[136]

International cooperation on legal frameworks is also crucial for protecting CEI from terrorism. Harmonizing legislation across countries can ensure that terrorism-related offenses are defined consistently, aligning with international counter-terrorism standards. This approach helps prevent situations where the same attack on an energy facility might not be classified as terrorism in some jurisdictions.

An example of such harmonization is the CIS Interparliamentary Assembly's “Model (Benchmark) Antiterrorism Legislation”. This initiative aims to standardize legal frameworks across Commonwealth countries, including those related to energy infrastructure security. The model legislation provides specific measures for protecting energy facilities from terrorist threats, aligning with the CIS Model Law “On Countering Terrorism,” particularly Article 12.[137]

[136] Available at https://www.aa.com.tr/en/africa/zambia-tanzania-agree-to-enhance-security-on-jointly-owned-oil-pipeline/2941120.
[137] CIS Model Law “on Countering Terrorism”, available at: https://www.cisatc.org/1289/9115/135/9126/9129/249.

Case Study 17

Petrol and Critical Infrastructures Protection Committee of the Gulf Cooperation Council (Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, the United Arab Emirates)

Given the importance of safeguarding national assets, particularly oil sites, the Ministers of Member States of the Gulf Cooperation Council (GCC) established the Petrol and Critical Infrastructure Protection Security Committee, which convenes annually.

The committee coordinates counter-terrorism activities across several key areas:

- Training and development: Developing and delivering specialized training programmes for security personnel, focusing on the protection of vital petroleum infrastructure in the context of contemporary security challenges.
- Educational resources: Preparing educational materials and establishing training institutions across GCC Member States.
- Information exchange: Facilitating the exchange of scientific and expert knowledge related to the protection of CEI from unlawful acts.

In alignment with the committee's objectives, national security educational and training institutions within GCC Member States conduct annual group field visits for officers and students.

Source: https://www.gcc-sg.org/en-us/CooperationAndAchievements/Achievements/SecurityCooperation/Achievements/Pages/Twelftheducationandsecuritytra.aspx.

5.3. Joint exercises and training

The cross-border nature of terrorist threats requires extensive international cooperation. This includes not only joint operations and patrols but also the sharing of knowledge, joint expertise and training programmes for security personnel. Furthermore, international collaboration extends beyond governmental bodies to encompass mutual training for non-governmental stakeholders and civil society.

5.3.1. International training courses

International training courses are essential for enhancing the capacity of agencies to secure critical energy facilities. These programs facilitate cross-border knowledge transfer, equipping agencies with the expertise needed to address evolving threats and ensure global energy security. By enabling the sharing of best practices and cutting-edge techniques, such programs strengthen energy security and mitigate vulnerabilities. They play a crucial role in enhancing both national and international energy security capabilities, serving as building blocks for a global defense system against terrorist threats to CEI. These courses highlight the collective responsibility of nations to share knowledge and expertise for a more secure energy future.[138]

[138] A notable example is the "Physical Security of Critical Energy Infrastructure" course and expert workshop organized by the Florence School of Regulation in 2024. This event aimed to assess current challenges in the physical protection of critical energy infrastructure and explore strategies for enhancing such protection. Available at https://fsr.eui.eu/event/the-physical-security-of-critical-energy-infrastructure/.

5.3.2. Joint counter-terrorism exercises

Joint counter-terrorism exercises are crucial for sharing practical experience and fostering direct cooperation among stakeholders in CEI protection. These exercises help master joint procedures for emergencies and address cross-border coordination challenges. Typically, joint CEI exercises are tactical and involve simulations of unlawful acts targeting energy facilities that are either cross-border or located near national boundaries.

Such interstate counter-terrorism exercises provide several benefits:

- Objective assessment: They allow for an objective evaluation of counter-terrorism security at key national CEI sites.
- Mechanism development: They help develop and refine mechanisms for coordination between special forces and security services during response operations against terrorist threats.
- Skill enhancement: They improve the use of collective interstate information and communication systems.

Case Study 18

Joint counter-terrorist exercises of the CIS ATC

In 2021, the joint counter-terrorism exercises "Caspian-Antiterror" were conducted to identify signs of terrorist activity and suppress attacks on maritime infrastructure and the oil and gas industry. These exercises were simultaneously held across eight Commonwealth countries: Armenia, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, and Uzbekistan.

In 2019, the "Ararat-Antiterror" exercises focused on training tasks at a nuclear power plant, involving seven CIS countries. Similarly, in 2016, the "Information Security Antiterror" exercises, which included nine Commonwealth countries, centred on a thermal power plant for training purposes.

These exercises highlighted the importance of cooperation between national authorities and law enforcement agencies. Organized by the CIS ATC, these activities have enabled:

- Enhanced cooperation in detecting and suppressing terrorist offenses at critical energy facilities
- Strengthened skills in using common information systems among CIS security agencies
- Sustained high levels of collaboration between operational security units

Source: https://eng.cisatc.org/1289/133/161/9077.

Case Study 19

International joint exercises "ADMM-Plus Maritime Security Field Training Exercise"

The 2019 joint exercises co-organized by Singapore and the Republic of Korea, involved security forces from 18 countries working together to address the threat of a maritime terrorist attack on an oil rig near Busan. The scenario simulated an intrusion into an energy facility, represented by the ROKS Cheonjabong, which was used as a stand-in for an oil rig, by a group of intruders arriving via vessels.

During the exercise, participating navies conducted various maritime security drills, including boarding operations and protection of key installations. They practiced the Code for Unplanned Encounters at Sea (CUES, 2014) and engaged in information-sharing to track vessels of interest. The drills also included helicopter cross-deck landings and replenishment at sea, enhancing confidence and practical cooperation among the forces.

Upon reaching the waters off eastern Singapore, boarding teams from the navies of Brunei, India, the Republic of Korea and Singapore simulated a search of a vessel of interest. ADMM-Plus ships were then activated to regain control, intercept hostile vessels surrounding the key installation, and recover the oil rig crew, who had been forced to jump overboard.

Source: https://www.mindef.gov.sg/web/wcm/connect/mindef/14d67a7b-f7a4-473c-958b-0ae2093590a0/Infographic.pdf?MOD=AJPERES&CVID=mGI0R7G.

Case Study 20

Computer-assisted Command and Staff Exercises – "Eternity-2023"

The international exercise "Eternity-2023," held in Baku, involved Azerbaijani, Georgian and Türkiye law enforcement officers. The primary goal was to enhance mutual cooperation and ensure interoperability in countering terrorist threats to strategically important facilities, including the CEI of the Baku-Tbilisi-Ceyhan pipeline. The scenario for the exercise centred on organizing the protection of the BTC oil pipeline during a crisis. The Azerbaijan-Georgia-Türkiye trilateral training is conducted annually on a rotating basis across the three countries.

Source: https://mod.gov.az/en/news/eternity-2023-computer-assisted-command-and-staff-exercises-held-in-baku-ended-video-49709.html.

5.4. Networking and information-sharing in the context of CEI protection

5.4.1. Types of information that could be shared at the interstate level

Increasing international cooperation, knowledge and information-sharing on CEI is essential for its effective security. Information-sharing related to energy infrastructure protection can be categorized into two types: incident-related and non-incident-related. The former involves the urgent, timely exchange of information during incidents, while the latter pertains to strategic, analytical data.

Since CEI protection is often coordinated by state authorities, information-sharing typically occurs between law enforcement, justice ministries and agencies and specialized security organizations. However, information-sharing should also be established among domestic energy infrastructure operators and entities from multiple countries.

Types of information that could be shared on an interstate level to enhance counter-terrorism activities and CEI protection include:

- Best practices for preventing and responding to terrorist threats at various types of energy facilities, such as methods and tactics for counter-terrorism operations and response plans for immediate victim support.
- Legal information, including electronic evidence for investigations of terrorist-related attacks on CEI, with due regard for fair trial guarantees and human rights.
- Information related to the financing of terrorist groups.
- Various types of intelligence information.

While this list is not exhaustive, these categories represent key areas for information exchange to strengthen counter-terrorism efforts and CEI protection.

5.4.2. Intelligence information-sharing in prevention and suppression of terrorism on critical energy facilities.

International intelligence information-sharing aims to enhance situational awareness regarding significant events or activities of international terrorist groups. In the context of CEI protection, intelligence-sharing can include information on:

- The movement and activities of transnational terrorist groups involved in attacks on energy facilities.
- Individuals and groups suspected of engaging in terrorist activities.
- Identified patterns and methods of both executed and planned terrorist attacks on energy infrastructure.
- Any other information of mutual interest.

Enhancing counter-terrorism capabilities for CI, including energy, through intelligence-sharing is a key effort of INTERPOL.[139] INTERPOL enjoys a unique position to provide a global and neutral law enforcement platform bringing together experts, governments, industry, academia and private sector to help member countries address these emerging threats.[140]

Given the crucial role of intelligence agencies in identifying patterns of terrorist activities that may seem insignificant in isolation, it is vital to provide a comprehensive view of what international terrorist groups are planning against energy infrastructure. It is essential to consider, including from a human rights perspective, the sensitive nature of the shared intelligence, including how it was gathered and its intended use.

5.4.3. Expert, research networking and international comprehensive capacity-building programmes

Policymaking for CEI protection should be supported by expert and scientific evidence to enhance its effectiveness, as it demands high levels of expertise across various domains. While protecting critical energy facilities is a priority for many countries, not all have the necessary resources and multidisciplinary skills readily available. Thus, knowledge-sharing and expert support through international collaboration are crucial.

Expert and research support for international cooperation on CEI protection is important for several reasons:

- Developing a common understanding of terrorist threats, trends and evolving methods of operation.
- Promoting scientific research on terrorist attacks against CEI.
- Establishing common terminology and definitions related to counter-terrorism activities on energy infrastructure.
- Sharing good practices for identifying suspicious activities related to terrorism.

A notable example of expert support and knowledge-sharing is the work of the non-state organization "Research Institute for CIS Security Problems," which has organized several international workshops and conferences on security issues related to oil and gas infrastructure, in collaboration with leading industry universities in Eastern Europe and Central Asia.[141]

In some cases, international expert and research cooperation may include joint training as a crucial component. For example, the Kuwait-USA joint expert collaboration from 2018 to 2019 involved comprehensive training sessions, data-sharing, and awareness-raising on terrorist threats related to oil and gas facilities.[142]

[139] The protection of critical infrastructures against terrorist attacks: Compendium of good practices, 2018, available at https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf.
[140] Ibid.
[141] Available at https://spi-cis.ru/deyatelnost/nauchnaya/.
[142] Available at https://nps.edu/web/eag/kuwait-energy-infrastructure.

5.4.4. Sensitive information securing

Information and data-sharing, a crucial aspect of interstate cooperation in energy facility protection, faces the challenge of safeguarding sensitive information. Interstate information-sharing encounters risks related to the confidentiality and security of information. Both accidental and intentional disclosures of classified intelligence can significantly undermine the effectiveness of intelligence services and other institutions.

To facilitate secure information-sharing, national agencies, law enforcement bodies and CEI operators must trust that their sensitive information is managed, stored and protected from unauthorized disclosure. Therefore, information-sharing should adhere to standardized mechanisms and protocols designed to safeguard and exchange CI information effectively. For instance, the Oil and Gas Sharing and Analysis Center (ONG-ISAC) employs the Traffic Light Protocol (TLP) for information-sharing, allowing members to share information either anonymously or with attribution.[143] Only ONG-ISAC members receive information that is classified as TLP Green, Amber and Red; non-members only receive information that is classified as TLP Clear.[144]

[143] Traffic Light Protocol was created to facilitate greater sharing of potentially sensitive information and more effective collaboration. Information-sharing occurs from one information source towards one or more recipients. TLP is a set of four labels used to indicate the sharing boundaries to be applied by the recipients.

[144] Available at https://ongisac.org/.

6. Renewable and non-traditional energy infrastructure protection

6.1. Terrorist threats to renewable energy infrastructure

6.1.1. Renewable energy infrastructure as a terrorist target

As modern societies increasingly rely on renewable energy infrastructure, these facilities become more attractive targets for terrorist attacks. For example, in 2023, the MGM Mega Solar Array facility in the USA was shut down following an incident considered a terrorist attack. An intruder crashed his car into the solar generator's transformer and then set the vehicle on fire.[145]

Renewable energy infrastructure often consists of large, geographically dispersed facilities equipped with advanced technology. For instance, wind farms may feature hundreds of turbines and cover vast areas spanning hundreds of square kilometers.

Offshore wind farms, in particular, are increasingly attractive targets for hostile entities. Their extensive size and remote location in open seas present numerous security challenges. Consequently, these facilities require continuous surveillance and comprehensive detection systems to monitor approaching surface and underwater threats.

6.1.2. Renewable energy infrastructure specific vulnerabilities

Renewable energy facilities are increasingly monitored and controlled using remote tools and applications, which rely heavily on the stability of information infrastructure. For instance, in recent years, the wind energy sector has faced attacks using ICTs that impacted its ability to monitor and manage wind turbines. In March 2022, a German wind turbine manufacturer had to shut down its IT systems across multiple locations and business units following one of these attacks. The incident was detected early by the IT security team, and response measures were promptly implemented. Authorities and emergency response personnel conducted extensive investigations and forensic analyses.

Due to the high level of interdependence in renewable energy systems, successful terrorist attacks can lead to significant disruptions and cascading failures. These attacks can affect not only the computer systems and physical components of wind energy facilities but also undermine the reliability of the entire electric grid.

[145] Available at https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/fbi-joins-investigation-into-alleged-terror-attack-on-las-vegas-solar-plant-73776901.

Similar to conventional energy facilities, renewable energy infrastructure is vulnerable to both ICT-based attacks and blended physical/ICT-based attacks. For example, a substation might have two separate SCADA networks: one for managing wind turbine operations and another for controlling the collection and injection of power into the grid. This segmentation can increase vulnerability to both physical and ICT-based attacks, potentially disrupting or distorting communication channels.

6.1.3. Facility-specific measures of protection

Physical and information security measures for renewable energy infrastructure often resemble those used for traditional energy facilities. However, there are notable exceptions and nuances due to the specific characteristics of these facilities.

While renewable energy infrastructure is a critical component of many countries' energy systems, it does not always adhere to the same stringent norms and standards as traditional energy facilities. This discrepancy can be attributed to a lower perceived threat level and the evolving nature of national protection practices. For example, experts from Sandia National Laboratories (USA) have highlighted a lack of standards for information technology-related equipment, security requirements for data-in-transit and certification protocols within the solar energy sector.[146]

Given the large scale of many renewable facilities, such as solar plants, traditional surveillance and intrusion detection technologies can become very expensive. Additionally, conventional detection tools like radars face challenges; for example, the movement of turbine blades can obstruct or interfere with radar beams, limiting their effectiveness.[147] Therefore, using fences equipped with intrusion detection sensors around facility perimeters, as demonstrated at the Hungarian Tázlár Solar Park, can be an effective and cost-efficient measure for enhancing physical security.

New technologies are also contributing to the protection of these facilities. For example, infrared sensors are a specific type of motion sensors that use infrared radiation. They could be used to provide surveillance and detection as an integral part of physical security of offshore wind farms. Furthermore, in many cases, these detection systems are accompanied with AI technologies to provide automatic recognition and classification of threats, smart alarm filtering and automatic responses (making screenshots, video, etc.).[148]

[146] Johnson Jay, Roadmap for Photovoltaic Cyber Security, Report number: SAND2017-13262, 2017, available at https://www.researchgate.net/publication/322568290_Roadmap_for_Photovoltaic_Cyber_Security.

[147] Available at https://www.roc.noaa.gov/wsr88d/windfarm/turbinesimpacton.aspx.

[148] For example: https://hgh-infrared.com/offshore-windfarm-security.

Box 8

Wind farm protection measures against malicious information and communications technology activities

According to studies on attacks on wind farms,[149] access vectors that terrorists might exploit to launch attacks using ICTs include:

- Physical access to wind turbines or collector substations.
- Remote access to information systems.
- Targeting transient information and communication assets, which may be classified as physical, informational or combined information-physical attacks depending on the method of compromise.

To mitigate these risks and safeguard wind farms from malicious ICT use, some of the following measures could be implemented:

- Physical security measures:
  - Equip each turbine with robust locking mechanisms, multi-factor authentication, motion sensors, security cameras and remote alarm notifications.
- Information security measures:
  - Isolation of turbines: Ensure turbines are isolated when turbine-to-turbine communication is not necessary.
  - System hardening: Disable unnecessary remote management interfaces.
  - Improved information security policies and procedures: Strengthen policies and procedures to enhance overall security.

Source: Staggs, Jason & Ferlemann, David & Shenoi, Sujeet. (2017). Wind farm security: Attack surface, targets, scenarios and mitigation. International Journal of Critical Infrastructure Protection. 17. 10.1016/j.ijcip.2017.03.001. https://www.researchgate.net/publication/315590797_Wind_farm_security_Attack_surface_targets_scenarios_and_mitigation.

6.2. Nuclear energy infrastructure protection from terrorist attacks

Attacks on nuclear energy facilities fall within the broader scope of nuclear terrorism risks. Such attacks are particularly alarming due to their potential for significant intimidation, which increases their attractiveness as targets for terrorists.

[149] Sarah G. Freeman, Matthew A. Kress-Weitenhagen, Jake P. Gentle, Megan J. Culler, Megan M. Egan, Remy V. Stolworthy Attack Surface of Wind Energy Technologies in the United States, 2024, available at https://inl.gov/content/uploads/2024/02/INL-Wind-Threat-Assessment-v5.0.pdf?utm_medium=email&utm_source=govdelivery.

In the preamble to the International Convention for the Suppression of Acts of Nuclear Terrorism (2005), Member States acknowledged that "acts of nuclear terrorism may result in the gravest consequences and may pose a threat to international peace and security". The preamble also emphasized the urgent need to enhance international cooperation among states to devise and implement effective measures for preventing such acts of terrorism and for prosecuting and punishing their perpetrators.

The motives behind terrorist attacks on nuclear plants are often driven more by the potential for catastrophic consequences rather than merely disrupting the supply chain.

6.2.1. Specific terrorist-related threats to nuclear power plants

The principal attractiveness of nuclear energy facilities as terrorist targets lies in the potential for creating a release of radioactivity large enough to produce significant casualties and land contamination. For example, in 2016 two nuclear power plants in Belgium were locked down under suspicion of an attempt by ISIL (Da'esh) to attack, infiltrate or sabotage the facilities to obtain nuclear and radioactive materials.[150]

The main international legal instruments in the area of nuclear security adopted under the auspices of the International Atomic Energy Agency (IAEA) are the Convention on the Physical Protection of Nuclear Material (CPPNM) and its 2005 Amendment.[151] These documents were crucial milestones in the development of the international legal framework for nuclear security, as they remain the only internationally legally binding undertakings in the area of physical protection of nuclear material and of nuclear facilities used for peaceful purposes. The CPPNM and its Amendment establishes legal obligations for parties regarding the physical protection of nuclear material used for peaceful purposes.

In accordance with international standards for protection against physical attacks, such as explosions and bombings, nuclear power plant operators have significantly enhanced their security measures. They have developed advanced security barriers, including entry barriers, multiple fences and structures resistant to physical impacts. Counter-terrorism measures at nuclear power plants include a dedicated contingency response force, biometric and other sophisticated access control systems, illuminated detection zones and a variety of intrusion detection aids. These aids include different types of detection fields, closed-circuit television systems and alarm/alert devices, as well as bullet-resistant barriers in critical areas.

Despite these high levels of protection against external attacks, nuclear facilities remain vulnerable to insider threats. The technological complexity of nuclear energy facilities highlights the crucial need for extensive knowledge of their operational principles and security practices. Terrorists would likely require insider knowledge to disable reactor controls and multiple security systems simultaneously. For instance, in 2024, the Royal Canadian Mounted Police arrested a former Ontario Power Generation employee for allegedly communicating safeguarded information about a nuclear plant to a terrorist group or foreign state.[152]

[150] Belgium evacuates nuclear plant staff after attacks / CBS news. URL: https://www.cbsnews.com/news/belgium-attacks-evacuation-tihange-nuclear-plant-staff-isis-dirty-bomb.

[151] Convention on the Physical Protection of Nuclear Material (CPPNM) and its Amendment, available at: https://www.iaea.org/publications/documents/conventions/convention-physical-protection-nuclear-material-and-its-amendment.

[152] Available at https://www.power-eng.com/news/ex-ontario-power-generation-employee-accused-of-sharing-information-with-foreign-entity-or-terrorist-group/#gref.

To deter threats, many Member States require nuclear plant employees to undergo criminal background checks and complete various security tests. Some facilities also enforce a "two-person rule," which prohibits employees from working alone in certain high-security areas of the nuclear power plant.

A notable example of an insider threat occurred in Belgium at the Doel nuclear plant in 2014.[153] An intruder entered Reactor No. 4 at the Doel nuclear plant and turned a valve, draining 65,000 litres of oil used to lubricate the turbines. This action caused significant friction, nearly overheating the machinery and forcing a shutdown. The damage was so severe that the reactor was out of commission for five months.

Additionally, nuclear plants are managed by information control systems, making them vulnerable to ICT-based attacks. An illustrative example occurred in 2019 at the Kudankulam Nuclear Power Plant, where malicious activities were detected in the ICT systems. It was later revealed that the logs included data from a compromised machine belonging to an employee.[154]

Nuclear facilities that could be targets include not only plutonium-production reactors but also associated spent-fuel-storage and fuel-reprocessing facilities. These locations are attractive targets for malicious acts due to the hazardous substances stored and handled there.

Additionally, the transportation of nuclear and other radioactive materials is also vulnerable to terrorist attacks. According to the ITDB factsheet, 52% of all reported thefts since 1993 have occurred during the authorized transport of radioactive materials.[155] International cooperation and joint training exercises on the transportation of nuclear and other radioactive materials is thus crucial. For example, Morocco and Spain conducted a joint tabletop and field exercise (“Gate to Africa”) on terrorist threats to the transportation of radioactive material in 2015. The joint exercise aimed to examine national nuclear security arrangements and capabilities in terms of event prevention, detection, protection and response during the sea transport of radioactive materials, and to discuss and practice responses to terrorist events involving radioactive materials.[156]

6.2.2. Nuclear facilities protection practices.

The IAEA plays a central role in setting international standards and norms for protecting nuclear power plants against both physical and ICT-based attacks. Key legal frameworks for international nuclear facility protection against terrorism and other illicit actions include:

- Convention on the Physical Protection of Nuclear Material (including its 2005 Amendment)
- International Convention for the Suppression of Acts of Nuclear Terrorism
- United Nations Global Counter-Terrorism Strategy
- United Nations Security Council Resolutions 1373 (2001), 1540 (2004) and 2325 (2016)
- Code of Conduct on the Safety and Security of Radioactive Sources

153 Available at https://www.brusselstimes.com/181163/enquiry-into-nuclear-plant-sabotage-comes-to-no-conclusion.
154 Breach at Kudankulam nuclear plant may have gone undetected for over six months, available at: https://economictimes.indiatimes.com/news/politics-and-nation/breach-at-kudankulam-nuclear-plant-may-have-gone-undetected-for-over-six-months-group-ib/articleshow/79412969.cms?from=mdr.
155 Available at https://www.iaea.org/resources/databases/itdb.
156 For more information: https://amssnur.org.ma/wp-content/uploads/2020/11/Gate-to-Africa-report.pdf.

The IAEA Nuclear Security Series of publications further supports these frameworks by offering best practices, technical guides, training manuals and other resources to assist Member States. Other relevant initiatives of the IAEA include their Nuclear Security Training and Demonstration Centre (NSTDC), opened at the IAEA's laboratories in Seibersdorf in 2023. The NSTDC supports countries in building capacity to combat nuclear terrorism and manage complex nuclear security challenges, offering specialized training, research, and development for projects requiring advanced technical infrastructure.[157]

Through its Global Programme on Countering the Terrorist Use of Weapons, UNOCT/UNCCT has been supporting Member States' efforts to counter nuclear terrorism through a dedicated portfolio of training activities, including on CIP, and technical assistance in the implementation of the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT, 2005).[158]

In order to provide member countries with information related to their investigation of terrorist and criminal acts involving radiological and nuclear materials, INTERPOL established the Geiger database and Incident and Trafficking Database (ITDB) (https://www.iaea.org/resources/databases/itdb). It is an analytical platform that collates law enforcement data on incidents involving radiological or nuclear material. It is used for analyzing patterns and trends, risks and threats, routes and methods, weakness and vulnerabilities, and contributes to the publication of INTERPOL notices and the CBRNE Bi-Monthly Digest.[159]

While international efforts have led to a complex set of strict standards and requirements, many Member States develop nation-specific tools and measures for nuclear safety. For instance, Japan's Nuclear Regulatory Authority mandates that local governments create evacuation plans for citizens living within a 30-kilometre radius of a nuclear power plant in the event of an emergency. This requirement is in addition to international standards on civil nuclear safety.

In some Member States, a specialized government body is established to coordinate nuclear plant protection and implement a whole-government approach. For example, the Indian government established the Council of Nuclear Safety in 2015, which operates under the stewardship of the Prime Minister.[160]

Another measure for protecting critical nuclear facilities is the establishment of specialized security forces or armed rapid response teams at the state level. For example, in the United Kingdom, the Civil Nuclear Constabulary serves as a dedicated armed force responsible for defensive duties at nuclear sites like Sellafield and Dounreay. Additionally, this force has the authority to make arrests at non-nuclear locations such as ports, airports and railway stations.[161] The constabulary also conducts patrols up to three miles from nuclear sites and has the authority to stop and search individuals and vehicles.

[157] For more information: https://www.iaea.org/about/organizational-structure/department-of-nuclear-safety-and-security/division-of-nuclear-security/iaea-nuclear-security-training-and-demonstration-centre.
[158] For more information: https://www.un.org/counterterrorism/cct/chemical-biological-radiological-and-nuclear-terrorism.
[159] https://www.interpol.int/Crimes/Terrorism/Radiological-and-Nuclear-terrorism/Our-response-to-radiological-and-nuclear-terrorism.
[160] Nuclear security in India, 2015, available at https://www.orfonline.org/wp-content/uploads/2015/02/NUCLEAR_SECURITY_IN_INDIA.pdf.
[161] Available at https://www.gov.uk/government/organisations/civil-nuclear-constabulary/about.

Annex 1

Examples of Good Practices Included in the Guide

Thematic area	International Good Practices	Description	Page Index
Legal framework	Integration of CEI protection into the national security policy	Listing the CEI protection among national security priorities to strengthen coordinated efforts and inter-agency cooperation	Pages 24-25
	Defining energy sector stakeholders, including the distribution of the relevant roles and responsibilities	National regulations to outline clear criteria for categorization of CEI stakeholders and their areas of roles and responsibilities in energy infrastructure safety and security	Page 27
	Defining criticality criteria for energy infrastructure	Legal frameworks to provide energy sector-specific criticality criteria for energy facilities, sites and assets using qualitive and quantitative indicators at the state (federal), regional (provincial) and local (municipality) levels	Pages 27-32
	Special requirements for the design, construction, operation and maintenance of CEI	CEI regulators elaborate standards or building codes for the design, construction, operation and maintenance of different types of energy infrastructure, including electrical facilities, to ensure a high level of security	Page 33
	Establishing industry-specific counter-terrorism security standards	National counter-terrorism law to provide security standards, inter alia, for energy sector infrastructure, including for different types of energy facilities and assets	Pages 33-34
Risk Management	Security certificates (“security passport”) of CEI	A "security passport" is a security planning document developed for each critical facility and/or asset of energy infrastructure and contains detailed information, including on potential socioeconomic impact of unlawful interference, specific security measures, emergency management plan, etc.	Page 35
	The “BCK” risk analysis model	A special risk analysis tool comprising multidimensional risk factor identification, event tree, knowledge graphs and tools to evaluate security risks, including terrorism related risks, on a critical energy facility or asset	Page 50

Thematic area	International Good Practices	Description	Page Index
	Attack modelling aligned with risks identified	Employing a structured methodology to model potential terrorist attacks on CEI, including attack typology, target identification, perpetrators identification, resource assessment and other stages	Page 54
Information security	Industry rules and standards for handling sensitive energy information	Development of clear rules and standards for the industry for handling sensitive energy information, including on vulnerabilities, threats, location, design, etc., to mitigate physical and information security risks	Page 35
	Computer Security Incident Response Teams for CEI	Establishment of specialized centres to collect data and report on each information security incident at critical energy facilities, including ransomware, phishing and other similar threats	Pages 58-60
	Integrated Data Security Systems for CEI	The Critical Infrastructure Security Data System contains computerized records of the security conditions of CI, including energy facilities across the national territory. This system encompasses the collection, processing, storage and retrieval of information	Page 60
	Laboratories on ICT-risk modelling in critical oil and gas facilities	Utilization of both software and hardware tools and a "digital twin" of typical information processes in an oil and gas company to simulate various types of ICT-based attacks	Page 60
	Traffic Light Protocol	Traffic Light Protocol, a system for classification of sensitive information, is also used in the energy industry to provide guidance for handling unclassified data to promote greater information exchange and ensuring that information is shared with the appropriate audience	Page 77
Physical Security	Infrared Sensors-Based Surveillance System	The Infrared Sensors-Based Surveillance System utilizes infrared radiation to provide uninterrupted surveillance and detection capabilities for offshore wind farms, effectively detecting maritime threats such as small boats without automatic identification systems and functioning well in corrosive maritime environments	Page 79
	Safety zones around critical oil/gas facilities	Establishment of special regulation to oblige CEI operators/owners to create zones around oil/gas facilities with additional security requirements as rules of authorization of persons, and transit accessibility	Page 34

Thematic area	International Good Practices	Description	Page Index
	Maritime patrol near offshore energy infrastructure	Physical security of offshore oil and gas infrastructure could be ensured through active patrolling of an area by patrol boats called “rapid support vessels”	Page 56
	Intrusion detection sensors	The deployment of perimeter fencing equipped with intrusion detection sensors, such as fibre-optic cable, around oil and gas facility or along pipelines constitutes an effective method for enhancing physical security of CEI	Pages 58, 79
	Detection systems with AI technologies	CEI detection sensors, integrated with AI technologies, enable the automated recognition and classification of threats, intelligent alarm filtering and automated response mechanisms such as screenshot and video capture	Page 79
	Physical Security Information Management (PSIM)	PSIM as a 3D visualization tool to design physical protection systems on CEI. This tool is aimed at enhancing operational security measures and select cost-effective methods to protect energy facilities	Page 53
Operational framework	Oil and gas security exercises	Oil and gas security exercises aim to enhance regional collaboration by developing comprehensive response measures, including policies and institutional frameworks, to effectively address oil and gas supply disruptions and infrastructure damage	Page 70
	Specialized security body with responsibility for the protection of CEI	Designating a special security unit within a responsible ministry to provide protection of critical facilities of the energy sector	Pages 40-41
	Energy sector stakeholders’ network managed by the designated government entity	Developing a collaborative approach for effective information-sharing for energy infrastructure protection to facilitate the exchange of data, knowledge and expertise among private and public energy sector stakeholders	Pages 42-43
	Regular contingency-based exercises	Conducting contingency-based exercises by PPPs to establish preparedness for the implementation of appropriate countermeasures in response to unforeseen disruptions	Page 47

Thematic area	International Good Practices	Description	Page Index
	"Whole-of-industry approach": engaging both private and public industry stakeholders in policymaking on CEI security	Involvement of private stakeholders in security standards development for CEI protection, when private sector stakeholders could suggest modifications to existing security standards, or government guidelines—for example, on safety-zone pipelines—within the framework of a transparent and consensus-driven process	Pages 44-45
Cross-border cooperation	Cross-border joint patrols	Implementing bilateral or multilateral armed maritime or foot patrols in border areas or maritime zones adjacent to oil platforms and gas pipelines	Page 71
	Cross-border counter-terrorism exercises on CEI protection	Conducting joint counter-terrorism exercises and manoeuvres to test and improve collaboration in emergency management	Page 73
	Harmonization of counter-terrorism legal frameworks for CEI protection	Harmonizing national counter-terrorism legislation and facilitating the exchange of regulatory information and practices pertaining to counter-terrorism measures within the energy sector	Page 71
	International training programmes for security personnel	Development and delivery of specialized courses on energy sector protection for security personnel to address new and emerging security threats and challenges	Pages 72-73

Annex 2

Recommendations on Countering Terrorism at the Energy Complex Facilities issued by the Collective Security Treaty Organization (CSTO), December 2022

Annex to
CSTO Parliament Assembly
Resolution No. 15-5.1
dd. December 5, 2022

RECOMMENDATIONS on countering terrorism at fuel-energy complex facilities (Unofficial translation)

1. General provisions

Recommendations on countering terrorism at energy facilities seek to formulate common approaches of the CSTO Member States to the legal regulation of countering terrorism at energy facilities.

1.1. Basic terms and definitions used in the current Recommendations

The following terms and their definitions are adopted for the purpose of the Recommendations:

- Anti-terrorism security of a fuel-energy complex facility means a state of a building, a structure, a construction or any other facility of the fuel-energy complex preventing commitment of a terrorist act.
- Safety exclusion area of a fuel-energy complex facility means a territory (water area) around an individual fuel-energy complex facility established by a government, within the boundaries of which measures aimed to provide special counter-terrorism protection regime of such facility are implemented.
- Categorization of a fuel-energy complex facility means the conduct of a set of events aimed at determining the compliance of a fuel-energy complex facility with the categorization criteria and their indicators.
- Critical facilities of the fuel-energy complex are the facilities of the fuel-energy complex, the disruption or termination of functioning of which will result in a decreased controllability or loss of control over the economy of a country, one or more administrative-territorial entities of the country, an industry or energy sector, a negative change (destruction) or a significant reduction of life safety of the population in the administrative-territorial entity.
- Critical element of the fuel-energy complex facility refers to potentially dangerous elements (sections) of a fuel-energy complex facility, which if the object of a terrorist act or other illegal action will result in termination of the normal functioning of the fuel-energy complex facility, its damage or an accident at the fuel-energy complex facility.
- Linear facilities of the fuel-energy complex refers to a system of linearly extended facilities of the fuel-energy complex (electric networks, main gas pipelines, oil pipelines and petroleum product pipelines) designed to provide transmission of electrical energy, transportation of gas, oil and petroleum products.

- Provision of anti-terrorism security of a fuel-energy complex facilities means implementation of a state-defined system of legal, economic, organizational, engineering, safeguarding and other measures aimed at preventing a terrorist act at the fuel-energy complex facilities.
- Fuel-energy complex facilities include facilities of the electric power industry, oil production, oil refining, gas production, gas processing, coal production, coal chemical, petrochemical, shale and peat industries, as well as petroleum product supply, heat supply and gas supply facilities.
- Anti-terrorism security certificate of a fuel-energy complex facility means a document containing information on anti-terrorism security of a fuel-energy complex facility.
- Potentially dangerous facilities of the fuel-energy complex include the facilities of the fuel-energy complex where explosive, flammable and hazardous chemicals are used, produced, processed, stored, transported or destroyed, as well as hydraulic structures, accidents at which, including those resulting from a terrorist act, can lead to emergencies with dangerous socioeconomic consequences.
- Potentially dangerous elements (areas) of a fuel-energy complex facility include territorially designated zones (areas), structural and technological elements of the fuel-energy complex facilities, accidents at which, including those resulted from a terrorist act or any other illegal action, can lead to emergency situations having dangerous socioeconomic consequences.
- Countering terrorism at the fuel-energy complex facilities includes activities of counter-terrorism entities aimed at preventing terrorism at the fuel-energy complex facilities, identifying, suppressing, solving and investigating a terrorist act and any other terrorist crimes at the fuel-energy complex facilities, minimizing and (or) eliminating the consequences of a terrorist act at the fuel-energy complex facilities.
- Physical protection system means a set of methods and means for ensuring the physical integrity of a fuel-energy complex facility, aimed at preventing a terrorist act or any other illegal action.
- Parties of counter-terrorism activities at the fuel-energy complex facilities include state authorities and local government and self-government bodies whose competence includes carrying out counter-terrorism measures, fuel and energy complex entities, public associations and other organizations, as well as citizens acting within the authority determined by the national legislation and providing assistance to the state authorities and local government and self-government bodies in countering terrorism at the fuel-energy complex facilities.
- Fuel-energy complex entities include individuals and legal entities who own the fuel and energy complex facilities by legal title or other legal right.
- Fuel-energy complex means a set of sectors of the state economy providing extraction, production, transportation, storage, processing and use of all types of energy resources, except for nuclear materials.
- Requirements on anti-terrorism security of fuel-energy complex facilities include the binding rules ensuring anti-terrorism security of the fuel-energy complex facilities.

Other terms used in the Recommendations shall be understood in accordance with their definitions established by the CSTO model laws and national legislation of a state.

1.2. Legal frameworks for countering terrorism at fuel-energy complex facilities

The legal frameworks for countering terrorism at the fuel-energy complex facilities include universally recognized principles and norms of international law, international treaties, other relevant sources of international law, the constitution of a state and other legal acts of a state.

1.3. Basic principles of countering terrorism at the fuel-energy complex facilities

The basic principles of countering terrorism at the fuel-energy complex facilities include:

1. Legitimacy.
2. Protection of human and civil rights and freedoms.
3. Objectivity, completeness and comprehensiveness in assessing terrorist threats.
4. Priority of measures aimed at preventing terrorism at fuel-energy complex facilities.
5. Integrated use of terrorism preventive measures.
6. Continued implementation of terrorism preventive measures.
7. Confidentiality of information on special means, techniques, tactics of counter-terrorism measures employed at fuel-energy complex facilities, as well as on the composition of their participants.
8. Scientific and technological support for the construction and operation of integrated and information security systems for fuel-energy complex facilities.
9. A combination of open and covert methods of countering terrorism at the fuel-energy complex facilities.
10. Efficient delineation of competence of parties of counter-terrorism activities at the fuel-energy complex facilities.
11. Unity of command in the management of forces and means involved in counter-terrorism operations.
12. Public awareness of an act of terrorism and conduct of counter-terrorism operations at the fuel-energy complex facilities.
13. International cooperation with other states and international organizations.
14. Inevitability of punishment for carrying out a terrorist act.
15. Minimized concessions to terrorists.

1.4. Goals and tasks of counter-terrorism activities at fuel-energy complex facilities

Countering terrorism at fuel-energy complex facilities is pursued for the purpose of sustainable and safe functioning of the fuel-energy complex, as well as to protect individuals, society and state interests against terrorism.

To achieve these goals, it is necessary to carry out the following:

1. Statutory regulation in the field of anti-terrorism security of fuel-energy complex facilities.
2. Elaboration and implementation of requirements on anti-terrorism security for fuel-energy complex facilities.
3. Elaboration and implementation of measures aimed at ensuring physical protection of fuel-energy complex facilities.
4. Categorization of fuel-energy complex facilities.
5. Identification of terrorist threats to fuel-energy complex facilities and their prevention.
6. Protection of state secrets in the field of anti-terrorism security of fuel-energy complex facilities and counteraction to foreign technical intelligence.
7. Specialists' training in the field of security of fuel-energy facilities.
8. Improvement of counter-terrorism intelligence operations of the competent state authorities.
9. Organization of preventive work of governmental bodies engaged in countering terrorism at fuel-energy complex facilities, jointly with personnel of fuel-energy complex facilities located in the territory of a state.
10. Organization of control and supervision over the implementation of laws in the field of anti-terrorism security of the fuel-energy complex facilities.

1.5. Categorization of fuel-energy complex facilities

The facilities are categorized in order to establish differentiated requirements on anti-terrorism security for fuel-energy complex facilities with due consideration of the degree of potential danger. The following is taken into consideration for the purpose of categorization:

1. Information on whether a fuel-energy complex facility is a critical facility and (or) a potentially dangerous facility.
2. The scale of possible socioeconomic consequences of a terrorist attack at a fuel-energy complex facility.
3. presence and state of security of critical elements of the fuel-energy complex facility.
4. Presence of potentially dangerous elements in the fuel-energy complex facility.
5. Presence of vulnerable spots at the fuel-energy complex facility.
6. Presence of components of the fuel-energy complex facility outside a common perimeter.
7. Presence of external threats of a terrorist act.

Basing on the categorization results, a fuel-energy complex facility is assigned to one of the following hazard categories:

- High danger (I category)
- Average danger (II category)
- Low danger (III category)

If a fuel-energy complex facility does not meet the hazard criteria and indicators of the above criteria, it is not assigned to any of those categories.

If two or more elements (areas) are located outside of a common perimeter of the fuel-energy complex facility, a hazard category shall be assigned (or not assigned) to each such element (area).

Depending on the categorization, the facilities are included on the list (register) of the fuel-energy complex facilities.

The procedure for categorizing fuel-energy complex facilities is established in the national legislation.

2. Legal frameworks for countering terrorism at fuel-energy complex facilities

2.1. State policy in countering terrorism at fuel-energy complex facilities

State policy in countering terrorism at fuel-energy complex facilities consists of a set of government measures aimed at ensuring the most efficient use of available resources and elaborating additional measures aimed to prevent, detect and suppress terrorist activities at fuel-energy complex facilities, minimize and eliminate consequences of their manifestations.

2.2. Parties in charge of countering terrorism at fuel-energy complex facilities

The parties in charge of countering terrorism at the fuel-energy complex facilities includes state bodies, local government and self-government bodies, fuel-energy complex entities, public associations and other organizations, as well as citizens acting within the scope of authority as envisaged in the national legislation.

2.3. Measures implemented by fuel-energy complex entities

A fuel-energy complex entity shall implement the following measures to counter terrorism:

1. Provide physical protection of fuel-energy complex facilities.
2. Improve the system of anti-terrorism security measures for fuel-energy complex facilities in accordance with law requirements for categorized fuel-energy complex facilities.
3. Guarantee the confidentiality of information which, if disseminated without control, could significantly reduce the level of anti-terrorism security of a fuel-energy complex facility.

4. Allow admission to work immediately related to the security of a fuel-energy complex facility only persons who have no unexpunged or outstanding conviction for committing an intentional crime, passed special training, meet qualification requirements, have no medical contraindications and have also undergone a special check in the prescribed manner.
5. Inform the government agencies involved in countering terrorism at fuel-energy complex facilities about the threat and perpetration of a terrorist act at fuel-energy complex facilities, as well as of all established facts of unauthorized actions with potentially dangerous technologies.
6. Introduce innovative organizational and managerial methods and technological solutions to ensure anti-terrorism security of fuel-energy complex facilities.

2.4. Participation of local government and self-governing bodies, public associations and other organizations in countering terrorism at fuel-energy complex facilities

Local government and self-governing bodies, public associations and other organizations participate in countering terrorism at fuel-energy complex facilities jointly with government bodies engaged in countering terrorism at fuel-energy complex facilities, in accordance with the national legislation.

2.5. Citizens' participation in countering terrorism at fuel-energy complex facilities

Citizens voluntarily participate in addressing problems of countering terrorism at fuel-energy complex facilities by providing assistance to government bodies tasked with combatting terrorism at those facilities. The procedure for involving citizens in countering terrorism at fuel-energy complex facilities is determined by the national legislation.

2.6. A procedure for reporting the threat or perpetration of a terrorist act at fuel-energy complex facilities and responding to the report

Once the information on the threat of a terrorist act at a fuel-energy complex facility is received, government bodies involved in countering terrorism at the fuel-energy complex facilities shall:

1. Receive, register and verify the specified information in accordance with the established procedure.
2. Inform the fuel-energy complex entities as a matter of priority.
3. Transmit, if necessary, information to the officials in charge of organizing priority measures to suppress a terrorist act at a fuel-energy complex facility.

The fuel-energy complex entities shall provide information on the threat of perpetration of a terrorist act at a fuel-energy complex facility to the competent government bodies for such threats.

Fuel-energy complex entities must immediately inform the government bodies involved in countering terrorism at fuel-energy complex facilities in the following cases:

1. When a fuel-energy complex entity identifies a threat or the perpetration of a terrorist act at the fuel-energy complex facility.

2. When a fuel-energy complex entity receives information, including anonymously, on a threat or the perpetration of a terrorist act at the fuel-energy complex facility.

Reports on the threat and perpetration of a terrorist act at a fuel-energy complex facility by a fuel-energy complex entity shall be made using the communication means at its disposal to the government bodies in charge of countering terrorism at the fuel-energy complex facilities which are stationed at the physical location of such facility.

The procedure for coordination between the government bodies in charge of countering terrorism at the fuel-energy complex facilities and the fuel-energy complex entities in checking the report on the threat of a terrorist act at a fuel-energy complex facility shall be set out in the national legislation.

3. Provision of anti-terrorism security of fuel-energy complex facilities

3.1. Requirements for anti-terrorism security of fuel-energy complex facilities

Anti-terrorism security for fuel-energy complex facilities is provided by the fuel-energy complex entities in cooperation with the government bodies in charge of countering terrorism at the fuel-energy complex facilities.

The requirements for anti-terrorism security of the fuel-energy complex facilities are determined by the national government depending on the established danger category of the facilities.

The specified requirements are binding for the government bodies and fuel-energy complex entities.

Requirements on anti-terrorism security of fuel-energy complex facilities at their design and construction (reconstruction) stage shall be established by the national government depending on the potential danger category of the facilities and are of mandatory implementation for the developers of the fuel-energy complex facilities. The potential hazard category of the fuel-energy complex facilities being designed or under construction (reconstruction) shall be determined based on the initial pre-categorization data.

Fuel-energy complex entities, in cooperation with the government bodies in charge of countering terrorism at the fuel-energy complex facilities, shall improve the system of anti-terrorism security measures for the fuel-energy complex facilities in accordance with the identified threats.

3.2. Planning and implementation of measures for anti-terrorism security of fuel-energy complex facilities

For the purpose of providing anti-terrorism security of the fuel-energy complex facilities, the fuel-energy complex entities in cooperation with the government bodies in charge of countering terrorism at the fuel-energy complex facilities shall plan and implement a system of measures for anti-terrorism security of those facilities.

The system of measures for anti-terrorism security of fuel-energy complex facilities shall be reflected in the anti-terrorism security certificate of a fuel-energy complex facility and include legal, organizational, engineering, surveillance and other measures.

Information on the system of measures for anti-terrorism security of fuel-energy complex facilities contained in the anti-terrorism security certificate of a fuel-energy complex facility is restricted in accordance with national legislation.

3.3. Physical protection of fuel-energy complex facilities

Physical protection of fuel-energy complex facilities against threats of terrorist acts shall be carried out on the basis of a unified system of planning and implementation of technical and organizational measures aimed at preventing unauthorized entry into protected fuel-energy complex facilities and timely detection and suppression of terrorism at the fuel-energy complex facilities.

Physical protection of a fuel-energy complex facility under construction that is destined upon commissioning to be classified as a high-hazard category facility (hazard category I) shall be provided at the construction stage.

Government bodies in charge of countering terrorism at fuel-energy complex facilities, security units involved in physical protection of fuel-energy complex facilities in accordance with the established procedure, shall have a right to prevent the presence of UAVs in the airspace of those facilities to ensure integrity and security of the guarded facilities by blocking or transforming a remote control and (or) navigation signal of the unmanned aerial vehicles. The procedure for preventing the presence of UAVs in the airspace of the fuel-energy complex facilities shall be determined by the national legislation.

Safety exclusion zones for fuel-energy complex facilities shall be established around individual fuel-energy complex facilities in order to improve the level of anti-terrorism security of the fuel-energy complex facilities in line with the results of their categorization.

The safety exclusion zones of fuel-energy complex facilities provide for a special regime of protection against terrorist acts, including measures to identify acts involving preparation or perpetration of terrorist acts and other illegal actions against those facilities.

Fuel-energy complex facilities with safety security zones, including description of the zones' boundaries, as well as measures aimed to provide a special regime of protection against terrorist acts, shall be determined by the national government.

3.4. Security of critical information infrastructure of fuel-energy complex facilities

Critical information infrastructure of fuel-energy complex facilities includes IT systems, information and telecommunication networks, automated control systems owned outright, under lease or under any other legal arrangement by the fuel-energy complex entities and used by them to carry out activities in the field of fuel-energy complex.

Security of critical information infrastructure of the energy complex facilities shall be provided on the basis of the state system of detection, prevention and elimination of consequences of attacks with the use of ICTs and response to computer incidents in accordance with the national legislation in the field of critical information infrastructure security.

The fuel-energy complex entities are obliged to immediately inform government bodies in charge of countering terrorism at fuel-energy complex facilities of computer incidents. Information on the critical information infrastructure of fuel-energy complex facilities is restricted in accordance with the national legislation.

3.5. Liability for violating legislation on counter-terrorism at fuel-energy complex facilities

Persons guilty of violating legislation on counter-terrorism at fuel-energy complex facilities bear civil, administrative, criminal and other liability in accordance with the national legislation.

4. International cooperation in the field of counter-terrorism at fuel-energy complex facilities

4.1. Legal frameworks of international cooperation in the field of counter-terrorism at fuel-energy complex facilities

The legal frameworks of international cooperation in the field of counter-terrorism at fuel-energy complex facilities include universally recognized principles and norms of international law, international treaties, other relevant sources of international law, state constitutions and other legal acts of a state.

4.2. Goals of international cooperation in counter-terrorism at fuel-energy complex facilities

International cooperation in counter-terrorism at fuel-energy complex facilities is carried out for the following purposes:

1. Developing a coordinated policy and uniting the efforts of the states in the field of counter-terrorism at the fuel-energy complex facilities.
2. Excluding double standards on counter-terrorism at fuel-energy complex facilities.
3. Improving efficiency of interaction between government bodies in charge of countering terrorism at fuel-energy complex facilities.
4. Improving the legal frameworks of international cooperation in counter-terrorism at fuel-energy complex facilities.
5. Harmonizing the national legislation of states in counter-terrorism at the fuel-energy complex facilities.

4.3. Key lines and forms of international cooperation in counter-terrorism at fuel-energy complex facilities

International cooperation in the field of counter-terrorism at the fuel-energy complex facilities is carried out in the following main areas:

1. Contractual
2. Scientific information
3. Scientific-technical.
4. Organizational
5. Information-analytical

6. Preventive
7. Educational

The main forms of international cooperation in counter-terrorism at fuel-energy complex facilities include:

1. Interaction between government bodies on improving their activities
2. Mutual consultations on problems of international cooperation
3. Elaboration and adoption of coordinated measures to eliminate the causes and conditions conducive to information aggression of terrorist and extremist organizations
4. Joint information-analytical activities
5. Rendering of assistance in conducting reporting-analytical activities
6. Joint training and re-training of personnel, advanced training of specialists and internships for representatives of government bodies
7. Exchange of information, research results and best practices
8. Organization of academic seminars and other scientific events
9. Joint scientific and scientific-technical research
10. Sharing of development works
11. Improvement of legal coverage for countering terrorism at fuel-energy complex facilities
12. Mutual legal assistance under international treaties between states
13. Sharing of guidance papers

5. Control and supervision in the field of counter-terrorism at fuel-energy complex facilities

5.1. State control in the field of counter-terrorism at fuel-energy complex facilities

State control in counter-terrorism at fuel-energy complex facilities is carried out by national government bodies in charge of countering terrorism at fuel-energy complex facilities, through scheduled and random inspections of the anti-terrorism security of fuel-energy complex facilities based on the decisions of the heads of those government bodies in compliance with the national legislation.

5.2. Oversight of the legality of counter-terrorism activities at fuel-energy complex facilities

Implementation of legislation in the field of counter-terrorism at the fuel-energy complex facilities is supervised by the state prosecutor general and subordinate prosecutors within their competence.

Bibliography

Guiding principles for Member States on countering the use of new and emerging technologies for terrorist purposes, available at https://documents.un.org/doc/undoc/gen/n23/427/65/pdf/n2342765.pdf?token=wXjQs88uWTUysSOoLA&fe=true.

Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017) and related international standards and good practices on preventing terrorists from acquiring weapons.

CTED trend report on "*Physical Protection of Critical Infrastructure against Terrorist Attacks*", 2017, available at https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted-trends-report-march-2017-final.pdf.

UNOCT – *Five Thematic Modules on the Protection of Vulnerable Target against Terrorist Attacks*, 2022, available at https://www.un.org/counterterrorism/es/node/20481.

UNOCT Guides (modules) on the protection of particularly vulnerable targets against terrorist attacks, in particular, *Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems*, 2022, available at https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod5-unmanned_aircraft_systems_final-web.pdf.

Global Report on the Acquisition, Weaponization and Deployment of Unmanned Aircraft Systems by Non-State Armed Groups for Terrorism related Purposes, available at https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_car_global_report_web_en.pdf.

The Use of Uncrewed Aerial Systems by Non-State Armed Groups, 2024, available at https://unidir.org/wp-content/uploads/2024/01/UNIDIR_Use_of_Uncrewed_Aerial_Systems_by_Non_State_Armed_Groups_Africa.pdf.

Conducting Terrorist Threat Assessment: The Use of New Technologies for Terrorist Purpose, 2023, available at https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_conducting_terrorist_threat_web.pdf.

Marina Mitrevska, Toni Mileski, Robert Mikac (2019), *Critical infrastructure concept and security challenges*, available at https://cip-association.org/wp-content/uploads/2020/07/Chapter1.pdf.

The UN Compendium of Good Practices on the Protection of Critical Infrastructure against Terrorist Attacks, 2022, available at https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf.

United Nations General Assembly (UNGA) Res 63/210 (19 December 2008) Un Doc A/RES/63/210, available at https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F63%2F210&Language=E&DeviceType=Desktop&LangRequested=False.

United Nations General Assembly (UNGA) Res 67/263 (17 May 2013) Un Doc A/RES/67/263, available at https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F67%2F263&Language=E&DeviceType=Desktop&LangRequested=False.

United Nations General Assembly (UNGA) Res 77/298 (22 June 2023) UN Doc A/RES/77/298, available at https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F77%2F298&Language=E&DeviceType=Desktop&LangRequested=False.

United Nations General Assembly (UNGA) Res 78/149 (19 December 2023) UN Doc A/RES/78/149, available at https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F78%2F149&Language=E&DeviceType=Desktop&LangRequested=False.

United Nations Security Council (UNSC) Res 1373 (28 September 2001) UN Doc S/RES/1373, available at https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1373(2001)&Language=E&DeviceType=Desktop&LangRequested=False.

United Nations Security Council (UNSC) Res 1540 (28 April 2004) UN Doc S/RES/1540, available at https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1540(2004)&Language=E&DeviceType=Desktop&LangRequested=False.

United Nations Security Council (UNSC) Res 2325 (15 December 2016) UN Doc S/RES/2325, available at https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2325(2016)&Language=E&DeviceType=Desktop&LangRequested=False

United Nations Security Council (UNSC) Res 2341 (13 February 2017) UN Doc S/RES/2341, available at https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2341(2017)&Language=E&DeviceType=Desktop&LangRequested=False.

United Nations Security Council (UNSC) Res 2370 (2 August 2017) UN Doc S/RES/2370, available at https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2370(2017)&Language=E&DeviceType=Desktop&LangRequested=False.

United Nations Security Council (UNSC) Res 2396 (21 December 2017) UN Doc S/RES/2396, available at https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2396(2017)&Language=E&DeviceType=Desktop&LangRequested=False.

United Nations Security Council (UNSC) *Letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council (28 December 2018)* UN Doc S/2018/1177, available at https://undocs.org/Home/Mobile?FinalSymbol=S%2F2018%2F1177&Language=E&DeviceType=Desktop&LangRequested=False.

Understanding the Challenge

Ahmad J., Shahid A., Reuters (2023), *Islamist militants in Pakistan kill six at oil and gas production site*, available at https://www.reuters.com/world/asia-pacific/islamist-militants-kill-six-gas-oil-extraction-plant-pakistan-2023-05-23/.

Al-Qaeda's North Africa branch claims attack on Algerian gas plant, Reuters, 2016, available at https://www.reuters.com/article/idUSKCN0WL0AM/.

Based on statistics of Kaspersky's reports on main incidents in the field of industrial information and communications technologies security in 2020, 2021, 2022, 2023, available at https://ics-cert.kaspersky.com/publications/reports/.

Bell, Alison & Rogers, Brooke & Pearce, Julia. (2018). *The Insider Threat: Behavioral indicators and factors influencing likelihood of intervention*. International Journal of Critical Infrastructure Protection. 24. 10.1016/j.ijcip.2018.12.001. Available at https://www.researchgate.net/publication/329419966_The_Insider_Threat_Behavioral_indicators_and_factors_influencing_likelihood_of_intervention.

Digitalisation – Essential for Energy System Transformation. But What About Communications? 12 June 2023, available at https://www.techuk.org/resource/digitalisation-essential-for-energy-system-transformation-but-what-about-communications-guest-blog-by-grid-scientific-limited.html.

Digitalisation, International Energy Agency, available at https://www.iea.org/energy-system/decarbonisation-enablers/digitalisation.

Digitalisation of the energy system, available at https://energy.ec.europa.eu/topics/energy-systems-integration/digitalisation-energy-system_en.

Donya Fakhravar, Nima Khakzad, Genserik Reniers, Valerio Cozzani, *Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network, Process Safety and Environmental Protection*, Volume 111, 2017, Pages 714-725, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2017.08.036, available at https://www.sciencedirect.com/science/article/abs/pii/S0957582017302914.

Energy sector faces 39% of critical infrastructure attacks, Security, available at https://www.securitymagazine.com/articles/99915-energy-sector-faces-39-of-critical-infrastructure-attacks.

Gambrell J., *Saudi Arabia: Drone attacks knocked out half its oil supply*, AP News, 2019, available at https://apnews.com/article/d20f80188e3543bfb36d512df7777cd4.

Gas pipeline in Egypt's Sinai attacked, Israel imports unaffected, Al Jazeera, 2020, available at https://www.aljazeera.com/economy/2020/2/3/gas-pipeline-in-egypts-sinai-attacked-israel-imports-unaffected.

Gökçe Küçük, *Daesh attacks oil facilities in Libya*, 2019, available at https://www.aa.com.tr/en/energy/energy-security/daesh-attacks-oil-facilities-in-libya/26031.

James A. Piazza, *Oil and Terrorism: An Investigation of Mediators*, Public Choice 169 (2016): 251–68, https://doi.org/10.1007/s11127-016-0357-0.

Keystone Pipeline System, available at https://www.tcenergy.com/operations/oil-and-liquids/keystone-pipeline-system/.

Lavrukhin, M. *Terrorism in the energy industry*. Energy policy / Energeticheskaya politika, Volume 179, 2023. Pages 24-37, available at https://doi.org/10.46920/2409-5516.2023_1179.24.

Law enforcement capabilities framework for new technologies in countering terrorism, UNOCT, UNCCT, INTERPOL, available at https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_law_enforecement_capabilities_web2.pdf.

Lee, Chia-yi. (2022). *Why do terrorists target the energy industry? A review of kidnapping, violence and attacks against energy infrastructure*. Energy Research & Social Science. 87. 102459. 10.1016/j.erss.2021.102459.

Libya: National Oil Corporation's Tripoli offices attacked, Al Jazeera, 2018, available at https://www.aljazeera.com/news/2018/9/10/libya-national-oil-corporations-tripoli-offices-attacked.

Manar Alanazi, Abdun Mahmood, Mohammad Jabed Morshed Chowdhury, *SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues*, Computers & Security, Volume 125, 2023, 103028, ISSN 0167-4048, DOI: 10.1016/j.cose.2022.103028, available at https://www.sciencedirect.com/science/article/pii/S0167404822004205.

Multi-Billion Dollar Opportunities in Cross-Border Cooperation for Oil and Natural Gas Projects in Southern Africa, available at https://energychamber.org/multi-billion-dollar-opportunities-in-cross-border-cooperation-for-oil-and-natural-gas-projects-in-southern-africa/.

New Danish rules on screening and approval of foreign investments, MAGNUSSON, available at https://www.magnussonlaw.com/news/new-danish-rules-on-screening-and-approval-of-foreign-investments/.

OSCE *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*, available at https://www.osce.org/files/f/documents/7/5/103954.pdf.

Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS), 2022, available at https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod5-unmanned_aircraft_systems_final-web.pdf.

Prodan T., "Maritime Terrorism and Resilience of Maritime Critical Infrastructure", National Security and the Future, 1-2/18 (2017), p. 103. pp. 103-122.

Sonangol Suffers Attempted Cyber-Attack, Business Elites Africa, 2019: https://businesselitesafrica.com/sonangol-suffers-attempted-cyber-attack/?v=04c19fa1e772.

Syria says pipeline blast was terrorist attack, U.S. suspects IS, Reuters, 2020, available at https://www.reuters.com/article/us-syria-blast-electricity/explosion-on-syria-gas-pipeline-a-terrorist-attack-minister-idUSKBN25K062/.

James A. Piazza, "*Oil and Terrorism: An Investigation of Mediators*," Public Choice 169 (2016): 251–68, https://doi.org/10.1007/s11127-016-0357-0.

The attack against Danish, critical infrastructure, 2023, available at https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf.

The Global Terrorism Database™ (GTD), available at https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=202012240006.

"*The In Amenas Attack, Report of the Investigation into the Terrorist Attack on In Amenas*," Statoil, February 2013, available at www.statoil.com/en/NewsAndMedia/News/2013/Downloads/In%20Amenas%20report.pdf.

Thomas G. Pledger, *The Role of Drones in Future Terrorist Attacks*, available at https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf.

Tichý, Lukáš. (2019). *Energy Infrastructure as a Target of Terrorist Attacks from the Islamic State in Iraq and Syria*. International Journal of Critical Infrastructure Protection. 25. 10.1016/j.ijcip.2019.01.003

Toft, Peter & Duero, Arash & Bi, Ar. (2010). *Terrorist targeting and energy security*. Energy Policy. 38. 4411-4421. 10.1016/j.enpol.2010.03.070.

Total declares force majeure on Mozambique LNG after insurgent attacks, Reuters, 2021: https://www.reuters.com/world/africa/frances-total-declares-force-majeure-mozambique-lng-project-2021-04-26/.

TotalEnergies, Mozambique LNG: TotalEnergies' response, 2023, available at https://totalenergies.com/media/news/press-releases/mozambique-lng-totalenergies-response.

Trans-European Networks for Energy, 2020, available at https://energy.ec.europa.eu/topics/infrastructure/trans-european-networks-energy_en.

Wang L., Wang X., Zhao Q., Zhao Y. *Multi-objective policing emergency logistics scheduling on multi-location coordinated terrorist attacks*, 2017, Xitong Gongcheng Lilun yu Shijian/System Engineering Theory and Practice. 37, available at https://www.researchgate.net/publication/322482361_Multi-objective_policing_emergency_logistics_scheduling_on_multi-location_coordinated_terrorist_attacks.

Beneath the Surface: Terrorist and Violent Extremist use of the Dark Web and Cybercrime-as-a-Service for Cyber-Attack, published by UNICRI and UNOCT/UNCCT (Global Counter Terrorism Programme on Cybersecurity and New Technologies).

Algorithms and Terrorism: The Malicious use of artificial intelligence for terrorist purposes, published by UNICRI and UNOCT/UNCCT (Global Counter Terrorism Programme on Cybersecurity and New Technologies).

National approaches on reducing terrorist-related risks to CEI: stakeholders' roles and good practices

Act of 1 July 2011 on the security and protection of critical infrastructure, available at https://crisiscentrum.be/sites/default/files/documents/files/2021-03/PDFsam_15_2.pdf.

Anti-terrorism exercises were held at an oil and gas facility in Dagestan (Дагестане на нефтегазовом объекте прошли антитеррористические учения), AiF-Dagestan (АиФ-Дагестан), 2020: https://dag-aif-

ru.turbopages.org/turbo/dag.aif.ru/s/society/v_dagestane_na_neftegazovom_obekte_proshli_antiterroristicheskie_ucheniya.

Bimo, Prabaswari, *Protecting critical infrastructure from cyberthreats*, The Jakarta Post, 2023, available at https://www.thejakartapost.com/paper/2023/08/09/cybersecurity-strategy-for-indonesias-critical-infrastructure-protection.html.

Christer Pursiainena, Eero Kytömaa, *From European critical infrastructure protection to the resilience of European critical entities: what does it mean?* Sustainable and Resilient Infrastructure 2023, VOL. 8, Pages 85–101, https://doi.org/10.1080/23789689.2022.2128562 available at https://www.tandfonline.com/doi/epdf/10.1080/23789689.2022.2128562?needAccess=true.

Commercial facilities as targets: New threats to critical infrastructures, Social Value Creation Report, NEC, 2016, available at https://sg.nec.com/en_SG/pdf/brochures/PublicSafety/SocialValueCreationReport_en_Vol.1.pdf.

Community Resilience Planning Guide for Buildings and Infrastructure System, available at https://crsreports.congress.gov/product/pdf/R/R47666.

Donya Fakhravar, Nima Khakzad, Genserik Reniers, Valerio Cozzani, *Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network*, Process Safety and Environmental Protection, Volume 111, 2017, Pages 714-725, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2017.08.036, available at https://www.sciencedirect.com/science/article/abs/pii/S0957582017302914.

Doran M., *New cyber offences for targeting key infrastructure, reporting of ransomware attacks made mandatory*, ABC News, 2021, available at https://www.abc.net.au/news/2021-10-13/government-will-mandate-business-reporting-ransomware-attacks/100534890.

Early Warning System for the Kuwait Oil Company, Telegrafia, 2017, available at https://www.electronic-sirens.com/success-story-early-warning-system-kuwait-oil-company/.

Energy Sector Regulatory Framework, Abu Dhabi Government, Department of Energy, available at: https://www.doe.gov.ae/en/Legislation-and-Compliance/Laws-and-Regulations.

Federal law of the Russian Federation № 256 from 26 July 2011 "On security of energy infrastructure", available at https://base.garant.ru/12188188/.

Handbook for Implementing the Principles for Resilient Infrastructure, UNDRR, 2020, available at https://www.undrr.org/media/87213/download?startDownload=20240612.

Handbook For Implementing the Principles for Resilient Infrastructure, UNDRR, 2023, available at https://www.undrr.org/media/87213.

Information security regulation in industrial control systems used in the energy sector (Enerji sektöründe kullanilan endüstriyel kontrol sistemlerinde bilişim güvenliği yönetmeliği), 2017, available at: https://www.resmigazete.gov.tr/eskiler/2017/07/20170713-5.htm.

Infrastructure Codes, Standards, and Regulations: Frequently Asked Questions, 2023, available at: https://sgp.fas.org/crs/misc/R47666.pdf.

KRITIS-Sektor definition Energie, available at: https://www.openkritis.de/it-sicherheitsgesetz/sektor_energie.html.

Melkunaite, Laura & Giroux, Jennifer, *Information Sharing for Critical Energy Infrastructure Protection: Finding value & overcoming challenges*. NATO Energy Security Centre of Excellence, 2013, available at: https://www.researchgate.net/publication/281584950_Information_Sharing_for_Critical_Energy_Infrastructure_Protection_Finding_value_overcoming_challenges.

Nereim V., *Aramco and Saudi navy start exercises to thwart drone and missile attacks*, World Oil, 2021, available at: https://www.worldoil.com/news/2021/3/22/aramco-and-saudi-navy-start-exercises-to-thwart-drone-and-missile-attacks.

Política Nacional de Defensa, Brazil, available at: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf.

Política Nacional de Segurança de Infraestruturas Críticas, DECRETO Nº 9.573, DE 22 DE NOVEMBRO DE 2018, available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm.

Order of the Minister of Economy, Commerce and Business Environment no. 1.178 of 6 June 2011, available at: https://cncpic.mai.gov.ro/en/sectoare/energetic.

OSCE, *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*, Vienna, 2013, available at: www.osce.org/atu/103500?download=true.

Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastructure državnega pomena v Republiki Sloveniji, 2012.

PRESS RELEASE: *Power system stress test: Federal Ministry for Economic Affairs and Climate Action stepping up precautionary measures to safeguard power grid stability this winter*, German Federal Ministry for Economic Affairs and Climate Action, 2022, available at: https://www.bmwk.de/Redaktion/EN/Pressemitteilungen/2022/09/20220905-power-system-stress-test.html.

Resolution of the Government of Kazakhstan on approval of the Rules and criteria for classifying objects as vulnerable to terrorism.

Security strategy of the Czech Republic, 2023, available at: https://mzv.gov.cz/file/5119429/MZV_BS_A4_brochure_WEB_ENG.pdf.

Strategic Environmental Assessment on the Development of a Petroleum Hub in Ghana, available at: https://www.phdc.gov.gh/documents/SEA%20for%20Petroleum%20Hub%20-%20Main%20Technical%20Report.pdf.

Subsecretaría de protección civil y abordaje integral de emergencias y catástrofes (1/2015), available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242082/norma.htm.

The Japanese Cybersecurity Policy for CIP, June 2022 (revised March 2024), available at: https://www.nisc.go.jp/eng/pdf/cip_policy_2024_eng.pdf.

The Petroleum Act, The United Republic of Tanzania, 2015, available at: https://www.ewura.go.tz/wp-content/uploads/2020/04/The-Petroleum-Act-2015-1.pdf.

UK's Public summary of sector security and response plan, 2018, available at: https://assets.publishing.service.gov.uk/media/5c8a7845ed915d5c1456006a/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf.

UK's Sector Security and Resilience Plans, available at: https://www.gov.uk/government/collections/sector-resilience-plans.

Valentin Weber, Maria Pericàs Riera, Emma Laumann, *Mapping the World's Critical Infrastructure Sectors*, 2023, available at: https://dgap.org/en/research/publications/mapping-worlds-critical-infrastructure-sectors.

Yao, Xijun & Wei, Hsi-Hsien & Shohet, Igal & Skibniewski, Miroslaw. (2020). *Assessment of Terrorism Risk to Critical Infrastructures: The Case of a Power-Supply Substation*. Applied Sciences. 10. 7162. 10.3390/app10207162, available at: https://www.researchgate.net/publication/346227204_Assessment_of_Terrorism_Risk_to_Critical_Infrastructures_The_Case_of_a_Power-Supply_Substation.

Zakon o kritičnim infrastrukturama NN 56/13, 114/22, 2022, available at: https://www.zakon.hr/z/591/Zakon-o-kritičnim-infrastrukturama.

International efforts to protect CEI

Energy Security Strategic EAG Supports Critical Energy Infrastructure Protection Course in Kuwait, Naval Postgraduate School, available at: https://nps.edu/web/eag/kuwait-energy-infrastructure.

Implementing the United Nations Global Counter-Terrorism Strategy in Central Asia Concept Paper, UNRCCA, available at: https://unrcca.unmissions.org/sites/default/files/concept_note_eng_0.pdf#:~:text=The%20UN%20Global%20Counter%20Terrorism,law%20as%20the%20fundamental%20basis.

Ivo Walinga, *OSCE activities on Critical Energy Infrastructure Protection*, 2020, available at: https://www.energycharter.org/fileadmin/DocumentsMedia/Forums/2-3_-_Critical_Infrastructure_Mr_Walinga.pdf.

Memorandum of Understanding on the Trans-ASEAN gas pipeline project, 2021, available at: https://asean.org/wp-content/uploads/2021/08/ASEAN-MoU-on-the-Trans-ASEAN-Gas-Pipeline.pdf.

Power blackout hits Kazakhstan, Kyrgyzstan and Uzbekistan, Reuters, 2022, available at: https://www.reuters.com/world/asia-pacific/power-blackout-hits-kazakhstan-kyrgyzstan-uzbekistan-2022-01-25/#:~:text=ALMATY%2C%20Jan%2025%20(Reuters)%20-,use%20to%20cover%20unexpected%20shortages.

"*Recommendations on Countering Terrorism at the Energy Complex Facilities*," issued by the Collective Security Treaty Organization (CSTO), pages 36-46, December 2022, available at: https://paodkb.org/uploads/publication/file/45/sbornik_5_december_2022.pdf.

The protection of critical infrastructures against terrorist attacks: Compendium of good practices, 2018, available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf.

Trans-ASEAN Gas Pipeline, available at: https://aseanenergy.org/apaec/trans-asean-gas-pipeline/.

Renewable and non-traditional energy infrastructure protection

Belgium evacuates nuclear plant staff after attacks, CBS news, available at: https://www.cbsnews.com/news/belgium-attacks-evacuation-tihange-nuclear-plant-staff-isis-dirty-bomb.

Breach at Kudankulam nuclear plant may have gone undetected for over six months, available at: https://economictimes.indiatimes.com/news/politics-and-nation/breach-at-kudankulam-nuclear-plant-may-have-gone-undetected-for-over-six-months-group-ib/articleshow/79412969.cms?from=mdr.

Ex-Ontario Power Generation employee accused of sharing information with foreign entity or terrorist group, Power Engineering, 2024, available at: https://www.power-eng.com/news/ex-ontario-power-generation-employee-accused-of-sharing-information-with-foreign-entity-or-terrorist-group/#gref.

How rotating wing turbine blades impact the Nexrad Doppler weather radar, Radar Operations Center, 2022, available at: https://www.roc.noaa.gov/wsr88d/windfarm/turbinesimpacton.aspx.

Japan's Nuclear Infrastructure: Risks and Mitigation Strategies, 2023, available at: https://www.democracylab.uwo.ca/research/current_research/Japan-Report.pdf.

Johnson Jay, *Roadmap for Photovoltaic Cyber Security*, Report number: SAND2017-13262, 2017, available at: https://www.researchgate.net/publication/322568290_Roadmap_for_Photovoltaic_Cyber_Security.

Nuclear security in India, 2015, available at: https://www.orfonline.org/wp-content/uploads/2015/02/NUCLEAR_SECURITY_IN_INDIA.pdf.

Police data management and analysis (Radiological and Nuclear), INTERPOL, available at: https://www.interpol.int/Crimes/Terrorism/Radiological-and-Nuclear-terrorism/Our-response-to-radiological-and-nuclear-terrorism.

Siciliano J., *FBI joins investigation into alleged terror attack on Las Vegas solar plant*, S&P Global, 2023, available at: https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/fbi-joins-investigation-into-alleged-terror-attack-on-las-vegas-solar-plant-73776901.

Staggs, Jason & Ferlemann, David & Shenoi, Sujeet. (2017). *Wind farm security: Attack surface, targets, scenarios and mitigation*. International Journal of Critical Infrastructure Protection. 17. 10.1016/j.ijcip.2017.03.001, available at: https://www.researchgate.net/publication/315590797_Wind_farm_security_Attack_surface_targets_scenarios_and_mitigation.

The Civil Nuclear Constabulary (CNC), available at: https://www.gov.uk/government/organisations/civil-nuclear-constabulary/about.

Update on cyber security incident, The Nordex Group, 2022, available at: https://www.nordex-online.com/en/2022/04/update-on-cyber-security-incident/.

Case Studies

Case Study – Canadian Resources Infrastructure Resilience Nexus (CRIRN)

Energy infrastructure security division, available at: https://natural-resources.canada.ca/sites/nrcan/files/science-and-data/science-research/cyber-security/eisd-booklet-en.pdf.

Case Study – Computer-assisted Command and Staff Exercises "Eternity-2023"

"Eternity-2023" computer-assisted Command and Staff Exercises held in Baku ended, Ministry of Defense of Azerbaijan, 2023, available at: https://mod.gov.az/en/news/eternity-2023-computer-assisted-command-and-staff-exercises-held-in-baku-ended-video-49709.html.

Case Study – CEI stakeholders in Turkey

The Regulation on Information Security of Industrial Systems Used in the Energy Sector, 13 July 2017, available at: https://www.resmigazete.gov.tr/eskiler/2017/07/20170713-5.htm.

Case Study – EU Commission Recommendation 2019/553 on cybersecurity in the energy sector

Commission Recommendation (EU) 2019/553 of 3 April 2019 on cybersecurity in the energy sector (notified under document C(2019) 2400), EUR-Lex, 2019, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019H0553.

Case Study – Georgia, Strategic Pipelines Protection Department of the Ministry of Internal Affairs Georgia (SPPD)

Source: https://police.ge/en/ministry/structure-and-offices/strategiuli-milsadenebis-datsvis-departamenti?sub=9658.

Case Study – Ghana's National Framework for Preventing and Countering Violent Extremism and Terrorism (NAFPCVET)

Ghana's National Framework for Preventing and Countering Terrorism and Violent Extremism, 29 January 2020, available at: https://www.peacecouncil.gov.gh/storage/2019/09/NAFPCVET-Document-29-Jan-2020.pdf.

Case Study – IAEA's Nuclear Security Training and Demonstration Centre

IAEA Nuclear Security Training and Demonstration Centre (NSTDC), International Atomic Energy Agency, available at: https://www.iaea.org/about/organizational-structure/department-of-nuclear-safety-and-security/division-of-nuclear-security/iaea-nuclear-security-training-and-demonstration-centre.

Case Study – Indonesia PPPs in energy facility protection against terrorist attacks

Strengthening Security of National Vital Object, Pertamina – Indonesian Navy Conducts Emergency Drill, Pertamina, 2023, available at: https://www.pertamina.com/en/news-room/news-release/strengthening-security-of-national-vital-object-pertamina-indonesian-navy-conducts-emergency-drill.

Case Study – International joint exercises "ADMM-Plus Maritime Security Field Training Exercise"

ADMM-Plus Maritime Security Field Training Exercise, MINDEF Singapore, 2019, available at: https://www.mindef.gov.sg/web/wcm/connect/mindef/14d67a7b-f7a4-473c-958b-0ae2093590a0/Infographic.pdf?MOD=AJPERES&CVID=mGI0R7G.

Case Study – Joint anti-terrorist exercises of the CIS ATC

Caspian-Antiterror - 2021 joint anti-terrorism drill of the competent authorities of the CIS member-states, CIS ATC, 2021, available at: https://eng.cisatc.org/1289/133/161/9077.

Case Study – Oil Police in Iraq

Understanding the security bureaucracy in Iraq: agencies and their tasks, July 2020, ORSAM Report, available at: https://orsam.org.tr/d_hbanaliz/understanding-the-security-bureaucracy-in-iraq-agencies-and-their-tasks.pdf.

Case Study – Petrol and Critical Infrastructures Protection Committee of the Gulf Cooperation Council (Saudi Arabia, Kuwait, the United Arab Emirates, Qatar, Bahrain, and Oman)

Twelfth: education and security training, the Cooperation Council for the Arab States of the Gulf, available at: https://www.gcc-sg.org/en-us/CooperationAndAchievements/Achievements/SecurityCooperation/Achievements/Pages/Twelfthedu cationandsecuritytra.aspx.

Case Study – Physical security measures on East African Crude Oil Pipeline Project (EACOP), Uganda

East African Crude Oil Pipeline Project, available at: https://eacop.com/overview.

Report on East African Crude Oil Pipeline Project environment and social impacts, Uganda, 2019, available at: https://www.eia.nl/projectdocumenten/00009498.pdf.

Case Study – PPPs in CEI protection in Algeria

Algeria Allocates $400 Mln to Protect Oil Facilities against Terrorism, Asharq Al Awsat, 2023, available at: https://english.aawsat.com/home/article/4102616/algeria-allocates-400-mln-protect-oil-facilities-against-terrorism.

Case Study – Turkmenistan's approach on inter-agency coordination in natural gas protection against terrorists attacks

Guarantees of reliability and safety, State Information Agency of Turkmenistan, 2013, available at: https://turkmenistan.gov.tm/ru/post/19819/garantii-nadezhnosti-i-bezopasnosti.

Case Study – USA's Pipeline Security and Incident Recovery Protocol Plan

Pipeline Security and Incident Recovery Protocol Plan, Department of Homeland Security, 2010, available at: https://www.tsa.gov/sites/default/files/pipeline_sec_incident_recvr_protocol_plan.pdf.

Tools

Tool – Laboratory to ICT-risk on critical oil and gas facility modelling **(Gubkin university)**

The training laboratory to study computer attack detention was established at Gubkin University, Gubkin University, available at: https://en.gubkin.ru/news/university-life/the-training-laboratory-to-study-computer-attack-detention-was-established-at-gubkin-university/.

Tool – ATC CIS 2019 Methodological recommendations for organizing interaction between security agencies, special services and law enforcement agencies of the CIS member states to ensure anti-terrorist protection of critical energy facilities

Materials the governing staff of bodies security and special services of states -participants of the CIS: Collection of materials – M.: Publishing house "Print Torg", 2019. – 362 p.

Tool – Attack modelling during threat scenario preparation

Zhadikov R.S., Bekzhanov M.A. *Organization of a system of anti-terrorist protection of objects vulnerable to terrorism: Scientific and practical manual*. Almaty: Academy of the National Security Committee of the Republic of Kazakhstan, 2018. 104 pages.

Tool – CEI information

Critical Energy/Electric Infrastructure Information (CEII), US' Federal Energy Regulatory Commission, available at: https://www.ferc.gov/ceii.

Sarah G. Freeman, Matthew A. Kress-Weitenhagen, Jake P. Gentle, Megan J. Culler, Megan M. Egan, Remy V. Stolworthy, *Attack Surface of Wind Energy Technologies in the United States*, 2024, available at: https://inl.gov/content/uploads/2024/02/INL-Wind-Threat-Assessment-v5.0.pdf?utm_medium=email&utm_source=govdelivery.

Tool – OSCE Good Practices Guide on Non-Nuclear CEI Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace

OSCE 2013, *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*, 2013, available at: www.osce.org/atu/103500?download=true.

Tool – Physical Security Information Management (PSIM)

PSIM tool «Iteration physical protection system», JSC, available at: https://iter.ru/en/TERATION_PHYSICAL_PROTECTION_SYSTEM.pdf.

Tool – Risk analysis method "BCK" model.

Rongchen Zhu, Xiaofeng Hu, Yiping Bai, Xin Li, *Risk analysis of terrorist attacks on LNG storage tanks at ports*, Safety Science Volume 137, May 2021, 105192, available at: https://www.sciencedirect.com/science/article/abs/pii/S0925753521000370.

Tool – Security certificate ("security passport") of critical energy facilities as a part of risk management in Azerbaijan, Kazakhstan, the Russian Federation

Framework on Security Passport of Critically Important Facilities Elaboration in the Russian Federation №2034, 10 November 2022, available at: https://base.garant.ru/405693779/.

Legal support for the safety of fuel and energy complex facilities: CIS experience (Правовое обеспечение безопасности объектов топливно-энергетического комплекса: опыт СНГ), 2022, available at: https://gubkin.ru/faculty/faculty-of-complex-safety-of-the-fuel-and-energy-complex/kafedry-i-podrazdeleniya/knb/files/metod_materialy/prav_obespech_obj_tek.pdf.

On approval of a standard passport for anti-terrorist protection of objects vulnerable to terrorism (Об утверждении типового паспорта антитеррористической защищенности объектов, уязвимых в террористическом отношении), 2023, available at: https://adilet.zan.kz/rus/docs/V2300032950.

www.un.org/counterterrorism/vulnerable-targets

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM