CTED-OSCE Trends Report Update

November 2025

PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURE AGAINST TERRORIST ATTACKS

IN PARTNERSHIP WITH THE OSCE PROJECT

PROTECT

United Nations Security Council
Counter-Terrorism Committee
Executive Directorate (CTED)

OSCE Organization for Security and Co-operation in Europe

CTED-OSCE Trends Report Update

PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURE AGAINST TERRORIST ATTACKS

DISCLAIMER
This Trends Report Update was jointly developed by the United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED) and the Organization for Security and Co-operation in Europe (OSCE). The views, findings, interpretations and conclusions expressed in the publication are those of the authors and contributors, and do not necessarily reflect the views or any official position of the OSCE and the CTED or United Nations Member States, including OSCE participating States.

This publication was funded in part by the OSCE Project PROTECT, which has received financial support from Germany and the United States of America.

Design and layout: Fanny Arnold
Image source: Pexels, UN Photo, Wikipedia

CTED
United Nations, New York, USA
www.un.org/securitycouncil/ctc/

OSCE Action against Terrorism Unit
Wallnerstrasse 6, 1010 Vienna, Austria
Tel.: +43 1 514 36 0 | atu@osce.org | www.osce.org

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

CI	critical infrastructure
AI	artificial intelligence
CBRN	chemical, biological, radiological and nuclear
CCTV	closed-circuit television
CER	(EU) Critical Entities Resilience (Directive)
CMM	capability maturity model
CTC	(United Nations Security Council) Counter-Terrorism Committee
CTED	(UN Security Council's) Counter-Terrorism Committee Executive Directorate
CTPN	Counter-Terrorism Preparedness Network
C-UAS	counter-unmanned aircraft systems
DDoS	distributed-denial-of-service
DHS	(United States) Department of Homeland Security
ECOWAS	Economic Community of West African States
EU	European Union
Europol	European Union Agency for Law Enforcement Co-operation.
HVAC	heating, ventilation and air conditioning (systems)
ICAO	International Civil Aviation Organization
ICS	industrial control systems
ICT	information and communication technology
IDS	intrusion detection system
IED	improvised explosive device
INTERPOL	International Criminal Police Organization
ISO	International Organization for Standardization
LLMs	large learning models
NATO	North Atlantic Treaty Organization
NIST	(US Department of Commerce) National Institute of Standards and Technology
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe
PPPs	public–private partnerships
UAS	unmanned aircraft systems
UN	United Nations
UNAOC	United Nations Alliance of Civilizations
UNDRR	United Nations Office for Disaster Risk Reduction
UNGA	United Nations General Assembly
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNOCT	United Nations Office of Counter-Terrorism
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution

INTRODUCTION

Globally terrorist groups are increasingly viewing critical infrastructure (hereafter: CI) as an attractive target. The easy online access to terrorist literature and instructional guides, combined with the growing availability of emerging technologies, has lowered the threshold for carrying out attacks. This has given rise to new and novel threats to the essential services on which modern societies depend. In response, United Nations Member States, including OSCE participating States are investing in new approaches to protect CI from both cyber and physical attacks. Nearly a decade after the United Nations Security Council adopted resolution 2341 (2017)[1] (hereafter: UNSCR 2341 (2017)) on the protection of CI against terrorist acts, this is a timely moment to review the complex landscape of CI-related threats and protection measures.

© A.Savin | Wikipedia

UNSCR 2341 (2017) marked an important recognition of the growing terrorist threat to CI. In support of this new commitment, the same year the Security Council's Counter-Terrorism Committee Executive Directorate (CTED) released the *Trends Report on the Physical Protection of Critical Infrastructure Against Terrorist Attacks*.[2] The aim of the report was to bring analytical perspectives from academia and international and regional organizations to the attention of policymakers. Since 2017, CTED has incorporated UNSCR 2341 (2017) into the assessment framework used during its country visits on behalf of the Counter-Terrorism Committee (CTC).

1 Security Council resolution 2341 was adopted on 13 February 2017.

2 United Nations Counter-Terrorism Committee Executive Directorate (CTED). 2017. *Trends Report on Physical Protection of Critical Infrastructure against Terrorist Attacks*. Available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted-trends-report-march-2017-final.pdf

It has been nearly a decade since UNSCR 2341 (2017) was adopted, making it an appropriate moment to reflect on its impact and the global status of its implementation, including persistent challenges and recommendations for further action. This reflection is complemented by research and analysis conducted elsewhere to enhance understanding of the current and future efforts to protect CI from an evolving terrorist threat. In UNSCR 2617 (2021), the Security Council directed CTED to carry out analytical work on emerging issues, trends and developments, and to make its analytical products available across the UN system. To this end, CTED has partnered with the Organization for Security and Co-operation in Europe (OSCE) to produce this *Trends Report Update*. The OSCE has developed extensive technical expertise in assisting its participating States in fostering public–private partnerships between critical infrastructure owners and operators and Governments in a counter-terrorism context,[3] and in protecting critical energy infrastructure,[4] international transport and other critical sites[5] from terrorist attacks.

TRENDS REPORT UPDATE

This *Trends Report Update* examines the current state of international frameworks and national efforts to physically protect CI from terrorist attacks and to preserve their functionality. To this end, the Report begins by taking stock of international commitments in this domain and their evolution since 2017. It then presents the main observations and analyses of the CTC and CTED, drawing on reports and recommendations from the Committee's country visits conducted since 2017, as well as on its dialogue with Member States and on technical assistance facilitation processes focused on the protection of CI.

Further, the Report provides a high-level overview of the terrorist threat specifically to CI, with particular attention to the dynamics that have changed over the last decade – such as the increasing use of commercial off-the-shelf unmanned aircraft systems (UAS) – as well as those that have remained constant, including the enduring attractiveness of CI attacks for terrorists. It then identifies several emerging trends in the field of CI protection that are shaping how such facilities are protected and managed in the 21st century. The Report concludes with a review of approaches that have proven to be valuable tools for enhancing the physical protection of CI.

This Report incorporates CTED's global insights deriving from its assessments and dialogue with United Nations Member States. It also draws on relevant examples from other international and regional organizations, including practices and frameworks of OSCE and its participating States.

3 Organization for Security and Co-operation in Europe (OSCE). 3 December 2007. Ministerial Council Decision No. 5/07 on public–private partnerships in countering terrorism. Available at: https://www.osce.org/mc/29569

4 OSCE. 3 December 2007. Ministerial Council Decision No. 6/07 on protecting critical energy infrastructure from terrorist attacks. Available at: https://www.osce.org/mc/29482

5 OSCE. 7 December 2012. OSCE Consolidated Framework for the Fight against Terrorism [PC.DEC/1063]. Available at: https://www.osce.org/files/f/documents/7/5/98008.pdf

WHAT IS CRITICAL INFRASTRUCTURE?

In UNSCR 2341 (2017),[6] the Security Council recognized that each State determines what constitutes its CI and how best to protect it from terrorist attacks. At the same time, international commitments related to CI protection have expanded over the last decade. This raises an important question: what is considered CI?

International and regional organizations worldwide have contributed to this discussion with the following definitions:

Un Office For Disaster Risk Reduction (2017)[7]	"The physical structures, facilities, networks and other assets which provide services that are essential to the social and economic functioning of a community or society."
European Union (2022)[8]	"… an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service".
The Economic Community of West African States (ECOWAS)[9]	"… systems, assets, and networks that are vital to national security, public health, and economic stability." ECOWAS emphasizes sectoral identification (e.g., energy, water, telecom), risk management, interagency collaboration, and public–private partnerships.
Critical Five (Australia, Canada, New Zealand, the United Kingdom, and the United States)[10]	"Critical infrastructure, also referred to as nationally significant infrastructure, can be broadly defined as the systems, assets, facilities and networks that provide essential services and are necessary for the national security, economic security, prosperity, and health and safety of their respective nations."

In 2019, the Organisation for Economic Co-operation and Development (OECD) assessed several national CI definitions and found:

> "Some definitions refer to critical infrastructure as infrastructure whose functioning is vital or essential to economic and social well-being, while others stress their importance for the functioning of the State or national security. […] Although definitions vary, it may be agreed that an overarching notion of critical infrastructure means that a disruption will have severe consequences on socio-economic well-being and public safety".[11]

While characteristics of CI vary around the world, the following are some of the common component parts:

- **Sectorial definitions:** Many States define CI by sector, such as energy, public health, financial services, or the chemical industry. Within each sector, there are facilities and systems that enable the provision of essential services. For example, in the energy sector, power plants, transmission lines, electrical substations, information and communication technology (ICT) services collectively ensure the supply of electricity to a given community.

---

6 United Nations Security Council (UNSC). 13 February 2017. Resolution 2341 (2017) [S/RES/2341]. Available at: https://docs.un.org/en/S/RES/2341(2017)

7 UNDRR. 2017. *The Sendai Framework Terminology on Disaster Risk Reduction*. "Critical Infrastructure". Available at: https://www.undrr.org/terminology/critical-infrastructure [accessed 22 June 2025]

8 EU. 2022. Directive 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, *OJ* L 333. Available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj

9 ECOWAS. Critical Infrastructure Protection Policies [website]. Available at: https://cyberportal.ecowas.int/cybersecurity/critical-infrastructure-protection-policies/ [accessed 6 October 2025]

10 Critical 5. March 2014. *Forging a Common Understanding for Critical Infrastructure: Shared Narrative*. Available at: https://www.cisa.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf

11 OECD. 2019. *Good Governance for Critical Infrastructure Resilience*. OECD Reviews of Risk Management Policies. Paris: OECD Publishing. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/good-governance-for-critical-infrastructure-resilience_7d5a9993/02f0e5a0-en.pdf

- **Selective designation:** Not all facilities within a given sector are defined as critical.
- **Designation criteria:** To identify a particular infrastructure as critical, many States develop criteria to guide such designation. While such criteria are often not publicly available, they are generally based, *inter alia*, on assessments of the potential impact resulting from a particular facility's disruption or destruction. For example, if a power plant were to be disrupted, authorities may consider the impact on public confidence, disruption of daily life and access to essential services, and potential environmental consequences. The scope of the impact may determine that the facility be designated as CI.
- **Ownership and management:** CI ownership, management and protection typically involve both public and private actors. Although ownership structures vary, many CI facilities are privately owned, operated, managed, and protected – even when the services they provide, such as electricity or drinking water, are public utilities.
- **Interdependence:** CI systems, processes, and sectors form complex, interdependent networks, including cross-border interconnections. For example, a country's energy sector may depend on financial services, chemicals, water and wastewater management, transport, ICTs, and other support from other sectors – of which some may operate beyond national borders. This interdependence means that disruptions, such as those caused by a terrorist attack can produce cascading effects beyond the targeted sector – an interrelationship recognized in the preamble of UNSCR 2341 (2017).

INTERNATIONAL FRAMEWORKS FOR CRITICAL INFRASTRUCTURE PROTECTION

UNITED NATIONS FRAMEWORK FOR CRITICAL INFRASTRUCTURE PROTECTION

The adoption of UNSCR 2341 (2017)[12] signalled the increased international attention given to the protection of CI. In this resolution, the Security Council recognized that each State determines what constitutes its CI and how best to protect it from terrorist attacks. The Council also acknowledged the growing importance of ensuring the reliability and resilience of CI – and its protection from terrorist attacks – for national security, public safety, and the economy of the concerned States, as well as for well-being and welfare of their populations. Furthermore, the Security Council:

- reaffirmed that countering the terrorist threat requires collective efforts on the basis of respect for international law, including international human rights law and international humanitarian law, and the Charter of the United Nations;
- recognized that preparedness for terrorist attacks includes prevention, protection, mitigation, response and recovery, with an emphasis on promoting security and resilience of CI, including through public–private partnerships, as appropriate;
- encouraged all States to make concerted and co-ordinated efforts, including through international co-operation, to raise awareness and expand knowledge and understanding of the challenges posed by terrorist attacks, in order to improve preparedness for such attacks against CI; and
- called upon Member States to consider developing or further improving their strategies for reducing risks to CI from terrorist attacks.

In the United Nations Global Counter-Terrorism Strategy,[13] the General Assembly expressed particular concern that terrorist attacks against CI could severely disrupt the functioning of both government and the private sector, and cause cascading effects beyond the targeted infrastructure sector. The General Assembly further urged all Member States to take necessary measures to prevent such attacks, as well as their possible radiological, radioactive and environmental consequences, and to counter these terrorist acts, including through the prosecution of perpetrators.

12 UNSC. 13 February 2017. Resolution 2341 (2017) [S/RES/2341]. Available at: https://docs.un.org/en/S/RES/2341(2017)

13 United Nations General Assembly (UNGA). 2023. Resolution adopted by the General Assembly on 22 June 2023 – The United Nations Global Counter-Terrorism Strategy: eighth review [A/RES/77/298]. Available at: https://docs.un.org/en/A/RES/77/298

In 2018, the Security Council Counter-Terrorism Committee completed its review of the 2015 *Guiding Principles on Foreign Terrorist Fighters* (Madrid Guiding Principles)[14] in light of the evolving threat posed by foreign terrorist fighters, and subsequently adopted the *Addendum to the Madrid Guiding Principles*. The Addendum includes Guiding Principles 50 and 51 dedicated to protecting CI, vulnerable or soft targets, and tourism sites.[15] These principles are intended to provide further guidance for Member States in implementing Security Council resolutions on counter-terrorism, including UNSCR 2341 (2017).

Additionally, CTED conducts country visits on behalf of the Counter-Terrorism Committee to assess Member States' counter-terrorism efforts, including progress achieved, remaining gaps and priority areas for technical assistance needs, as well as to identify terrorism-related trends, challenges and good practices in the implementation of relevant Security Council resolutions. These country visits, together with dialogue with national experts, consistently include assessments of States' capabilities to protect CI. CTED facilitates technical assistance by matching available projects and programmes with the needs identified during assessment visits. Furthermore, CTED collaborates with regional organizations such as the OSCE by integrating the Counter-Terrorism Committee's latest findings into partner projects, including the OSCE Project PROTECT.[16]

The United Nations supports its Member States in their efforts to protect CI, including through the Global Programme on Countering Terrorist Threats against Vulnerable Targets,[17] led by the United Nations Office of Counter-Terrorism (UNOCT) in co-operation with CTED, the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Alliance of Civilizations (UNAOC), in close consultation with the International Criminal Police Organization (INTERPOL). The Programme also collaborates closely with regional partners such as the OSCE.

OSCE AND OTHER REGIONAL FRAMEWORKS FOR CRITICAL INFRASTRUCTURE PROTECTION

The protection of CI is firmly embedded in the OSCE mandate, including through the 2012 Consolidated Framework for the Fight against Terrorism, which calls on the Organization to pursue activities that enhance co-operation and build the capacity of its participating States to "improve the security of international transportation and of other CI".[18] This framework builds on previous OSCE commitments related to the protection of CI, including Ministerial Council Decision No. 5/07 on public–private partnerships in countering terrorism,[19] and Decision No. 6/07, which focuses on protecting critical energy infrastructure from terrorist attacks.[20]

14 CTED. 2015. *Madrid Guiding Principles: A practical tool for Member States to stem the flow of foreign terrorist fighters* [S/2015/939]. Available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/madrid-guiding-principles_en.pdf

15 UNSC. 2018. 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 [S/2018/1177]. Available at: https://docs.un.org/en/S/2018/1177

16 OSCE. Project PROTECT [website]. Available at: https://www.osce.org/project/PROTECT [accessed 6 October 2025]

17 United Nations Office of Counter-Terrorism (UNOCT). Threat to Vulnerable Targets [website]. Available at: https://www.un.org/counterterrorism/vulnerable-targets [accessed 6 October 2025]

18 OSCE. 7 December 2012. OSCE Consolidated Framework for the Fight against Terrorism [PC.DEC/1063]. Available at: https://www.osce.org/files/f/documents/7/5/98008.pdf

19 OSCE. 30 November 2007. Public–Private Partnerships in Countering Terrorism (OSCE Ministerial Council Decision No. 5/07). Available at: https://www.osce.org/files/f/documents/3/e/29569.pdf

20 OSCE. 30 November 2007. Protecting Critical Energy Infrastructure from Terrorist Attack [MC.DEC/5/07]. Available at: https://www.osce.org/files/f/documents/4/5/29482.pdf

Similar commitments to CI protection have been made by other regional frameworks, reflecting the broad concern and sustained interest in protecting CI from a range of threats and hazards:

- **The European Union (EU) and North Atlantic Treaty Organization (NATO):** The EU's 2022 Critical Entities Resilience Directive,[21] and NATO's 2022 Strategic Concept[22] establish policy frameworks for protecting CI within their respective memberships.
- **Organization of American States (OAS):** In its 2015 Declaration on the Protection of Critical Infrastructure from Emerging Threats, the OAS Inter-American Committee against Terrorism reiterated its "commitment to identifying and combating emerging terrorist threats, regardless of their origin or motivation, such as threats to CI, and cybersecurity".[23]
- **Association of Southeast Asian Nations (ASEAN):** Through its 2019 Critical Information Infrastructure Protection Framework, ASEAN encouraged its Member States to "develop bilateral and/or multilateral co-operative agreements to enhance security of interdependent [critical information infrastructures] within ASEAN".[24]
- **Joint Plan of Action For the Implementation of the United Nations Global Counter Terrorism Strategy in Central Asia:** Adopted in 2011 and updated in 2022 by Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan, the UN Joint Plan of Action for Central Asia includes collaborative measures to protect critical infrastructure, and emphasizes border security, law enforcement co-operation and resilience building.[25]

© Barnabas Davoti | pexels.com

21 European Parliament and Council of the EU. 14 December 2022. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557. Note that this Directive applies not only to all EU Member States, but also to all those under accession agreements, including many States in South-Eastern Europe.

22 NATO. 29 June 2022. *NATO 2022 Strategic Concept*. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

23 OAS Inter-American Committee against Terrorism (CICTE). 23 March 2015. Protection of CI from Emerging Threats [Declaration]. Available at: https://www.oas.org/en/sms/cicte/documents/sessions/2015/CICTE%20DOC%201%20DECLARATION%20CICTE00955E04.pdf

24 ASEAN. 2019. *Critical Information Infrastructure Protection Framework*. Available at: https://www.etda.or.th/getattachment/2dc40cad-45fe-4433-874c-599d89525558/ASEAN-CIIP-Framework-2019.pdf.aspx

25 UNOCT. March 2022. Joint plan of action : for the implementation of the United nations global counter terrorism strategy in Central Asia, Tashkent 3-4 March 2022. Available at: https://digitallibrary.un.org/record/4061440?v=pdf&ln=zh_CN

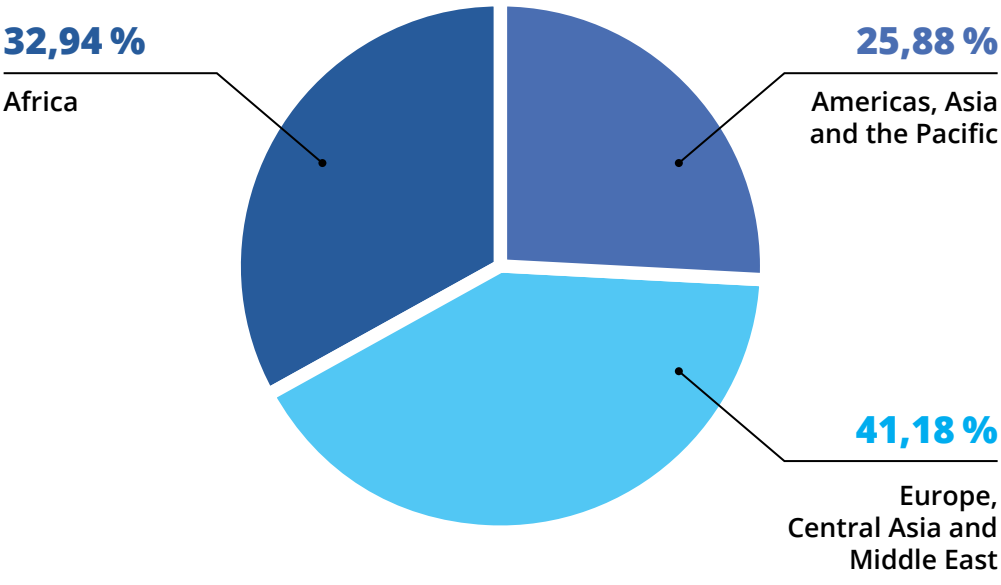
UNITED NATIONS SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE ASSESSMENTS: FINDINGS AND RECOMMENDATIONS 2017-2025

Since 2017, CTED has integrated UNSCR 2341 (2017) and the protection of CI into its assessment visits and technical engagements with Member States. These efforts aim to assist Member States in identifying vulnerabilities, developing coherent national frameworks and strengthening operational resilience against evolving terrorist threats.

This section highlights common gaps and challenges identified by CTED during country assessment visits regarding the implementation by Member States of Security Council resolutions on terrorism and counter-terrorism in the area of CI protection.

Between 2017 and 2025, CTED engaged in extensive dialogue with Member States and conducted 85 country assessment visits to 77 Member States on behalf of the Counter Terrorism Committee. The chart below presents the number of assessment visits according to the CTED's geographical divisions:

ASSESSMENT VISITS BY GEOGRAPHICAL ORDER
according to the CTED's geographical divisions



STRATEGIC FRAMEWORKS FOR CRITICAL INFRASTRUCTURE PROTECTION

Since the adoption of UNSCR 2341 (2017), CTED has observed encouraging developments, including the emergence of national strategies and policy frameworks aimed at addressing terrorism-related risks to CI. However, significant challenges remain. Between 2017 and 2025, CTED found that more than half of the Member States assessed have either only partially developed national CI strategies or rely on broader security or disaster management frameworks that do not adequately address terrorism-specific threats to CI. Approximately half of the visited States have identified, or are in the process of identifying, their CI, and are developing response plans across different CI sectors. However, the level of operation of these strategies varies considerably: while some Member States have no formal or written strategy, others have already tested theirs in various emergency scenarios. Among coastal States, a recurring issue is the uneven level of security across maritime infrastructure, particularly at ports.

Common Gaps and Challenges identified by CTED

- Absence of a dedicated CI protection strategy aligned with UNSCR 2341 (2017);
- Limited integration of CI protection into broader counter-terrorism policies;
- Draft legislation or strategy documents aimed at enhancing CI protection have been developed but remained stalled in political or bureaucratic processes, sometimes for extended periods. In several cases, the lack of formal mandates or designated national lead entities has contributed to institutional delays in developing or endorsing CI-related policies and strategies.
- Outdated or fragmented policy documents that do not address hybrid or cyber-related threat scenarios;
- Limited or no integration of soft target protection within broader CI strategies;
- Lack of structured review cycles or updating mechanisms based on risk assessment outcomes, reducing the ability of States to ensure that CI strategies remain adaptable and responsive to emerging threats;
- Absence or insufficient use of threat and vulnerability assessments to guide the prioritization of potential CI targets, the development of security plans and the allocation of sufficient resources.

Progress identified by CTED

- 10 Member States assessed have developed national strategies and action plans, established comprehensive legal and operational frameworks, and integrated CI protection into broader counter-terrorism policies.
- Several Member States have created national commissions, interagency task forces or dedicated CI focal points. These structures support the design and implementation of whole-of-government policies and strategies, and enable stronger co-ordination between ministries, security and intelligence services, and private operators.

INSTITUTIONAL CO-ORDINATION AND STAKEHOLDER ENGAGEMENT

Effective protection of CI requires close co-ordination among government institutions and meaningful engagement with non-governmental actors, particularly in the private sector. In UNSCR 2341 (2017), the Security Council acknowledged the vital role of informed and alert communities in promoting the awareness and understanding of the terrorist threat environment, as well as the importance of strengthening public awareness, engagement and public–private partnerships through regular national and local dialogue, training and outreach.

Challenges in this area were identified in 20 of the Member States assessed. Recommendations and technical assistance needs include support to enhance collaboration between government entities and the private sector, as well as assistance in formalizing sectoral procedures and agreements.

Common Gaps and Challenges identified by CTED

- Absence of an interagency platform with a national mandate to co-ordinate CI protection efforts, leading to discrepancies in implementation and weak horizontal communication, which continues to limit the effectiveness of CI protection measures;
- Unclear division of roles and responsibilities among ministries and relevant agencies with mandates for CI protection;
- Limited or informal engagement with CI owners and operators, the private sector and other stakeholders;
- Lack of a systematic approach to co-ordination and information sharing with relevant stakeholders – including non-governmental actors – or such efforts remain ad hoc in nature and reliant on individual institutional relationships;
- Insufficient co-ordination between cybersecurity and physical security authorities;
- Limited involvement of local governments and civil society in preparedness and awareness-raising initiatives.

Progress identified by CTED

- Several Member States assessed have formalized institutional co-operation and stakeholder engagement arrangements through national legislation or policy measures to strengthen sustainability and institutional memory.
- A few examples of designated CI liaison positions and the conduct of multi-agency planning exercises have contributed positively to advancing a whole-of-government approach.
- Seven Member States demonstrated active engagement with the private sector and have established co-operative and advisory mechanisms for public–private partnerships.

OPERATIONAL PREPAREDNESS AND RISK MITIGATION

While growing awareness of terrorism-related threats to CI has led to progress in certain areas – particularly in physical security upgrades and emergency planning – significant gaps remain in preparedness, technical capabilities and the systematic application of risk-mitigation practices.

Operational readiness is essential to safeguarding CI from a wide range of threats, including physical sabotage, cyberattacks, improvised explosive devices (IEDs), and hybrid tactics combining physical and digital elements. CTED assessments indicate that many States remain underprepared to detect, prevent, respond to, and investigate such attacks in a co-ordinated and timely manner. Challenges in this area were identified in approximately 30 of the Member States assessed. Recommendations and technical assistance needs include guidance on conducting national threat assessments, support for cybersecurity-related risk management, specialised training on CI protection and counter-IED strategies, and the development of surveillance capabilities in and around CI facilities (for example, through the use of UAS).

Common Gaps and Challenges identified by CTED

- Incomplete or outdated national CI inventories, risk assessments and emergency response plans;
- Lack of comprehensive, scenario-based exercises incorporating threat simulations as part of incident response mechanisms for attacks on CI;
- Limited integration of cybersecurity considerations into CI protection planning;
- Gaps in interagency protocols for CI emergency response and continuity of operations;
- Insufficient technical expertise in areas such as cyber forensics, IED disposal and real-time threat monitoring;
- Preparedness measures remain heavily focused on high-profile locations (e.g. government buildings), while critical services such as public health, utilities and transportation systems are comparatively under-protected. Moreover, general disaster response mechanisms are not always tailored to counter-terrorism-specific requirements, reducing their overall effectiveness.

Progress identified by CTED

- With regard to operational preparedness, CTED has identified promising practices in some States, including the use of integrated planning tools, the conduct of joint exercises and the deployment of rapid response units trained for infrastructure-specific threat scenarios.
- 10 of the Member States assessed had implemented both cybersecurity and physical security measures, provided specialised training and insider-threat prevention, and facilitated the sharing of cyber-protection knowledge and practices among relevant national agencies.

HUMAN RIGHTS COMPLIANCE IN COUNTER-TERRORISM AND CRITICAL INFRASTRUCTURE PROTECTION

The Security Council has consistently emphasised that effective counter-terrorism measures must be implemented in full compliance with international human rights, humanitarian and refugee law. While each State defines CI in accordance with its specific national context and priorities, the potential human rights impact should inform these considerations.[26] UNSCR 2341 (2017) outlines a range of measures – including interdiction, screening, access control, and physical protection – for the safeguarding of CI. The 2022 UN *Compendium of Good Practices on the Protection of Critical Infrastructure against Terrorist Attacks*[27] underscores that such measures may affect certain rights but must comply with international human rights law. Damage to or destruction of CI can directly impact fundamental human rights, including the rights to life, health, education, water and other basic needs. At the same time, when designing and planning measures to protect CI, States should assess impact of those measures to ensure they are non-discriminatory, respect privacy, uphold refugee rights and are gender-sensitive.

On that topic, the 2025 OSCE Project PROTECT *Technical Guide on Physical Security Considerations for Protecting Critical Infrastructure from Terrorist Attacks*[28] dedicates a chapter to human rights considerations and highlights operational issues such as the involvement of third parties (including CI owners and operators, and private security companies) in CI protection, the use of force at CI sites, and privacy and data protection.

Since the adoption of UNSCR 2341 (2017), CTED has issued frequent recommendations to assessed Member States on a range of human rights issues, including those relevant to the protection of CI:

- **The Principle of Legality:** UNSCR 2341 (2017) called upon States to criminalize attacks targeting critical infrastructure, as well as the planning, training, financing and logistical support related to such acts. The CTC has consistently recommended that Member States ensure that the legal definitions of terrorist acts, including those involving CI, are clear, precise and strictly limited to conduct envisaged under international counter-terrorism instruments, in full compliance with international human rights law, particularly the principle of legality. Legal proceedings for terrorist offences must uphold the right to a fair trial, including the principles of equality of arms and admissibility of intelligence-gathered evidence.
- **Freedoms of Expression, Peaceful Assembly and Association:** Security measures around CI must not unduly restrict human rights. And restrictions should be risk-based, proportionate, necessary and non-discriminatory. Oversight mechanisms and human rights training for law enforcement, including those responsible for CI protection, are recommended.
- **The Right to Privacy:** In accordance with UNSCR 2341 (2017), which calls upon States to prevent, protect, mitigate, investigate, respond to, and recover from terrorist attacks on CI, many States have established databases, border-control protocols, passenger-screening systems, surveillance mechanisms and intelligence-sharing frameworks. Safeguards must be in place to protect privacy in surveillance, data collection and intelligence-sharing processes. These include transparency and oversight of watchlists, clear legal procedures for the retention and use of digital evidence, and protections against the misuse of personal data. Public–private partnerships must also operate within legal frameworks that uphold privacy rights.

---

26 UNSC. 2018. Addendum to the guiding principles on foreign terrorist fighters, para 52 [S/2018/1177]. Available at: https://docs.un.org/en/S/2018/1177

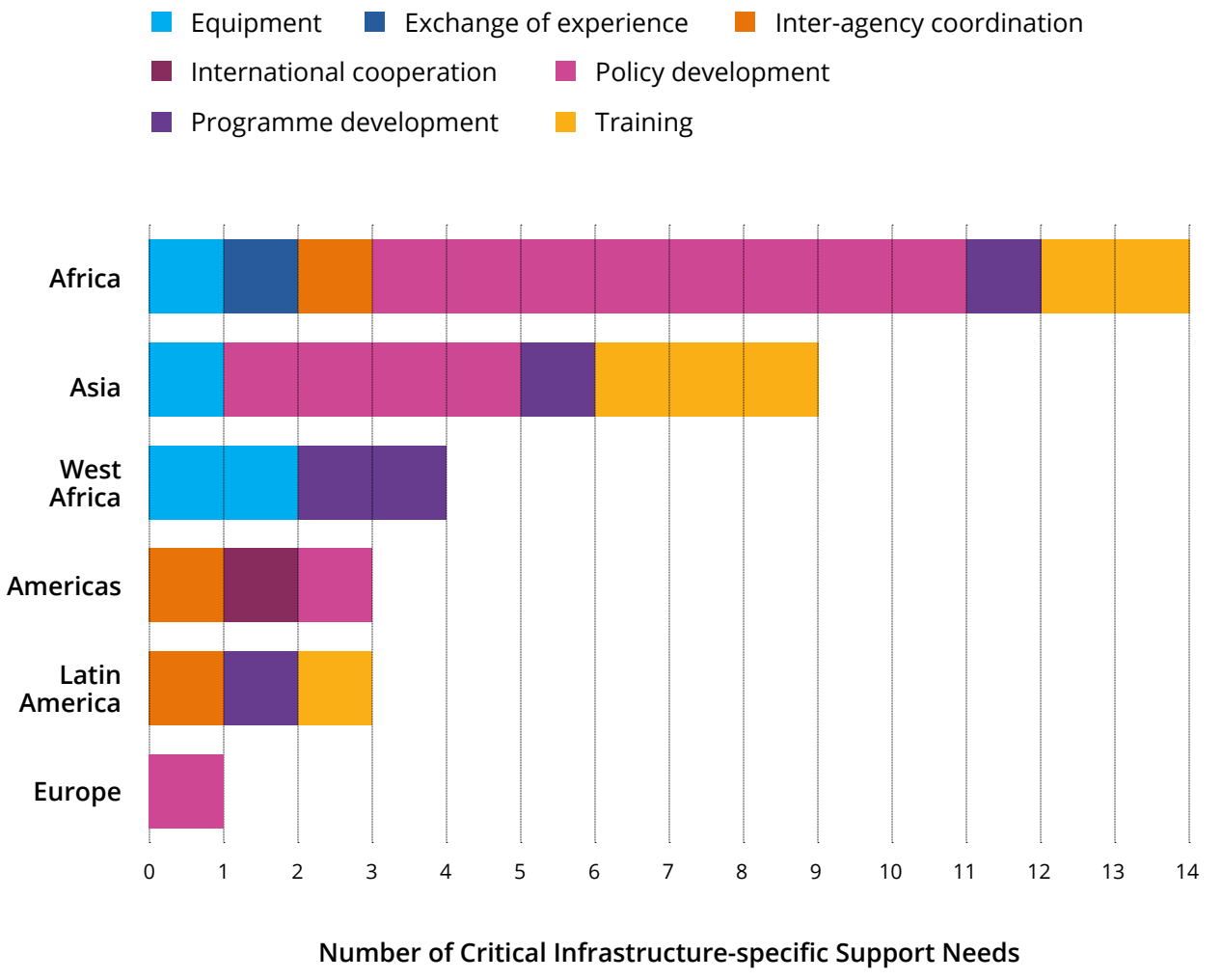
27 UNOCT, CTED, INTERPOL. 2022. *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices*. Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf

28 OSCE. 2025. *Technical Guide on Physical Security Considerations for Protecting Critical Infrastructure from Terrorist Attacks*. Available at: https://www.osce.org/secretariat/597756

- **Victims of Terrorism:** Terrorist attacks targeting CI can cause extensive and long-term harm to victims, including physical injury and psychological trauma. Such attacks may also disrupt economic and social life, impeding access to essential services. The CTC has recommended that Member States promote and protect the rights of victims of terrorism through compensation, dedicated funds, protection programmes and access to justice, while minimizing further harm.
- **Non-discrimination:** Counter-terrorism policies must not target specific groups or communities. States should monitor the impact of such measures on minorities and ensure that gender-responsive approaches are incorporated. Independent oversight, accessible complaint mechanisms and legal avenues for recourse are essential to upholding this principle.

CTED also works to identify the types of assistance required during country assessment visits. The following chart provides a summary of the CI-related assistance needs identified for assessed countries during the 2017–2025 period, disaggregated by region. Recommendations related to policy development appear most frequently across all regions – most notably in Africa – followed by requests for training in CI protection.

TYPES OF CRITICAL INFRASTRUCTURE-SPECIFIC SUPPORT NEEDS BY REGION
identified during CTC country assessments (2017-2025)



REVISITING THE TERRORIST THREAT TO CRITICAL INFRASTRUCTURE

The current terrorist threat comprises both persistent challenges and recent developments that have lowered the barriers to entry for those seeking to compromise the physical security of CI. Across time and regions, terrorists have continued to perceive CI as a highly attractive target – one capable of causing widespread disruption to economic processes and the general population, while drawing attention to their causes.

WIDESPREAD ATTRACTION OF CRITICAL INFRASTRUCTURE ATTACKS

Although terrorist groups differ in their grievances, ideological positions and objectives, attacks against CI continue to represent a common goal for many of them. In recent years, the United Nations Security Council's Analytical Support and Sanctions Monitoring Team – pursuant to resolutions 1526 (2004) and 2253 (2015) concerning ISIL (Da'esh), Al-Qaida and the Taliban and associated individuals and entities – has reported specific terrorist plots targeting CI in Morocco,[29] Iraq,[30] Egypt[31] and Somalia,[32] along with efforts by terrorist groups to establish control over CI facilities, such as in Yemen.[33]

In 2023, the Polish Platform for Homeland Security surveyed 55 EU Protective Security Advisors and other stakeholders on terrorist threats.[34] When asked which locations are of greatest interest to terrorists in the European Union, the most frequent response was CI (63.6 per cent of all respondents). When asked to

29 UNSC. 2024. Letter dated 19 July 2024 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council [S/2024/556]. Available at: https://docs.un.org/en/S/2024/556 and
UNSC. 2023. Letter dated 24 July 2023 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council [S/2023/549]. Available at: https://docs.un.org/en/S/2023/549

30 UNSC. 2022. Letter dated 11 July 2022 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council [S/2022/547]. Available at: https://docs.un.org/en/S/2022/547

31 UNSC. 2021. Letter dated 21 January 2021 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council [S/2021/68]. Available at: https://docs.un.org/en/S/2021/68

32 UNSC. 2021. Letter dated 15 July 2021 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council [S/2021/655]. Available at: https://docs.un.org/en/S/2021/655

33 UNSC. 2022. Letter dated 3 February 2022 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council [S/2022/83]. Available at: https://docs.un.org/en/S/2022/83

34 Wojtasik, Karolina. 2023. *Results of the survey on the perception of terrorist threats among EU PSA participants*, PTBN Analyses No. 1 (2023). Warsaw: Polish Association for National Security. Available at: https://ptbn.online/wp-content/uploads/2025/01/PTBN-Analyses-1-2023.pdf

identify the top three types of facilities expected to face the highest terrorist threat levels during the 2023–2026 period, the largest share of respondents (40 per cent) ranked critical energy infrastructure first. Overall, more than 70 per cent of respondents placed critical energy infrastructure facilities among the top three targets. In the 2025 iteration of the same survey, 64 per cent of the respondents again assessed CI facilities as among the top targets for terrorist or sabotage attacks – the highest proportion across all categories.[35]

AVAILABILITY OF PROPAGANDA AND INSTRUCTIONAL MATERIALS

The ongoing development and dissemination of terrorist propaganda and instructional materials online continue to provide terrorists and other threat actors with the technical knowledge required to construct improvised weapons, select targets and ultimately conduct attacks on CI. Such guidance remains widely accessible across online platforms and is disseminated by threat actors spanning the ideological spectrum.[36] [37]

USE OF UNMANNED AIRCRAFT SYSTEMS (UAS) FOR TERRORIST PURPOSES

In addition to these persistent challenges, more recent developments have further impacted the terrorist threat to CI – most notably the increasing availability and modifiability of commercial off-the-shelf UAS. The threat posed by UAS to CI and public safety is both growing and evolving, as terrorist groups increasingly acquire and weaponize these systems owing to their affordability, accessibility and adaptability.

The Security Council has recognised this emerging threat. In UNSCR 2370 (2017), the Council strongly condemned the continued flow of weapons – including small arms and light weapons, military equipment, *UAS and their components*, and improvised explosive device components – to and between ISIL (Da'esh), Al-Qaida, their affiliates and associated groups, illegal armed groups and criminals, and encouraged Member States to prevent and disrupt procurement networks for such weapons, systems

35 Wojtasik, K.; Szlachter, D. 7 May 2025. Results of the survey on the perception of terrorist and sabotage threats among the experts of the EU Protective Security Advisors. *Terrorism – Studies, Analyses, Prevention*, 2025, special edition. Available at: https://ejournals.eu/czasopismo/terroryzm/artykul/results-of-the-survey-on-the-perception-of-terrorist-and-sabotage-threats-among-the-experts-of-the-eu-protective-security-advisors

36 Frolik, Adam. 28 February 2025. Decoding Saboteurism: An Explanation of Infrastructure Attacks by Far-Right Extremists [webpage]. Available at: https://gnet-research.org/2025/02/28/decoding-saboteurism-an-explanation-of-infrastructure-attacks-by-far-right-extremists/ [accessed 13 October 2025]

37 Clifford, Bennett. May 2018. "Trucks, Knives, Bombs, Whatever:" Exploring Pro-Islamic State Instructional Material on Telegram. *CTC Sentinel* 11.5. Combating Terrorism Center, U.S. Military Academy. Available at: https://ctc.westpoint.edu/trucks-knives-bombs-whatever-exploring-pro-islamic-state-instructional-material-telegram/

and components. In UNSCR 2617 (2021), the Council further noted with concern the growing global misuse of UAS by terrorists to conduct attacks against, and incursions into, restricted commercial and government infrastructure and public places.

CTED's assessments indicate that, between 2017 and 2019, there was limited attention to, or measures in place to counter, the threat posed by UAS. In 2019, CTED was increasingly alerted by Member States to their growing concern at the potential risks posed by the terrorist use of UAS. This concern, combined with inconsistent national, regional and international regulatory and policy responses, suggested that greater efforts are needed to address the potential risks posed by terrorist use of UAS.[38] In recent years, Member States have expressed growing concern over the potential use of UAS for terrorist purposes and CTED's findings show that many have begun incorporating UAS-related threats into national threat assessments and security planning. A few Member States have also deployed UAS to strengthen border security and monitor potential security incidents.

Since 2022, an increasing number of Member States have requested technical assistance to develop UAS surveillance capacity and enhance counter-UAS (C-UAS) capabilities to better protect CI. Some have decided to prohibit the use of UAS without specific authorization, while others are establishing UAS no-fly zones, particularly in the proximity of CI sites such as airports.

© Eric Santoyo | pexels.com

Terrorists are capable of constructing sophisticated devices and modifying commercial UAS for terrorist purposes. They use social media and online platforms to facilitate the acquisition of UAS and their components, and to share knowledge and technical guidance on how to assemble and deploy these systems to conduct attacks. This has enabled the faster adoption of UAS by terrorist actors and has increasingly globalized the threat.[39]

Groups such as Da'esh, Al-Qaida and their affiliates are increasingly employing UAS for surveillance, reconnaissance and targeted attacks. These systems are frequently modified from commercial models and, in some cases, locally manufactured – reflecting growing technical sophistication and operational autonomy. A notable trend is the development of suicide UAS, with groups such as ISIL in Somalia and the Allied Democratic Forces in the Democratic Republic of the Congo testing and deploying repurposed UAS equipped with explosive devices.[40]

38 United Nations Counter-Terrorism Committee Executive Directorate (CTED). 2019. Trends Alert on Greater Efforts Needed to Address the Potential Risks Posed by Terrorist Use of Unmanned Aircraft Systems. Available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted-trends-alert-may_2019.pdf

39 UNSC. 2023. Non-binding guiding principles on threats posed by the use of unmanned aircraft systems for terrorist purposes [S/2023/1035], also referred to as the "Abu Dhabi Guiding Principles". Available at: https://docs.un.org/en/S/2023/1035

40 UNSC. 2025. Thirty-fifth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities [S/2025/71]. Available at: https://docs.un.org/en/S/2025/71. Also see: Global Counterterrorism Forum. Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems. Available at: https://www.thegctf.org/LinkClick.aspx?fileticket=j5gj4fSJ4fI%3D&portalid=1

Cross-group collaboration has further accelerated the spread of UAS expertise, with instances of shared training, technology transfer and joint operations observed among various terrorist groups. Strategically, UAS allow terrorists to bypass conventional defences and conduct precision strikes, particularly in areas with limited counterterrorism security measures, including C-UAS systems. In addition, some groups have reportedly conducted training activities exploring the use of chemical weapons delivered via UAS.[41]

In recent years, terrorist groups have used UAS to conduct attacks or incursions targeting energy utilities, transport hubs, airports and government facilities. Reported incidents include UAS entering restricted airspace, disrupting airport operations or hovering over sensitive sites such as oil fields and military installations.[42] These activities have caused delays, panic, and operational shutdowns – even when the UAS involved were unarmed.

Terrorist groups in Africa are increasingly exploring the use of UAS, with indications of intent to target CI. Although confirmed successful UAS attacks have yet to be reported, groups such as Ahlu Sunna Waljama'a in Mozambique and Al-Shabaab in Somalia have used UAS for surveillance near strategic sites, including ports and airports. Concerns persist regarding terrorist efforts to weaponize UAS for attacks on civil aviation infrastructure. In Libya, security forces disrupted a Da'esh-affiliated cell reportedly preparing a UAS-based attack on gas pipelines, raising alarm about the potential use of UAS for delivering biological agents. These trends reflect a broader shift toward more sophisticated and potentially high-impact terrorist tactics involving UAS technology.[43]

The United Nations supports its Member States in their efforts to counter the threat posed by the use of UAS for terrorist purposes through the Global Counter-Terrorism Programme on Autonomous and Remotely Operated Systems (AROS)[44] led by the United Nations Office of Counter-Terrorism in close co-operation with CTED, the International Civil Aviation Organization (ICAO), the United Nations Global Service Centre under the United Nations Department of Operational Support and the United Nations Department of Peace Operations and Conflict Armament Research.

TERRORIST ADOPTION OF EMERGING TECHNOLOGIES

With the public release of large learning models (LLMs) such as ChatGPT, commentators have expressed growing concern about the potential of malicious actors to exploit these technologies to acquire knowledge related to weapons development,[45] in particular using explosive devices, target selection, the identification of vulnerabilities in specific targets, and to generate and disseminate propaganda.[46] At present, it remains unclear whether LLMs can provide information that would otherwise be inaccessible to determined threat actors, or whether such information is consistently accurate enough to represent a significant advancement in terrorist attack planning capabilities.

---

41 UNSC. 2025. Thirty-fifth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities [S/2025/71]. Available at: https://docs.un.org/en/S/2025/71

42 UNOCT. 2024. *Global Report on the Acquisition, Weaponization and Deployment of Unmanned Aircraft Systems by Non-State Armed Groups for Terrorism-related Purposes*. New York: UNOCT.
Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2024_unoct_car_global_report_web.pdf

43 United Nations Institute for Disarmament Research (UNIDIR). 2024. *The Use of Uncrewed Aerial Systems by Non-State Armed Groups: Exploring Trends in Africa*. Available at: https://unidir.org/wp-content/uploads/2024/01/UNIDIR_Use_of_Uncrewed_Aerial_Systems_by_Non_State_Armed_Groups_Africa.pdf

44 See: https://www.un.org/counterterrorism/autonomous-and-remotely-operated-systems

45 NDTV. 14 September 2023. Hacker manipulates ChatGPT into revealing instructions for making homemade bomb.
Available at: https://www.ndtv.com/feature/hacker-manipulates-chatgpt-into-revealing-instructions-for-making-homemade-bomb-6579701 [accessed 22 June 2025]

46 Weimann, G.; Pack, A. T.; Sulciner, R.; Scheinin, J.; Rapaport, G.; & Diaz, D. 19 January 2024. Generating Terror: The Risks of Generative AI Exploitation. *CTC Sentinel* 17.1. Combating Terrorism Center, U.S. Military Academy.
Available at: https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation/

Deepfakes, AI-generated content, and synthetic audio present new avenues through which threat actors may target CI owners and operators, members of the public, policymakers, or private-sector entities. Such technologies can be used to spread misinformation, manipulate public perception, or gain unauthorised access to specific virtual or physical systems. A 2025 report from NATO's Centre of Excellence Defence Against Terrorism assessed that these tools may be used to fabricate audio or video communications that mimic official instructions, thereby enabling attackers to mislead or confuse populations, particularly during times of crisis.[47]

Additional developments that may facilitate or encourage terrorist attacks on CI include, but are not limited to:

- The use of encrypted communication platforms to facilitate information-sharing, propaganda dissemination and attack planning, as noted by the United Nations' Interregional Crime and Justice Research Institute (UNICRI) in 2024[48] and Europol in 2025.[49]
- The attractiveness of copycat attacks: as one threat actor gains media attention from a particular attack, others – whether motivated by similar or different ideological objectives – may attempt to replicate it. This may have been the case with a series of arson attacks on telecommunication infrastructure across Europe during the early phase of the COVID-19 pandemic, as documented by Europol in 2021.[50]
- The growing number of ransomware attacks affecting industrial control systems at CI facilities: A 2025 report by Dragos identifies an"[e]scalating frequency and complexity of ransomware operations affecting sectors such as manufacturing, transportation, industrial control systems (ICS) equipment, and engineering".[51] The report warns that these multi-domain tactics exploit the interconnectedness of CI at a time when operators face threats that simultaneously compromise both digital and physical layers of security.
- Heightened risk that ICT infrastructure, such as Internet cables and data centres, are viewed as desirable terrorist targets, risking the entire communication systems and the wellbeing of the populations reliant on them.
- Increased threat by the use and exploitations of dual use technologies for terrorist purposes such as 3D-printing, robotics and synthetic biology.

47 Pfaff, C. A.; Deveraux, B.; Lohmann, S.; Lowrance, C.; Özçelik, Ş. B.; Spahr, T.; & Uveges, A. J. 2025. *The Weaponization of AI: The Next Stage of Terrorism and Warfare*. Ankara: Centre of Excellence Defence Against Terrorism.
Available at: https://www.tmmm.tsk.tr/publication/researches/21-TheWeaponizationofAI-TheNextStageofTerrorismandWarfare.pdf

48 UN Counter-Terrorism Centre (UNCCT) & United Nations Interregional Crime and Justice Research Institute (UNICRI) . 21 June 2024. *Beneath the Surface: Terrorist and Violent Extremist Use of the Dark Web and Cybercrime-as-a-Service*.
Available at: https://unicri.org/beneath-surface-terrorist-and-violent-extremist-use-dark-web-and-cybercrime-service-june-2024

49 Europol. 2025. *European Union Terrorism Situation and Trend report 2025*.
Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf

50 Europol. 2021. *European Union Terrorism Situation and Trend report 2021*.
Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2021_0.pdf

51 Alamri, A.H.; Monney, L. 21 May 2025. Dragos Industrial Ransomware Analysis: Q1 2025 [webpage].
Available at: https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q1-2025/#:~:text=Ransomware%20remains%20a%20persistent%20threat,360%20in%20the%20previous%20quarter [accessed 13 October 2025].

EMERGING TRENDS IN CRITICAL INFRASTRUCTURE PROTECTION

The terrorist threat to CI is not the only factor that has evolved in the near decade since the adoption of UNSCR 2341 (2017). Developments in policy approaches to infrastructure protection, as well as the adoption of new technologies, have also transformed the physical protection landscape. This section presents several high-level trends that add nuance to ongoing efforts to physically protect CI from a range of threats and hazards, including terrorist attacks.

CONVERGENCE OF CYBER-PHYSICAL SYSTEMS

Since 2017, the increasing integration of digital technologies into CI operations has been a notable trend that – while bringing many benefits – has intensified the interconnection between cyber and physical security risks, often referred to as the "cyber-physical convergence" or "cyber-physical security convergence". In practical terms, this has led to a growing recognition among policymakers and CI owners and operators of the need for stronger integration between cybersecurity and physical security systems, and for closer co-operation between experts in both domains within a holistic CI security management framework.

The convergence of cyber-physical systems offers significant benefits to CI operators, including improved operational efficiency, enhanced regulatory compliance and faster decision-making.[52] Beyond facilitating CI operations, emerging technologies such as artificial intelligence (AI) can be harnessed to strengthen cybersecurity by analysing vast amounts of data, identifying emerging threats and automating incident responses through the anticipation of specific scenarios and assessment of impacts.[53] These capabilities can support efforts to protect CI from sophisticated cyberattacks[54] that may have destructive or debilitating effects on physical operations.

Yet this digital transformation also introduces new risks that affect both cybersecurity and physical security systems, as well as the interaction between them. As a result of this convergence, these systems are now deeply interconnected: physical operations at a CI facility can be compromised by a cyberattack, while cybersecurity can, in turn, be affected by a physical terrorist attack. Although this trend was already

52 The World Bank, Korea Internet & Security Agency. December 2023. *Strengthening Cybersecurity and Resilience of CI Insights from the Republic of Korea and other digital nations*, World Bank Korea Office Innovation and Technology Note Series, Note Series Number 10. Available at: https://documents1.worldbank.org/curated/en/099705012152346616/pdf/IDU044546588061b004aaf08b5805c55aaee4128.pdf

53 Counter Terrorism Preparedness Network (CTPN). 2025. *Artificial Intelligence in Cities: Securing Our Future*. Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/ctpn_ai_report_2025.pdf

54 World Economic Forum. 2025. *Global Cybersecurity Outlook 2025*. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

well under way in 2017,[55] decreasing costs for digital technologies – such as AI services and the use of Internet of Things devices – and their widespread adoption across CI sectors have continued to accelerate it, drawing increased attention from policymakers and the private sector alike.

This trend has been recognised by international and regional bodies across both the public and private sectors. In 2019, the OECD, in its report *Good Governance for Critical Infrastructure Resilience*, observed that "[t]he rapid evolution of technologies and increasing digitalisation of many CI processes call for a constant watch of digital security threats and a regular assessment of emerging capabilities of malicious actors."[56] Similarly, in its 2023 Directive on the resilience of critical entities (2022/2557), the EU noted that "[d]ue to the increasingly interconnected and cross-border nature of operations using CI, protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place."[57] That same year, the International Security Ligue and Council of European Security Services reported that "the explosion in the number of devices being added to networked systems is exponentially multiplying security risk and increasing the number of ways attackers can gain entry into cyber-physical systems. […] With connectivity, the threat surface extends outside of secured locations and may link to critical operational and physical systems."[58]

What does this trend mean for efforts to ensure the physical protection of CI, particularly against terrorist attacks? From a security management perspective, it underscores the need for stronger integration between cybersecurity and physical security systems, and for a more unified approach to overall security management – a view increasingly echoed by policymakers and stakeholders worldwide.[59] Many of the technologies that support the functioning of CI – such as industrial control systems, communication platforms, and heating, ventilation and air conditioning (HVAC) systems – are now networked or connected to the internet, making them more susceptible to cyberattacks with tangible physical consequences. For example, a cyberattack could alter HVAC system functions, causing overheating and disabling their operation.[60] This level of connectivity enables an increasingly diverse range of threat actors – including terrorists – to disrupt or compromise on-site operations at a CI facility remotely, or as part of a complex attack that combines cyber and kinetic means.

---

55 UNSC Resolution 2341 (2017) refers to cybersecurity as relevant for CI protection; the 2017 CTED Trends Report highlighted the vulnerability of CI to terrorist attacks committed through the internet.

56 OECD. 2019. *Good Governance for Critical Infrastructure Resilience*, OECD Reviews of Risk Management Policies. Available at: https://doi.org/10.1787/02f0e5a0-en

57 EU. 2022. Directive 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, *OJ* L 333. Available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj

58 International Security Ligue, Confederation of European Security Services (CoESS). February 2023. *Cyber-Physical Security and CI: Protecting nations and societies in the era of connected systems and hybrid threats*. Available at: https://www.bdsw.de/images/pdf/isl-coess-cyberphysicalsecurity-wp.pdf

59 For example, the European Commission's Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union [NIS 2 Directive] states: "In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between [the Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities] and this Directive". See EU. 2022. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (NIS 2 Directive), OJ L 333, para 30. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555 [Accessed 13 March 2025]. The International Security Ligue and Confederation of European Security Services state that "[c]ritical infrastructure entities should adopt a framework to unify, align, and integrate physical and cybersecurity and facilitate better coordination with other resiliency functions… An integrated effort to mitigate security-related risk is critical to protect CI security in a world of interdependent risks". See Security Ligue and CoESS. February 2023. *Cyber-Physical Security and CI: Protecting nations and societies in the era of connected systems and hybrid threats*. Available at: https://www.bdsw.de/images/pdf/isl-coess-cyberphysicalsecurity-wp.pdf

60 Cybersecurity and Infrastructure Security Agency (CISA). 2021. *Cybersecurity and Physical Security Convergence* [webpage]. Available at: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520and%2520Physical%2520Security%2520Convergence_508_01.05.2021.pdf [accessed 13 October 2025]

SHIFTING POLICY FOCUS FROM PROTECTION TO RESILIENCE

National efforts to enhance the protection of CI from terrorist and other threats surged globally in the late 1990s and early 2000s.[61] Broadly speaking, this initial wave of efforts largely focused on safeguarding and protecting CI assets against a range of threats and hazards, including terrorism. Since then, some policymakers have increasingly shifted their attention from the *protection* of CI assets to the *resilience* of CI systems – a trend that has accelerated over the past decade.

As identified in the Preamble to UNSCR 2341 (2017),[62] this shift reflects a more complex and dynamic threat landscape for Member States and CI owners and operators, as well as increasingly interconnected and interdependent national, regional and international CI networks. CTED's assessments further suggest that Member States are increasingly recognizing that the rapidly evolving security landscape demands more than traditional protection measures. To effectively address emerging and unpredictable threats, resilience should be built into national systems – encompassing institutional, legal, operational and policy frameworks – and extended down to the CI facility level. This enables flexibility, adaptability, and sustained operational capacity in the event of a terrorist attack. A number of Member States have explicitly included resilience as an objective in their national counter-terrorism or security strategies, suggesting that measures developed in the near future may be increasingly resilience-driven.

Resilience is a well-established concept in the field of disaster risk management, most notably in the *Sendai Framework for Disaster Risk Reduction 2015–2030*. In the Framework's official terminology from 2017, resilience is defined as the "ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management."[63] While there is no UN-level definition of resilience specifically applicable to CI systems, several multilateral organizations have developed their own interpretations, including the OECD[64] and the EU.[65] When applied to CI, definitions of resilience generally refer to the capacity to absorb shocks, maintain continuity of essential services and adapt to evolving circumstances.

---

61 In June 2004, the European Council requested the European Commission to prepare a strategy to increase the protection of CI. This resulted in the Commission's October 2004 Communication on CI protection in the fight against terrorism, which expressed an intention to established European Programme for CI Protection. This proposal was adopted by the European Council on 2 December 2004. On 12 December 2006, a Communication on establishing the European Programme for CI was adopted with the general objective to: "to improve the protection of CI in the European Union". In 2008, the European Council Directive 2008/114/EC on the identification and designation of European CIs and the assessment of the need to improve their protection was adopted. It was repealed in 2024 by the European Directive 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. See: European Commission. 2004. Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Critical Infrastructure Protection in the fight against terrorism. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33259&frontOfficeSuffix=%2F. See also: European Commission. 2007. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33260&frontOfficeSuffix=%2F. On 22 May 1998, the President of the United States produced a Presidential Policy Directive expressing the President's intention that "the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our CIs, including especially our cyber systems". See: The White House. 22 May 1998. Presidential Decision Directive/Nsc-63 on Critical Infrastructure Protection. Available at: https://irp.fas.org/offdocs/pdd/pdd-63.htm

62 "Recognizing a growing importance of ensuring reliability and resilience of CI 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, [...] Recognizing that preparedness for terrorist attacks includes prevention, protection, mitigation, response and recovery with an emphasis on promoting security and resilience of CI, including through public-private partnership as appropriate". UNSC Resolution 2341 (2017). Available at: https://documents.un.org/doc/undoc/gen/n17/038/57/pdf/n1703857.pdf

63 UNDRR. 2017. *The Sendai Framework Terminology on Disaster Risk Reduction*. "Resilience" [webpage]. Available at: https://www.undrr.org/terminology/resilience [accessed 16 May 2025].

64 "Resilience can be defined as the capacity of CI to absorb a disturbance, recover from disruptions and adapt to changing conditions, while still retaining essentially the same function as prior to the disruptive shock. This definition includes the indispensable ability to withstand shocks without loss of functionality, limiting the duration of service interruption as well as minimising the recovery time." OECD. 17 April 2019. *Good Governance for Critical Infrastructure Resilience*. Available at: https://www.oecd.org/en/publications/good-governance-for-critical-infrastructure-resilience_02f0e5a0-en.html

65 Defined as "a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident". See: EU. 2022. Directive 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, *OJ* L 333. Available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj

Perhaps the clearest evidence of this policy shift from CI protection to CI resilience can be found in the EU's Directive on the Resilience of Critical Entities (2022/2557), known as the Critical Entities Resilience (CER) Directive. In its preambular text, the Directive – which must be transposed into domestic legislation by all EU Member States – repeals and replaces the previous EU Directive on Critical Infrastructure Protection (2008/114/EC). The description below summarises this transition:

> "Council Directive 2008/114/EC [...] focuses exclusively on the protection of such infrastructure. However, the evaluation of Directive 2008/114/EC conducted in 2019 found that, due to the increasingly interconnected and cross-border nature of operations using CI, protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place. Therefore, it is necessary to shift the approach towards ensuring that risks are better accounted for, that the role and duties of critical entities as providers of services essential to the functioning of the internal market are better defined and coherent, and that Union rules are adopted to enhance the resilience of critical entities. Critical entities should be in a position to reinforce their ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from incidents that have the potential to disrupt the provision of essential services."

Within the context of addressing terrorist threats to CI, resilience is an increasingly valuable concept, as it broadens the focus beyond the purely technical aspects of asset protection to include efforts aimed at reducing recovery time after an incident and limiting cascading effects. Such measures can make terrorist attacks on CI less impactful. As many definitions emphasise, resilient CI networks are designed to absorb shocks more effectively – for example, mitigating the cascading consequences of a service disruption caused by an explosive terrorist attack on a water treatment facility or electrical substation.

What promise does this trend hold for efforts to counter terrorist threats to CI? A stakeholder focused solely on CI protection may ask "How do I protect my asset from a terrorist attack?" The answer typically focuses on physical security, target hardening and other protective measures. By contrast, efforts centred on strengthening CI resilience may prompt policymakers and other stakeholders to ask "What would be the impact *if* a terrorist attack were to occur on this CI asset?" This reframing can open broader discussions – still encompassing CI protection – among business owners, CI owners and operators, private security providers, civil society, academics and members of the public on preparedness, response and recovery efforts. Such dialogue better prepares society overall for disruptions to critical services.

While the overarching policy shift from infrastructure protection to resilience – or a combined focus on protection *and* resilience – may represent broad global trend, many questions remain unresolved. In 2022, "[t]hrough engagement with member states, the United Nations Office for Disaster Risk Reduction (UNDRR) has recognized that one of the key gaps in the infrastructure resilience arena is a shared view of: what infrastructure is in scope; the extent of resilience; the scale and ambition for resilience; the definition of resilience; and what can be done to improve infrastructure resilience."[66]

66 UNDRR. 2022. *Principles for resilient infrastructure*. Available at: https://www.undrr.org/publication/principles-resilient-infrastructure#editors-recommendations

USE OF UNMANNED AIRCRAFT SYSTEMS AS A THREAT AND A TOOL

While concern over the threat posed by UAS to CI and public safety has grown, as described above, UAS also offer benefits and opportunities for relevant national authorities to counter terrorism and crime, and to protect CI. UAS can be effectively deployed for multiple purposes, including:

- gathering intelligence on criminal or terrorist activities without putting personnel at risk;
- monitoring movements, suspicious activity or threats in the vicinity of power plants, airports, seaports, government buildings or CI located in remote areas;
- detecting and intercepting UAS used by terrorists for surveillance or attacks targeting CI;
- providing real-time aerial views to support rapid incident response;
- co-ordinating emergency responses following a terrorist attack.

In its resolution 2617 (2021), the Security Council acknowledged the need to strike a balance between fostering innovation and preventing the misuse of UAS as their applications expand. It also noted international efforts aimed at raising awareness of and preparedness for potential terrorist use of UAS as the technology becomes more accessible and widely employed across both the public and private sectors.

The trend identified here centres on the dual nature of UAS as both a threat (as described above) and a tool. States are increasingly incorporating the threat posed by the use of UAS for terrorist purposes into national counter-terrorism strategies, security strategies, and/or action plans for the protection of CI and "soft" targets.[67] However, there are currently no standardized counter-UAS capabilities across all Member States and many face technological and legal gaps in detecting, tracking and neutralizing unauthorized UAS, particularly in sensitive environments such as CI. The rapid evolution of UAS technology further complicates defensive measures. These challenges underscore the importance of adopting national legislation, where necessary, to regulate the manufacture, supply, transfer and use of UAS, in order to keep pace with technological developments and to strengthen identification, threat-prevention and detection mechanisms.

67 This approach is promoted in the Abu Dhabi Guiding Principles, 2023. Available at: https://docs.un.org/en/S/2023/1035

INTEGRATION OF INFORMATION AND COMMUNICATION TECHNOLOGIES INTO CRITICAL INFRASTRUCTURE OPERATIONS, INCLUDING ARTIFICIAL INTELLIGENCE

CI owners and operators are increasingly integrating emerging technologies into their daily work. While these technologies offer tools for improved operational efficiency, enabling predictive maintenance, enhancing emergency response and optimizing other processes, they also create new opportunities for malicious actors to disrupt and damage CI functionality. Although the growing use of AI and other advanced technologies by CI owners and operators brings clear benefits – and tools such as facial recognition-equipped CCTV can strengthen security – it is equally important that their deployment respects privacy, data protection and non-discrimination rights.[68]

The assessments of CTED increasingly indicate that Member States are developing responses to the potential threats posed by emerging technologies – particularly ICTs – which was not yet the case in 2017. For instance, several Member States have since adopted ICT-specific legislation or national cyber-security strategies, and most assessed States are investing in cyber expertise, establishing dedicated cyber-investigation units and authorizing task forces to address cyber-related issues. A number of States have set forth regulations of online content and are now beginning to enact AI-specific legislation.[69] However, some Member States have yet to take such measures, either due to limited capacity or difficulties in enacting legislative frameworks in this area. Consequently, their ability to respond to cybersecurity incidents, including those affecting CI operations, often remains ad hoc and case specific. CTED's recent assessments indicate that, given current technological development and uptake, AI-driven systems and tools still serve as a complement to, not replacement of existing counter-terrorism measures and human-supervised monitoring systems.


© Igor Passchier | pexels.com

68 See: Council of Europe. 2024. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series - No. 22. Available at: https://rm.coe.int/1680afae3c
For general principles on the development and use of AI, see: INTERPOL. *Principles for Responsible AI Innovation, AI Toolkit*. Available at: https://www.interpol.int/content/download/20934/file/AI_Toolkit_-_Principles_for_Responsible_AI_Innovation%5B1%5D.pdf

69 In the United States, for example, Congress put forward the "Generative AI Terrorism Risk Assessment Act" earlier this year, which, if adopted, would mandate regular assessments of how terrorist groups are using AI and other digital tools. In 2024, the European Union introduced the Artificial Intelligence Act, the first comprehensive regulation for AI. The Act bans certain AI practices across the EU and establishes a risk-based approach to regulation. The EU also recognized the need for law enforcement agencies to deploy some high risk AI tools in certain circumstances, to include for countering terrorism, but this is constrained by judicial authorization, transparency, proportionality, and oversight.

On the business side of CI operations, emerging technologies have increasingly been integrated into processes over the past decade, creating opportunities for more efficient and effective approaches to CI protection and resilience. For example:

- Machine learning and generative artificial intelligence (AI) can be – and in some cases already are – used by energy infrastructure operators to detect equipment failures, predict maintenance needs, detect and diagnose anomalous events, and support modelling and simulations for improved decision-making,[70] [71]
- AI-based predictive maintenance systems can analyse large datasets from sensors, logs and other performance indicators across CI operations, thus minimizing unplanned disruptions to transportation networks, water supply systems and healthcare services.[72]
- "Digital twins" – virtual replicas of a physical infrastructure assets – can be used by CI owners and operators to simulate crisis scenarios and test response mechanisms,[73] including modelling the impact of natural disasters on CI assets and systems.[74]
- According to a 2025 report from the Counter-Terrorism Preparedness Network, AI is increasingly being used to enhance the capabilities of drones and autonomous vehicles, including to "complet[e] independent data analysis and mak[e] autonomous decisions".[75]

However, while CI owners and operators are adopting emerging technologies to support their objectives, malicious actors have likewise recognised their utility. Terrorist threats in the cyber domain include phishing, distributed-denial-of-service (DDoS), and ransomware. While such attacks are not new, machine learning has the potential to automate key aspects of DDoS attacks – for example, by managing the botnets that execute attacks or by identifying vulnerable systems through advanced network reconnaissance.[76] In 2025, the Counter-Terrorism Preparedness Network (CTPN) identified six ways in which AI poses potential terrorist threats, many of which could impact CI security:[77]

- "New attack patterns and tactics that use AI in yet unknown ways,
- Semi or fully automated attacks using autonomous and remote systems,
- Radicalization to violence and recruitment of individuals by targeting groups in a situation of vulnerability,
- Hostile reconnaissance, intelligence collection, and operational planning/instructions,

---

70 Nambiar, I. *Artificial intelligence – Exploring its use in grid modernization*, California ISO (CAISO). Available at: https://www.caiso.com/about/news/energy-matters-blog/artificial-intelligence-exploring-its-use-in-grid-modernization [accessed 6 October 2025];
see also: U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response (CESER). 26 April 2024. *Summary report: Potential Benefits and Risks of Artificial Intelligence for Critical Energy Infrastructure* (EO 14110). Available at: https://www.energy.gov/sites/default/files/2024-04/DOE%20CESER_EO14110-AI%20Report%20Summary_4-26-24.pdf

71 U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response (CESER). 26 April 2024. *Summary report: Potential Benefits and Risks of Artificial Intelligence for Critical Energy Infrastructure* (EO 14110).
Available at: https://www.energy.gov/sites/default/files/2024-04/DOE%20CESER_EO14110-AI%20Report%20Summary_4-26-24.pdf

72 Olufemi O. D.; Ejiade, A. O.; Ogunjimi O.; & Ikwuogu, F.O. 13 November 2024. AI-enhanced predictive maintenance systems for critical infrastructure: Cloud-native architectures approach, *World Journal of Advanced Engineering Technology and Sciences* 13.2 (2024) 229–257.
Available at: https://wjaets.com/sites/default/files/WJAETS-2024-0552.pdf

73 Mitxelena, J. 18 March 2025. Digital Twin for Critical Infrastructure Management [webpage].
Available at: https://digitaltwinproject.eu/digital-twin-for-critical-infrastructure-management/ [accessed 6 October 2025]

74 Dianyou, Y. & He, Z. Digital twin-driven intelligence disaster prevention and mitigation for infrastructure: advances, challenges, and opportunities. *Natural Hazards* 112 (2022) 1–36.

75 CTPN. 2025. *Artificial Intelligence in Cities: Securing Our Future*.
Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/ctpn_ai_report_2025.pdf

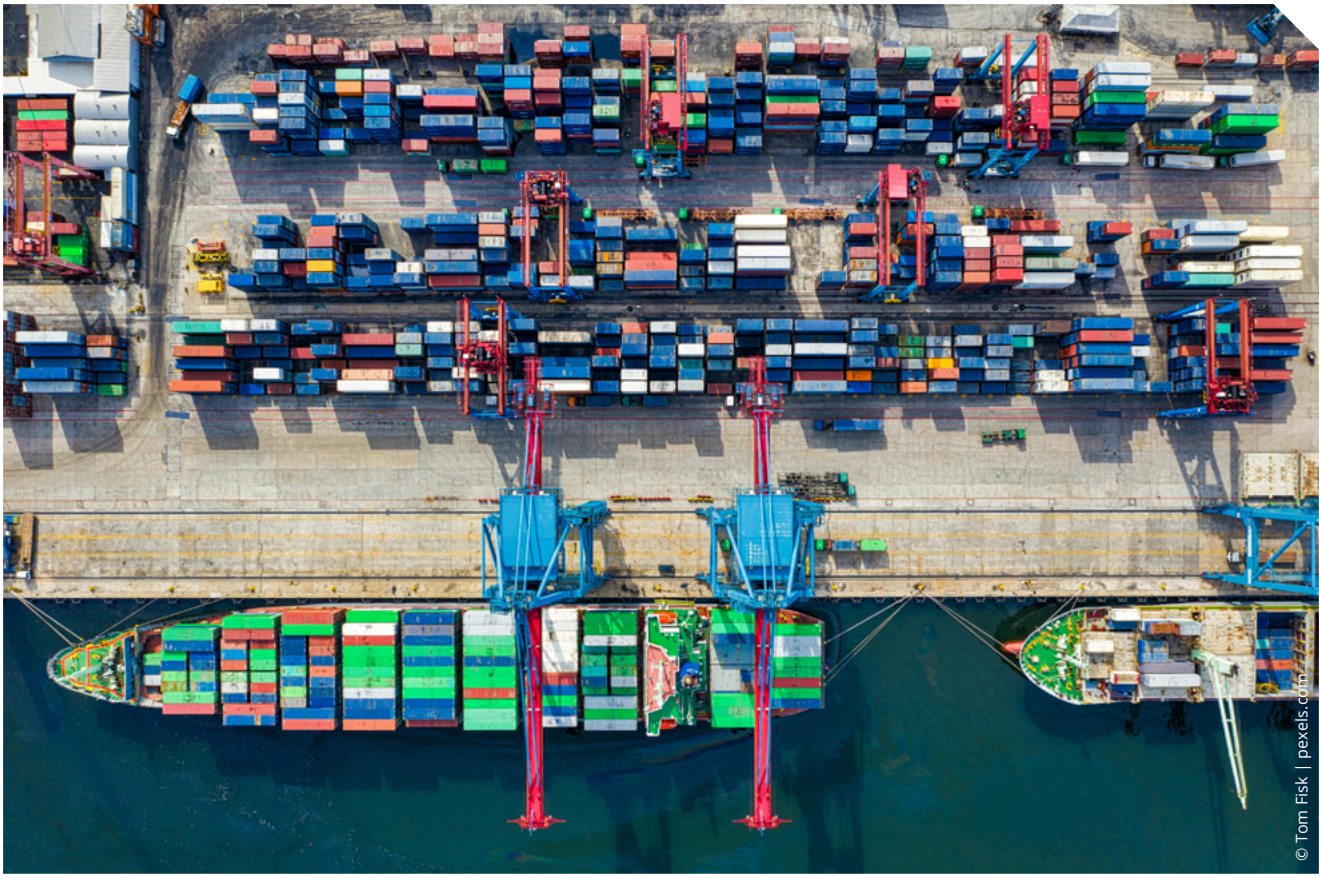
76 UNICRI & UNCCT. 2021. *Algorithms and terrorism: The malicious use of artificial intelligence for terrorist purposes*.
Available at: https://unicri.org/sites/default/files/2021-06/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20Report_Web.pdf

77 CTPN. 2025. *Artificial Intelligence in Cities: Securing Our Future*.
Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/ctpn_ai_report_2025.pdf

- Enhanced and higher volumes of propaganda and disruption through disinformation,
- Higher tempo of cyberattacks, lowing the entry point for those that are most sophisticated."

Governments have become increasingly focused on the malicious use of emerging technologies. In 2024, the United States Department of Homeland Security issued guidelines to help CI owners and operators mitigate AI risks.[78] Specifically, it has warned that AI can be used, *inter alia*:

- "to augment threat actor capabilities and operations (e.g., autonomous malware, reconnaissance, use of deepfakes, automatic parsing of text for vulnerability insights, modeling and model inference and completion, unauthorized data access, cyberattack detection evasion, vulnerability identification and exploitation, machine-speed decision-making, optimization, prompt injections to reveal sensitive information)" and
- to engage in "AI-enabled psychological manipulation to trick users into revealing sensitive information or performing actions that compromise security controls, including the use of deepfakes or AI-enhanced phishing attempts."



78 US Department of Homeland Security. April 2024. *Mitigating Artificial Intelligence (AI) Risk: Safty and Security Guidelines for Critical Infrastructure Owners and Operators*.
Available at: https://www.dhs.gov/sites/default/files/2024-04/24_0426_dhs_ai-ci-safety-security-guidelines-508c.pdf

VALUE-ADD APPROACHES FOR ENHANCING THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURE

Thus far, this Trends Report Update has highlighted the evolving terrorist threats and emerging trends that are shaping how critical facilities are protected and managed in the 21st century. These developments raise an important question: how can policymakers, CI owners and operators, and security professionals respond and adapt?

This section presents a series of approaches and actions that may add value to ongoing efforts to enhance the physical protection of CI and support stakeholders in navigating this increasingly complex domain.

PURSUING INTERAGENCY CO-OPERATION, PUBLIC–PRIVATE PARTNERSHIPS AND ENGAGEMENT WITH ACADEMIA AND CIVIL SOCIETY

National-level interagency co-operation and multi-stakeholder approaches are essential in protecting CI in the counter-terrorism context, as they enable a unified, co-ordinated, and effective response to complex and evolving threats. Countering terrorism threats against CI spans multiple domains – security, intelligence, law enforcement, border control, criminal justice, cyber defence, and emergency management. By fostering collaboration among agencies, governments can pool expertise, share intelligence in real time and close operational gaps that terrorists might otherwise exploit.

Both the Security Council and the OSCE Ministerial Council have identified the value of public-private partnerships specifically in this context. In UNSCR 2341 (2017), the Security Council recognised that the effectiveness of CI protection is greatly enhanced when it is based on an approach that considers all threats and hazards – notably terrorist attacks – and is combined with regular and substantive consultation and co-operation among CI operators, law enforcement, and security officials responsible for CI protection, as well as, when appropriate, other stakeholders, including private sector owners. In 2007, the OSCE participating States acknowledged "the usefulness of joint counter-terrorist efforts by government bodies and the private sector", including in the context of "Identifying, prioritizing, and protecting critical infrastructure and addressing preparedness/consequence management issues".[79]

In UNSCR 2617 (2021), the Security Council recognised the importance of civil society – including community-based organization, grassroots initiatives, the private sector, academia, think tanks, the media, youth,

79 OSCE. 30 November 2007. Public–Private Partnerships in Countering Terrorism (OSCE Ministerial Council Decision No. 5/07). Available at: https://www.osce.org/files/f/documents/3/e/29569.pdf

women and cultural, educational, and religious leaders – in raising awareness of terrorist threats and enhancing collective efforts to counter them. In the same resolution, the Council encouraged CTED to support Member States in developing or further improving their strategies to reduce risks to CI and soft targets from terrorist attacks. This includes, *inter alia*, promoting better interoperability, across all levels of government, as well as with private industry and civil society, as appropriate and in line with UNSCR 2341 (2017).

INTER-AGENCY CO-OPERATION

In addition to the Security Council, several international and regional organizations have addressed national interagency co-operation in countering terrorism through their respective instruments and guidance.[80] Protecting CI requires co-ordinated security planning, underpinned by risk management approaches that engage all levels of government and all agencies with responsibilities for CI protection. Based on information gathered during CTED country visits, many Member States may find added value in creating clearer co-operation and information-sharing frameworks or protocols, as well as access to or connectivity with information-sharing mechanisms. Several Security Council instruments outline the key elements required for effective interagency co-ordination and information-sharing processes, which are essential to ensure that relevant agencies can rapidly communicate threat and operational information in the event of an attack against CI.[81] Building trust and shared understanding across agencies is equally critical, as is the inclusion of public safety bodies and the private sector to enrich the overall information landscape related to CI protection.

© Eskinder Debebe | UN Photo

Interagency co-operation and co-ordination are also vital for implementing robust CI protection strategies. Given the cross-sectoral nature of CI, national strategies must bridge various domestic agencies – ranging from security, justice, defence, communications and transport agencies to regional bodies and

80 See: Council of the EU. 30 November 2025. *The European Union Counter-Terrorism Strategy*. Available at: https://data.consilium.europa.eu/doc/document/ST%2014469%202005%20REV%204/EN/pdf; African Union. 2011. *African Model Anti-Terrorism Law*. Available at: https://archives.au.int/bitstream/handle/123456789/8313/african-model-law-E.pdf?sequence=1; ASEAN. 2011. *ASEAN Convention on Counter Terrorism* (ACCT). Available at: https://asean.org/wp-content/uploads/2021/01/ACCT.pdf; OAS CICTE. CICTE Program: Inter-American Counter-Terrorism Network. Available at: https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=899&lang=1; OSCE. 7 December 2012. OSCE Consolidated Framework for the Fight against Terrorism [PC.DEC/1063]. Available at: https://www.osce.org/files/f/documents/7/5/98008.pdf; UNOCT, National Interagency Coordination Mechanism – Fusion Cells [website]. Available at: https://www.un.org/counterterrorism/fusion_cells [accessed 6 October 2025], which aims to support Member States in the development of national interagency co-ordination mechanisms.

81 UNSC Counter-Terrorism Committee. 2019. *Security Council Guiding Principles on Foreign Terrorist Fighters: The 2015 Madrid Guiding Principles + 2018 Addendum*. Available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/security-council-guiding-principles-on-foreign-terrorist-fig.pdf

regulators. However, achieving seamless co-ordination presents notable challenges. Differences in terminology, procedures and institutional cultures can hinder effective communication and joint action.[82] In this regard, institutionalized interagency co-operation mechanisms can support synchronized procedures and facilitate information exchange among the agencies responsible for CI protection. Such mechanisms also enable the conducting of joint exercises, ensuring operational integration across relevant agencies. In doing so, they ensure that new systems and personnel are oriented towards collaborative functioning throughout all phases – prevention, protection, mitigation, response and recovery from terrorist attacks on CI – and that efforts to promote security and resilience are sustained.

PUBLIC-PRIVATE PARTNERSHIPS AND MULTI-STAKEHOLDER APPROACHES

To enhance the protection of CI, Member States are encouraged to establish national frameworks that support risk-based decision-making, information-sharing and public–private partnerships. These frameworks should foster collaboration between government and industry to jointly determine priorities and develop tools such as surveillance guidelines and tailored protective measures for vulnerable targets, including CI. In addition, processes should be established to facilitate the exchange of risk assessments and other relevant information between government entities and private sector partners, including through mechanisms such as employee background checks and security clearances. Promoting such partnerships also entails supporting business owners, infrastructure managers and industry stakeholders by sharing plans, policies and procedures aimed at strengthening overall security and resilience.[83]

Given that many CI assets are privately owned, operated or include partial private holdings, the establishment of public–private partnerships (PPPs) is essential for effectively protecting CI and achieving infrastructure resilience. The OSCE 2025 *Technical Guide on Physical Security Considerations for the Protection of Critical Infrastructure from Terrorist Attacks* provides a valuable overview of PPPs within the CI protection domain.[84] Such partnerships enable both State authorities and the private sector to address security needs, reduce vulnerabilities and share information with a view to mitigating the risk of attack, while ensuring that human rights considerations are integrated at every stage of protection, mitigation, response and recovery.[85]

The United Nations, regional organizations such as the OSCE, and a number of Member States have developed a range of projects, reports and guidelines emphasizing the importance of multi-stakeholder approaches to protecting CI from terrorist threats, particularly through public–private partnerships.[86]

---

82 UNOCT, CTED, INTERPOL. 2022. *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices*. Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf

83 United Nations Security Council Counter-Terrorism Committee. 2019. *Security Council Guiding Principles on Foreign Terrorist Fighters: The 2015 Madrid Guiding Principles + 2018 Addendum*, principles 50 and 51. Available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/security-council-guiding-principles-on-foreign-terrorist-fig.pdf

84 OSCE. 2025. *Technical Guide on Physical Security Considerations for Protecting Critical Infrastructure from Terrorist Attacks*. Available at: https://www.osce.org/secretariat/597756

85 United Nations Office of the High Commissioner for Human Rights. 2011. *Guiding Principles on Business and Human Rights : Implementing the United Nations "Protect, Respect and Remedy" Framework*. Available at: https://digitallibrary.un.org/record/720245?v=pdf

86 See for example: OSCE. 7 December 2012. OSCE Consolidated Framework for the Fight against Terrorism [PC.DEC/1063]. Available at: https://www.osce.org/files/f/documents/7/5/98008.pdf; Council of the EU. 30 November 2025. *The European Union Counter-Terrorism Strategy*. Available at: https://data.consilium.europa.eu/doc/document/ST%2014469%202005%20REV%204/EN/pdf; European Commission. 2007. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33260&frontOfficeSuffix=%2F; European Commission. 2025. EU Preparedness Union Strategy. Available at: https://ec.europa.eu/newsroom/cipr/items/884584/en; *Global Counterterrorism Forum Soft Target Protection Initiative Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context*. Available at: https://www.thegctf.org/Portals/1/Documents/Links/Meetings/2017/Twelfth%20GCTF%20Coordinating%20Committee%20Meeting/GCTF%20-%20Antalya%20Memorandum%20on%20the%20Protection%20of%20Soft%20Targets%20in%20a%20Counterterrorism%20Context.pdf?ver=2017-09-17-010844-720; OAS CICTE, UNICRI. 2023. *Public–private partnerships: A risk management approach to address security threats*. Available at: https://www.oas.org/en/sms/cicte/KMSMESec/images/tools/32.pdf; ASEAN. *ASEAN Critical Information Infrastructure Protection (CIIP) Framework*. Available at: https://www.etda.or.th/getattachment/2dc40cad-45fe-4433-874c-599d89525558/ASEAN-CIIP-Framework-2019.pdf.aspx; OSCE. 2025. *Technical Guide on Physical Security Considerations for Protecting Critical Infrastructure from Terrorist Attacks*. Available at: https://www.osce.org/secretariat/597756

Regardless of the approach taken, effective co-operation requires clearly defined roles, continuous communication and joint planning – especially in complex environments such as transportation hubs, where public and private security actors must co-ordinate closely.

Common elements of international guidance defining effective multi-stakeholder practices for CI protection include:

- Public–private partnerships that span the full security cycle – from planning and preparedness to response and recovery – and feature joint decision-making processes;
- Legal and regulatory frameworks and agreements, such as memoranda of understanding, that establish clear roles and facilitate information-sharing and data protection;
- Inclusive stakeholder engagement involving government, the private sector, civil society, academia and community leaders, and incorporating a gender perspective.

EFFECTIVE RISK MANAGEMENT

In UNSCR 2341 (2017), the Security Council called upon States to consider developing or further improving their strategies for reducing risks to CI from terrorist attacks, including, *inter alia*:

- assessing and raising awareness of relevant risks;
- taking preparedness measures, including implementing effective responses to such attacks and promoting better interoperability in security and consequence management; and
- facilitating effective interaction among all stakeholders involved.

Risk management is defined as a set of "coordinated activities to direct and control an organization with regard to *risk*".[87] Risk is distinct from threat, which may be defined as a credible attempt or intention to carry out an attack, based on the capabilities and motivations of perpetrators, but not taking into account existing security measures.

Since 2017, CTED has identified either significant gaps or a complete absence of risk management processes in nearly all assessed Member States with regard to countering terrorist threats to CI. In particular, CTED recommendations have encouraged States to ensure that risk management is a dynamic, multi-layered process that accounts for all threats and scenarios and is regularly updated on an ongoing basis. Risk management is an essential component in countering terrorist attacks on CI, as it enables governments and CI owners and operators to proactively identify, assess and mitigate risks before they materialize into attacks. Although terrorism is inherently unpredictable and adaptive, structured risk management allows authorities to prioritise resources, strengthen resilience and reduce exposure to high-impact threats.

One of the core strengths of risk management lies in its ability to tailor responses to specific contexts. By evaluating the likelihood and potential consequences of different terrorist scenarios – such as attacks using explosives or UAS against a CI site – decision-makers can implement proportionate and effective security measures. These may include hardening CI, enhancing surveillance and improving emergency response protocols.

87 International Organization for Standardization (ISO). 2018. ISO 31000:2018 – Risk management — Guidelines. Available at: https://www.iso.org/standard/65694.html#:~:text=What%20is%20ISO%2031000?,communicating%20risks%20across%20an%20organization
Also see: National Institute of Standards and Technology (NIST), Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST SP 800-37 Rev. 2. Available at: https://csrc.nist.gov/pubs/sp/800/37/r2/final

Moreover, risk management processes foster interagency co-ordination and strategic planning. They encourage the sharing of intelligence and information, the development of contingency plans and the training of personnel to respond to evolving threats. In the case of emerging technologies such as UAS, risk management helps anticipate misuse, assess vulnerabilities and guide the deployment of counter-measures. Ultimately, risk management shifts the focus from reactive crisis response to proactive prevention, making it a cornerstone of modern counter-terrorism strategies.[88]

COUNTER-UAS MEASURES

As described above, concern over the use of UAS for terrorist purposes has grown significantly worldwide in the past two years. In 2023, the CTC adopted the Abu Dhabi Guiding Principles, a set of non-binding guiding principles on the threats posed by the use of UAS for terrorist purposes.

In responding to this evolving threat, States are encouraged to adopt proactive measures such as mapping routine UAS activity to establish baselines and identify anomalies; conducting risk assessments to understand vulnerabilities and potential exploitation scenarios; and developing engagement protocols to train personnel in observing, documenting and safely interacting with UAS operators. These steps are essential to building a layered and adaptive defence, in particular to protect CI where UAS pose a unique threat. To strengthen UAS response capabilities, States should implement both upstream measures – such as national policies, legislation, border controls and regulation of UAS components – and downstream measures – including incident response, forensic exploitation and criminal justice processes. A capability maturity model provides a structured framework for systematically assessing the maturity of processes and practices, identifying gaps and helping States improve their preparedness. Effective countermeasures require interagency co-ordination, international co-operation and the integration of human rights considerations across all counter-UAS strategies.[89]

To effectively counter the UAS threat to CI, Member States should adopt a multi-layered security approach encompassing regulatory reform, public–private partnerships, counter-UAS technologies and stakeholder co-ordination. Integrating UAS threat assessments into security planning, deploying detection and interdiction systems, and enhancing law enforcement and intelligence capabilities are essential components to

88 Many countries and international organizations have developed CI risk management frameworks that are similar in structure and can be tailored to national contexts and sector specific CI. See for example the ICAO's Aviation Security Risk Assessment Methodology, which is designed to help States assess and manage risks to civil aviation, including airports and aircraft; UNOCT, CTED, INTERPOL. 2022. *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices*. Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf; European Commission. 2007. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33260&frontOfficeSuffix=%2F; U.S. CISA Critical Infrastructure Risk Management Framework. 2013. NIPP Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach. Available at: https://www.cisa.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf; OECD. 2025. Managing Emerging Critical Risks: Case Studies and Cross-Country Synthesis Report. Available at: https://doi.org/10.1787/1f9858ea-en; ECOWAS. 2024. Regional Critical Infrastructure Protection Policy. Available at: https://cyberportal.ecowas.int/download/72/critical-infrastructure-protection-policies/1753/ecowas-regional-critical-infrastructure-protection-policy-en.pdf; Critical 5. 2024. *Adapting to Evolving Threats: A Summary of Critical 5 Approaches to CI Security and Resilience*. Available at: https://www.cisa.gov/sites/default/files/2024-11/FINAL_Critical_5_Shared_Narrative.pdf; ASEAN. *ASEAN Critical Information Infrastructure Protection (CIIP) Framework*. Available at: https://www.etda.or.th/getattachment/2dc40cad-45fe-4433-874c-599d89525558/ASEAN-CIIP-Framework-2019.pdf.aspx; OAS. 2024. *A Practical Guide for Protecting Critical Infrastructure Against All Hazards*. Available at: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fscm.oas.org%2Fdoc_public%2FENGLISH%2FHIST_24%2FCP49174E03.docx&wdOrigin=BROWSELINK; United Nations Economic and Social Commission for Asia and the Pacific (ESCAP). 2020. *Risk-informed Infrastructure planning Central Asia Pilot in Kazakhstan and Kyrgyz Republic*, Asia-Pacific Information Superhighway (AP-IS) Working Paper Series. Available at: https://repository.unescap.org/server/api/core/bitstreams/8147f1f6-3fdd-436d-a030-cf84bfe844b6/content

89 UNCCT, CTED, UNIDIR, United Nations Global Counter-Terrorism Coordination Compact. 2022. Preventing Terrorists from Acquiring Weapons. 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. Available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Mar/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.pdf

a comprehensive response to the UAS threat.[90] In particular, law enforcement agencies and security practitioners should prepare for, test and defend against UAS threats in public spaces, at major events and around CI. Scenario-based testing, interagency co-ordination and legal compliance tailored to national contexts constitute recognized good practice.[91] Unlike conventional threats, UAS threats are more difficult to counter. At the same time, UAS can serve as an effective tool to address various threat scenarios and to enable national authorities to reach difficult or inaccessible locations.

ICAO has developed a regulatory framework to support the safe and secure integration of UAS into national airspace, particularly in response to the growing threat of their terrorist misuse.[92]
Key elements of this framework include:

- UAS traffic management;
- licensing and registration;
- a risk-based, operation-centric approach;
- integration with civil aviation law; and
- support for counter-UAS measures.

USEFUL SECURITY-ORIENTED TASKS

To better understand what is involved in the physical protection of CI, it is useful to begin with UNSCR 2341 (2017). In this resolution, the Security Council:[93]

- recognizes that "protection efforts entail multiple streams of efforts, such as planning; public information and warning; operational coordination; intelligence and information sharing; interdiction and disruption; screening, search and detection; access control and identity verification; cybersecurity; physical protective measures; risk management for protection programmes and activities; and supply chain integrity and security," and
- underlines that effective CI protection "requires sectoral and cross-sectoral approaches to risk management and includes, inter alia, identifying and preparing for terrorist threats to reduce vulnerability of critical infrastructure, preventing and disrupting terrorist plots against critical infrastructure where possible, minimizing impacts and recovery time in the event of damage from a terrorist attack, identifying the cause of damage or the source of an attack, preserving evidence of an attack and holding those responsible for the attack accountable".

The physical protection of CI relies on the implementation of comprehensive and integrated tasks encompassing policies, plans, measures and practices at CI facilities, underpinned by legislation and regulation from competent authorities. Since the adoption of UNSCR 2341 (2017), several guidance documents that consolidate good practices in areas such as national and local laws and regulations have been issued, including:

---

90 UNOCT. 2022. *Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS): Good Practices Guide: Specialized module*. Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod5-unmanned_aircraft_systems_final-web.pdf

91 INTERPOL. October 2023. *Stadia Protection and Mitigation from Drone Incursion and Threats: Guidelines for Testing and Evaluation of Counter Unmanned Aircraft Systems (C-UAS) Capabilities*. Available at: https://www.interpol.int/en/content/download/20515/file/Guidelines%20for%20Testing%20and%20Evaluation%20of%20C-UAS%20Capabilities-October%202023.pdf

92 International Civil Aviation Organization (ICAO). The ICAO UAS Toolkit [website]. Available at: https://www2023.icao.int/safety/UA/UASToolkit/Pages/default.aspx [accessed 6 October 2025]

93 UNSC. 13 February 2017. Resolution 2341 (2017) [S/RES/2341]. Available at: https://docs.un.org/en/S/RES/2341(2017)

OSCE (2025), *Technical Guide on Physical Security Considerations for the Protection of Critical Infrastructure from Terrorist Attacks:* Chapter 2 "Strategic and Legal Frameworks"[94]

UNOCT-CTED-INTERPOL (2022), *Compendium of Good Practices for the Protection of Critical Infrastructure Against Terrorist Attacks*[95]

UNOCT-CTED-UNAOC-UNICRI (2024) *Technical Guide on Protecting Critical Energy Infrastructure against Terrorist Attacks*[96]

In the following section, the (1) policies and plans, (2) measures and (3) practices that advance the physical protection of CI are examined in greater depth. While not a strict typology, this three-pillar approach helps to categorize the diverse tasks undertaken by CI owners and operators to strengthen CI physical protection. The OSCE *Technical Guide on Physical Security Considerations for the Protection of Critical Infrastructure from Terrorist Attacks* provides detailed guidance on these and related tasks. Here, only a selection of high-level considerations is drawn from the Guide and presented.

POLICIES AND PLANS

Policies and plans that support CI protection are typically the strategic governance tools guiding CI operations and personnel. They provide the framework within which physical protection is defined and implemented. As governance tools, they also represent a commitment by CI owners and operators to regulate or prepare for specific issues of concern. For example, personnel security policies may demonstrate a commitment to managing insider threats, while response plans for active shooter incidents reflect a commitment to protecting facility personnel and critical operations from such threats. Although it is not an exhaustive overview of the relevant policies and plans supporting effective CI protection, the OSCE Technical Guide identifies several categories in which policymaking and planning are particularly advantageous for addressing terrorist threats. These include:

- **Defining a CI facility's security system:** Implementing physical security measures begins with developing a cohesive policy framework for a security system tailored to the facility's unique profile and needs. Such a framework should comprise components that function together to provide an appropriate level of protection and enable it to absorb, adapt to and/or recov¬er rapidly from a range of threat scenarios, including terrorist attacks.
- **Pursuing PPPs:** PPPs are formal or informal co-operation arrangements between public authorities and private companies. Many private CI owners and operators bear primary responsibility for protecting their facilities and, in some cases, protective duties are outsourced to private security providers. Consequently, in preparing for, preventing and responding to terrorist attacks at CI sites, private stakeholders play a vital role.
- **Complying with human rights obligations and commitments:** Because physical protection and responses to terrorist threats at CI facilities may involve the use of force, armed security personnel, and the processing and analysis of personal data, it is vital that CI owners and operators maintain policy frameworks compliant with obligations under national and international law, including human rights law.

94 OSCE. 2025. *Technical Guide on Physical Security Considerations for Protecting Critical Infrastructure from Terrorist Attacks*. Available at: https://www.osce.org/secretariat/597756

95 UNOCT, CTED, INTERPOL. 2022. *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices*. Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf

96 UNOCT. September 2024. *Technical Guide on Protecting Critical Energy Infrastructure against Terrorist Attacks*. Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/vulnerable_targets_energy_guide_en_web.pdf

- **Planning for specific terrorist incidents:** Terrorist threats to CI facilities are diverse and may involve the use of vehicles, firearms, explosives, chemical, biological, radiological and nuclear materials, UAS, hostage-taking, or insider assistance. Each potential scenario – if assessed as relevant by competent authorities – may require specific plans to ensure an effective response. A key component of this is crisis communication, which should be integrated into such plans to prevent secondary challenges such as confusion, reputational damage, or unmanaged media coverage during an incident.
- **Managing insider threats:** The wide range of threats that insiders can pose to CI facilities has led to diverse policy approaches by CI owners and operators, enabling them to address the particular ways in which insiders may pose a threat to their organizations (both intentionally and unintentionally).
- **Managing periods of enhanced threat:** Every CI facility has a unique and dynamic threat profile. For terrorist threats, this profile may be shaped by global or regional events, terrorist group ideologies and capabilities, strategic objectives, and a range of other factors. When an increased threat level is assessed, a predefined policy framework specific to periods of enhanced threat should guide the measures and practices implemented as a response.
- **Planning for business continuity:** CI owners and operators must plan for a range of disruptive incidents, including terrorist attacks. Such plans typically form part of a broader business continuity management system that defines how an organization will maintain critical services and recover from disruptions.
- **Training and exercising for specific terrorist incidents:** Policies mandating professional development, training, and exercises are central to cultivating a resilient and security-conscious workforce at CI facilities.

MEASURES

Measures refer to the concrete alterations or improvements made to a CI facility to enhance its physical protection. Several examples are presented below for consideration by CI owners, operators and other stakeholders to further improve facility-level protection.

- **Intrusion detection measures:** Managing and detecting authorized and unauthorized entry is a key component of a CI facility's physical protection. This is typically achieved through an intrusion detection system (IDS). Using surveillance tools such as motion detectors, this system identifies changes in the target environment – such as the presence of an intruder – and alerts relevant personnel through alarms. In addition to surveillance and alarm functions, an effective IDS is supported by monitoring and response capabilities, either on-site or remotely.
- **Video surveillance measures:** These involve strategically placed cameras that provide visual monitoring, for example as part of an intrusion detection system. The effectiveness of video surveillance depends on the types and placement of cameras, as well as the procedures for monitoring video feeds and responding to incidents. Such systems can be deployed at access points, perimeters, areas of critical business operation and zones containing high-value or critical assets. Video surveillance systems should comply with local laws on data collection, storage and protection, and be necessary and proportionate.
- **Security lighting measures:** Lighting requirements vary among CI facilities depending on their specific needs and threat assessments. Security lighting should include measures against tampering or damage, and ensure standby power supplies for essential systems. Control panels for such systems should be located in secure areas with restricted access.
- **Perimeter security measures:** Maintaining a secure perimeter is essential to the physical protection of a CI facility. A well-secured perimeter controls access for vehicles and personnel, delays unauthorized entry and deters potential attackers. Perimeter elements may include fences, barriers (natural or man-made), dense vegetatio or other structural installations.

- **Access control measures:** Preventing unauthorized access is a central aspect of physical protection. CI owners and operators therefore implement a range of access control measures, located both externally (at the perimeter) and internally (to restrict access within the facility). These may include electronic access systems with specific protocols for sensitive areas.
- **Building structure and integrity:** The structural integrity of a facility is fundamental to its physical protection against a range of threats and hazards, including terrorist attacks. Relevant measures include design decisions concerning entrances and exits, walls, ceilings, floors, windows, mailrooms and HVAC systems.
- **Hostile vehicle mitigation measures:** Many CI owners and operators employ measures to prevent or mitigate vehicle-borne attacks. These may include specific access controls (e.g., Sally ports), road design decisions that limit vehicle speeds, and passive or active barriers placed at key locations.
- **Counter-UAS measures:** Where UAS threats are identified as relevant, mitigation options may include counter-UAS technologies, anti-UAS nets or fences, blast curtains and specialized window glazing incorporated into building or perimeter designs.
- **Redundancy measures:** These include back-up power supplies or other systems to ensure the continued operation of security systems such as video surveillance or access controls.

PRACTICES

Practices may refer to the routine activities carried out by facility personnel, private security and other relevant stakeholders at a CI facility in pursuit or support of physical protection objectives. These activities may be formally mandated by policies – such as visitor security screening – or informally adopted as part of the facility's broader security culture. A selection of relevant practices is presented below.

- **Developing a security culture at CI facilities is vital to the overall physical protection mission.** In this context, a robust security culture among all facility personnel comprises a set of practices that form a fundamental part of the organization's broader culture. These include actions such as recognizing and reporting potential hostile reconnaissance by threat actors or other suspicious behaviour.
- **Conducting routine multi-stakeholder and multi-agency exercises:** Exercising involves rehearsing specific skills or plans in a safe environment and engaging with all actors who could be affected by a potential incident in or near a CI facility. Such exercises should include all relevant stakeholders – including CI owners and operators, law enforcement, national and local government officials, emergency response authorities and others – and should be followed by an evaluation process to identify and address both strengths and shortcomings.

CONCLUSION

In 2017, the Security Council established a vital framework for addressing terrorist threats to CI through UNSCR 2341 (2017). This Report has highlighted several key aspects of the resolution, including the prerogative of each State to determine its own CI, the value of an all-threats and all-hazards approach, interagency co-operation and the central importance of risk management, PPPs and comprehensive protection strategies. A major outcome of the 2017 resolution has been its integration into CTED's assessment framework, which enables Member States to align with its provisions and allows CTED to identify progress, remaining gaps, priority areas for technical assistance, and good practices, trends and challenges. In this same period, the OSCE engaged its participating States both in support of the implementation of UNSCR 2341 (2017) and the unique commitments made by the OSCE participating States, including through innovative initiatives such as Project PROTECT.

All of this has taken place as the threat environment continues to evolve. This Report has highlighted several key aspects of the resolution, including the prerogative of each State to determine its own CI, the value of an all-threats and all-hazards approach, interagency cooperation and the central importance of risk management, PPPs, and comprehensive protection strategies. It is likely that the threat landscape will continue to evolve as terrorists and other threat actors adopt new tactics and adapt to law enforcement and private-sector countermeasures, all of which has implications for ongoing efforts to strengthen the physical protection of CI.

© Eddson Lens | pexels.com

Additionally, this Report identified several overarching trends affecting the CI protection ecosystem, particularly those related to technological advancements and policy developments. These include the growing convergence of cyber-physical systems, the integration of ICTs into CI operations, and the gradual shift in policy focus from protection to resilience. When examining national and sectoral approaches to CI protection, policymakers may wish to analyse these trends and assess how they are likely to shape the policy landscape for governments and CI owners and operators in the foreseeable future. With threats and trends identified, this Trends Report Update concludes by outlining areas for action – policies, plans, measures, and practices that can be implemented at CI facilities to enhance their physical protection against terrorist attacks.

Looking back on nearly a decade since the adoption of UNSCR 2341 (2017), it is clear that the continuous monitoring of terrorist threats, as well as of technological and policy developments impacting the CI protection landscape, remains vital. No country can function without the essential services its CI provides and that largely depends on physical infrastructure that requires effective protection. This Trends Report Update aims to provide policymakers in government and key security stakeholders in the private sector with new insights to support their adaptation to this rapidly evolving domain – an endeavour made all the more vital given 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".[97]

97 UNSC. 13 February 2017. Resolution 2341 (2017) [S/RES/2341]. Available at: https://docs.un.org/en/S/RES/2341(2017)

United Nations Security Council
Counter-Terrorism Committee
Executive Directorate (CTED)

Organization for Security and
Co-operation in Europe