

PROTECT

TECHNICAL GUIDE



**PHYSICAL SECURITY CONSIDERATIONS FOR
PROTECTING CRITICAL INFRASTRUCTURE
FROM TERRORIST ATTACKS**

The materials in this publication are for ease of reference only. Although the OSCE has invested the utmost care in its development, it does not accept any liability for the accuracy or completeness of any information, instructions and advice provided, as well as for misprints. The contents of this publication, the views, opinions, findings, interpretations and conclusions expressed herein are those of the authors and contributors and do not necessarily reflect the official policy or position of the OSCE and its participating States.

© 2025 Organization for Security and Co-operation in Europe (OSCE); www.osce.org

The OSCE Project PROTECT has received financial support from the United States of America and the Federal Republic of Germany.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means – electronic, mechanical, photocopying, recording, or otherwise without the prior written permission of the publishers. This restriction does not apply to making digital or hard copies of this publication for internal use within the OSCE and for personal or educational use when for non-profit and non-commercial purposes, providing that copies bear the above mentioned notice and a following citation:

OSCE Project PROTECT Technical Guide on Physical Security Considerations for Protecting Critical Infrastructure from Terrorist Attacks 2025 © OSCE

Design and Layout: Peno Mishoyan
Print: Druckerei Ferdinand Berger & Söhne GmbH
Image source: Envato Elements Pty Ltd & Shutterstock, Inc.

Action against Terrorism Unit
Transnational Threats Department
OSCE Secretariat
Wallnerstrasse 6 A.
1010 Vienna, Austria
Tel: +43 1 514 360, atu@osce.org

Contents

Acknowledgments	5
Foreword	7
Executive Summary	8
Acronyms and Abbreviations	9
1 Introduction	13
1.1 OSCE Mandate on Critical Infrastructure Protection from Terrorist Attacks	15
1.2 United Nations Mandate on Critical Infrastructure Protection from Terrorist Attacks	15
1.3 OSCE Project PROTECT Overview	16
1.4 Structure of this <i>Technical Guide</i>	17
1.5 Note on Critical Infrastructure Resilience	18
1.6 Note on Cybersecurity	22
2 Strategic and Legal Frameworks for Critical Infrastructure Protection	27
2.1 Critical Infrastructure Identification: Criteria and Processes	32
2.2 Policy Guidance on Risk Management	37
2.3 Emergency and Crisis Management	38
2.4 International Co-operation	42
3 Human Rights Considerations	49
3.1 Human Rights and their Application	51
3.2 Involvement of Third Parties in Protecting Critical Infrastructure	55
3.3 The Use of Force and the Rights to Life, Security and Humane Treatment	58
3.4 The Rights to Privacy, Data Security and Protection	64
4 Public–Private Partnerships	71
4.1 OSCE and United Nations Frameworks for Public–Private Partnerships to Protect Critical Infrastructure	71
4.2 Common Values as the Baseline for Public–Private Partnerships	73
4.3 Information-Sharing within Public–Private Partnerships	76
5 Terrorism Threat and Risk Assessment	81
5.1 How Do Terrorists Attack Critical Infrastructure?	83
5.2 Threat and Risk Assessments: Considerations and Differences	85
5.3 The Importance of an “All Threats and All Hazards Approach”	87
5.4 Assessing Risk	87
5.5 Managing Risk	89

6 Physical Security Measures	95
6.1 Conceptualizing Physical Security	97
6.2 Defensive Layers or Defence-in-Depth	100
6.3 Developing a Security System	101
6.4 Intrusion Detection Systems	104
6.5 Lighting	108
6.6 Video Surveillance Systems	110
6.7 Perimeter Security	113
6.8 Access Control Systems	115
6.9 Security Screening	119
6.10 Restricted Areas	121
6.11 Building Structure	122
7 Security Planning and Target Hardening	131
7.1 Terrorist Attack Planning through Hostile Reconnaissance	131
7.2 Security Planning for Hostile Vehicle Attacks	138
7.3 Security Planning for Explosive Attacks	148
7.4 Security Planning for Chemical, Biological, Radiological, and Nuclear Attacks	160
7.5 Security Planning for Firearms Attacks	168
7.6 Security Planning for Hostage Situations	171
7.7 Planning for Invacuation, Evacuation and Lockdowns	176
7.8 Business Continuity Management	180
7.9 Crisis Communications	181
8 Insider Threat Management	189
8.1 Defining Insider Threats	191
8.2 Factors Affecting Individuals' Likelihood to Engage in Hostile Insider Behaviour	196
8.3 Indicators of Hostile Insider Activity	196
8.4 Organizational Responses to Insider Threats	197
9 Training and Exercising	205
9.1 Training	207
9.2 Exercising	208
10 Enhanced Threat Escalation Options	215
10.1 National Terrorism Threat Assessments	215
10.2 Enhanced Threat Escalation Options	217
10.3 Costs of Enhanced Threat Escalation Options	219

Acknowledgments

The Action against Terrorism Unit of the OSCE Transnational Threats Department would like to express its sincere gratitude to the various participating States, experts, consultants and staff members who contributed to this *Technical Guide*.

Project PROTECT Technical Guide Expert Advisory Group (2024–2025)¹

Amin Boutaghane
Expert Lead
Civipol Project “Enhancing protection of public spaces and critical infrastructures in the Western Balkans”

Agnieszka Mizgalska
Aviation Security Technical Officer
Aviation Security and Facilitation,
Aviation Security Policy
International Civil Aviation
Organization

Camille Scotto de César
Policy Analyst, Chemical, Biological,
Radiological, Nuclear, Explosive and
Vulnerable Targets Sub-Directorate
Counter-Terrorism Directorate
INTERPOL

Dr. Ing. Martin Larcher
Senior Researcher for Security
and Defence
Space, Connectivity and Economic
Security Unit
Directorate for Societal Resilience
and Security
Joint Research Centre, European
Commission

Dr. Monica Cardarilli
Advanced Science for Policy
Researcher
Space, Connectivity and Economic
Security Unit
Directorate for Societal Resilience
and Security
Joint Research Centre, European
Commission

United Nations Global Programme
on Countering Terrorist Threats
against Vulnerable Targets:

- Ignacio Ibañez, Coordinator,
United Nations Office of Counter-
Terrorism
- Anne-Maria Seesmaa, Legal
Officer, Security Council Counter-
Terrorism Committee Executive
Directorate, United Nations
- Duccio Mazarese, Programme
Management Officer, United
Nations Interregional Crime and
Justice Research Institute

National Critical Infrastructure Team
Federal Policing National Security
Royal Canadian Mounted Police
Canada

Catherine Piana
Director General
Confederation of European
Security Services

Marybeth Kelliher
Senior Policy Advisor
Bureau of Counterterrorism
Department of State
United States of America

Johannes Heiler
Adviser on Anti-Terrorism Issues
Office for Democratic Institutions
and Human Rights
OSCE

Maximilian Scheid
Associate Human Rights Officer
Office for Democratic Institutions
and Human Rights
OSCE

Heiko Nils Hutter
Colonel, Military Adviser
Permanent Mission of Germany to
the OSCE
Federal Republic of Germany

Giulia Manconi
Senior Energy Security Officer
Economic and Environmental
Activities
OSCE

Deepak Chaturvedi
Chairperson
Physical Security Community
ASIS International

Daler Valiev
State Committee for National Security
Government of Republic of
Tajikistan

Assiya Mergalieva
Anti-terrorism Centre
Government of Republic of
Kazakhstan

Daniel Golston
Expert Advisory Group Chair and
Project PROTECT Lead
Action against Terrorism Unit
Transnational Threats Department
OSCE

Erlan Battalov
Anti-terrorism Centre
Government of Republic of
Kazakhstan

Julian Stafford
General Secretary
European Utilities Telecom Council

¹ This *Technical Guide* does not necessarily reflect the national or institutional positions of members of the Expert Advisory Group.

Technical Guide Experts

Dr. David BaMaung
Lead Expert
Physical Security and Personnel
Security Expert
Director, AbleSecurity Consultants
Honorary Professor, Glasgow
Caledonian University
Visiting Professor, Coventry
University

Stefano Betti
Legal Expert

Benjamin Greenacre
Human Rights Expert

Professor John Cuddihy FRSA
Threat and Risk Expert
Protective Security Lab
Coventry University

Dr. Alessandro Lazari
Independent Expert Reviewer
Centre for Interdisciplinary
Research on Critical Infrastructure
Security and Resilience
Department of Engineering for
Innovation
Università del Salento
Italy

OSCE Action Against Terrorism Unit Staff

Daniel Golston
Project PROTECT Lead

Kamila Sabyrrakhim
Project Assistant

Anna Gussarova
Assistant Project Officer

Alice Czimmermann
Project Assistant

This *Technical Guide* was edited by Cynthia Peck-Kubaczek, David Wells and Daniel Golston.

The OSCE wishes to thank the Infrastructure Security Division of the United States of America's Cybersecurity and Infrastructure Security Agency for its review.

Foreword

The modern world relies on access to electricity, energy, water, internet and other essential services. These are the services that underpin daily life in each and every OSCE participating State, and governments and critical infrastructure owners/operators dedicate notable effort to ensuring that these services remain available to us on a daily basis. Given the central importance of these essential services to our lives and economies, terrorists often target critical infrastructure in order to maximize harm.

The terrorist threat to energy infrastructure, international transportation and other critical infrastructure has been recognized by the 57 OSCE participating States, the United Nations Security Council and United Nations General Assembly – resulting in nearly twenty years of dedicated efforts from the OSCE.

Decades ago, the OSCE participating States called on the Organization to pursue activities that improve the security of international transportation and other critical infrastructure. Since then, the OSCE has worked with participating States to increase the protection of critical infrastructure through in-country capacity-building, facilitating regional dialogue and consolidating and sharing good practices.

The OSCE participating States hold a vast amount of experience in the field of critical infrastructure protection, as shown throughout this *Technical Guide*. The many good practices cited from across our membership are a testament to the depth and breadth of this knowledge and expertise.

We hope that this *Guide* brings valuable insights to participating States' policymakers, OSCE Partners for Co-operation, national critical infrastructure owners and operators, as well as all other actors involved in the protection of critical infrastructure. By sharing the guidance and good practice compiled in this *Guide* with both public and private stakeholders, we are confident we can improve our collective security against evolving terrorist threats and protect the essential services these terrorists threaten.

Ambassador Alena Kupchyna
Co-ordinator of Activities to Address Transnational Threats
OSCE Secretariat

Executive Summary

Critical infrastructure (CI) provides the essential services that enable the daily functioning of societies and economies across the entire OSCE area. As a result of their central importance, CI assets have historically been and continue to be targeted by violent extremist and terrorist organizations. The interconnected nature of CI networks means that a single attack can have cascading effects on other CI systems and services. This not only increases the disruptive impact of a single attack, but also provides additional media attention for the attackers themselves. For these reasons, improving the security of CI is a pressing priority for the entire OSCE area. And yet, while this is an important end goal, the path to it is often undefined.

With the exception of highly regulated CI sectors, detailed instructions on the physical security measures to be implemented at a facility level are not provided in many OSCE participating States. What exists is a complex web of practices, principles and non-binding guidance documents which governments, CI owners/operators and those with security duties at CI facilities must examine in order to ensure effective physical security for sites and facilities under their care.

This *Technical Guide* provides structured guidance on practices, principles and considerations that can enhance the physical security of permanent CI sites and facilities, with a view towards preventing, better preparing for and mitigating terrorist attacks. Its intended audience includes policymakers with oversight, advisory and/or regulatory roles vis-à-vis CI owners/operators in OSCE participating States, CI owners/operators themselves, and those with security duties at CI facilities (including private security providers). This *Guide* has been developed with a range of CI sectors, facilities and sites in mind, both in urban centres and in remote locations.

Importantly, rather than dictating a single approach to physical security, this *Guide* presents a range of publicly available practices in order to reflect the diverse approaches that currently exist. Most of the practices cited throughout this *Guide* are from OSCE participating States. This showcases the vast wealth of knowledge present in the OSCE's membership, as well as the importance of harvesting these practices and sharing them for the benefit of all.

The *Guide* is divided into several chapters which move from strategic matters, such as policy and legislative approaches to critical infrastructure protection (CIP), to compliance with human rights frameworks and technical considerations, such as designing intrusion detection and access control systems. Throughout, emphasis is placed on preparing and planning for a range of terrorist threat scenarios, such as hostage situations, firearms attacks and hostile vehicle attacks. Planning is also featured in sections dedicated to crisis communications, business and continuity management, training and exercising. Notably, around the OSCE area, CI sectors have a high degree of private sector penetration, which means that public-private partnerships are featured throughout the *Guide*. As much as possible, international and regional standards are signposted for further reading.

Acronyms and Abbreviations

ASF – anti-shatter films

CBR – chemical, biological and radiological

CBRE – chemical, biological, radiological and explosive

CBRN – chemical, biological, radiological and nuclear

CCTV – closed-circuit television

CEPES – critical entity of particular European significance

CER – Critical Entities Resilience (Directive) (the EU's Directive on the resilience of critical entities [2022/2557])

CI – critical infrastructure

CIP – critical infrastructure protection

CISA – (US) Cybersecurity and Infrastructure Security Agency

CJEU – Court of Justice of the European Union

CoE – Council of the European Union

CoESS – Confederation of European Security Services

DCAF – Geneva Centre for Security Sector Governance

DHS – (US) Department of Homeland Security

EAP – emergency action plan

ECHR – European Court of Human Rights

EN – European Standard

EU – European Union

FEMA – (US) Federal Emergency Management Agency

HRC – (UN) Human Rights Committee

HVAC – heating, ventilation and air conditioning

IAEA – International Atomic Energy Agency

ICAO – International Civil Aviation Organization

ICCPR – International Covenant on Civil and Political Rights

ICoCA – International Code of Conduct Association

IDS – intrusion detection system

IEDs – improvised explosive devices

IMO – International Maritime Organization

INTERPOL – International Criminal Police Organization

ISO – International Organization for Standardization

IT – information technology
LEP – law enforcement paradigm
MoU – memorandum of understanding
NATO – North Atlantic Treaty Organization
NNCEIP – non-nuclear critical energy infrastructure protection
NPSA – (UK) National Protective Security Authority
NSRA – National Security Risk Assessment (of the UK)
ODIHR – (OSCE) Office for Democratic Institutions and Human Rights
OECD – Organisation for Economic Co-operation and Development
OHCHR – (UN) Office of the High Commissioner for Human Rights
OSCE – Organization for Security and Co-operation in Europe
PBIED – person-borne improvised explosive device
PIDAS – perimeter intrusion detection and assessment system
PPP – public–private partnership
RBPSs – risk-based performance standards
UAS – unmanned aircraft systems (drones)
UK – United Kingdom
UN – United Nations
UNDP – United Nations Development Programme
UNDRR – United Nations Office for Disaster Risk Reduction
UNDSS – United Nations Department for Safety and Security
UNGA – United Nations General Assembly
UNITAD – United Nations Investigative Team to Promote Accountability for Crimes Committed by Da’esh/Islamic State in Iraq and the Levant
UNOCT – United Nations Office of Counter-Terrorism
UNODC – United Nations Office on Drugs and Crime
UNSC – United Nations Security Council
US – United States (of America)
VBIED – vehicle-borne improvised explosive device
VSS – video surveillance system



Introduction



//

Violent extremist and terrorist organizations across the OSCE area view critical infrastructure as a major target. Their propaganda, completed attacks and thwarted plots all point to a continued – if not increased – intent and capability to disrupt the critical services needed for our daily social and economic lives.

//

1 Introduction

Violent extremist and terrorist organizations across the OSCE area view critical infrastructure (CI) as a major target. Their propaganda, completed attacks and thwarted plots all point to a continued – if not increased – intent and capability to disrupt the critical services (also known as essential services) needed for our daily social and economic lives. Though the ideological motivations for these malicious actors are diverse, many eventually settle on CI as a target for violent attacks since it offers high impacts, media attention and propaganda value.



CI systems are interdependent, meaning a single attack can have cascading, amplifying effects. A successful attack on an electrical substation, for example, can cascade to other critical assets and disrupt hospitals, water treatment facilities, public transportation, emergency communications, etc. Impacts can range from a loss of life to major economic and social costs, a reduction in public confidence in government and an emboldening of terrorist organizations, both domestically and abroad. For these reasons, improving the security of CI is a pressing priority for the entire OSCE area.

While this is an important end goal, the path to it is often undefined. With the exception of highly regulated CI sectors, such as the nuclear energy sector, detailed guidance on the physical security measures to be implemented at a facility level is not provided in many OSCE participating States. What exists is a complex web of practices, principles and non-binding guidance documents which governments, CI owners/operators and those with security duties at CI facilities (including private security providers) must examine in order to ensure effective physical security for sites and facilities under their

care. This *Technical Guide* seeks to support these stakeholders by gathering experience and expertise from across the OSCE area and beyond and consolidating it in one place.

This *Technical Guide* provides structured guidance on practices, principles and considerations that can enhance the physical security of permanent CI sites and facilities, with a view towards preventing, better preparing for and mitigating terrorist attacks. This *Guide* has been developed with a range of CI sectors, facilities and sites in mind, not only in urban centres but also in remote locations.

Rather than dictating a single approach to physical security, the *Technical Guide* presents a range of publicly available practices from across the OSCE area and beyond, including from governments, international and regional organizations, and private actors. In this way, it reflects the diverse range of perspectives and approaches taken across the OSCE area to advance the common objective of strengthened physical security for CI sites and facilities.

While this document provides non-binding guidance, actual decisions on physical security arrangements and all matters explored in this *Technical Guide* should be made by competent stakeholders in a multidisciplinary fashion, meaning with involvement of and consultation with engineers and experts in legal matters, human rights, policing, counter-terrorism and other relevant disciplines, as appropriate. Moreover, these physical security arrangements should be made in compliance with international law, including international human rights law, national laws and local regulations. Nothing in this *Guide* should be seen as overriding such laws and regulations.

This *Technical Guide* is designed for policymakers with oversight, advisory and/or regulatory roles vis-à-vis CI owners/operators in OSCE participating States, CI owners/operators themselves, and those with security duties at CI facilities (including private security providers). However some of its contents may also be valuable for anyone interested in enhancing the physical security of their premises, including soft targets such as places of worship, hotels, concert halls, etc.

This *Technical Guide* focuses on physical security considerations. However, were a CI facility to come under terrorist attack, physical security measures alone cannot ensure its security; in many cases, they represent a last line of defence after other measures have failed. Physical security measures should be integrated with personnel security, procedural security and cybersecurity measures, which all work together to create a comprehensive and sustainable security framework for a given facility. As a result, at times, guidance veers into broader issues of counter-terrorism, crisis management, training and exercising, as well as other areas. This is due to the primary threat that this *Technical Guide* seeks to mitigate: terrorism. Given the dynamic terrorist threat and the fact that terrorist organizations can be highly capable and innovative with their attacks, all physical security frameworks should work as part of a broader security framework to provide adequate protection at a CI facility. Where necessary, this *Guide* touches on that broader framework.

It is important to note that this *Technical Guide* does not address the physical security of CI in situations of armed conflict. Nor is it designed to provide comprehensive guidance on the establishment of a national CI protection framework.

1.1 OSCE Mandate on Critical Infrastructure Protection from Terrorist Attacks

The protection of CI against terrorist attacks is firmly embedded in the OSCE's mandate, demonstrating almost two decades of political attention to this topic from the OSCE's 57 participating States. An early reference to critical infrastructure protection (CIP) is found in Ministerial Council Decision 5 (2007) on public–private partnerships in countering terrorism. In this Decision, the OSCE is instructed to promote the role of the private sector and civil society in its counter-terrorism activities, with specific attention paid to “identifying, prioritizing, and protecting critical infrastructure and addressing preparedness/consequence management issues.”² In the same year, the Ministerial Council adopted Decision 6 on protecting critical energy infrastructure from terrorist attacks. This Decision calls for co-operation with other organizations, exchanging best practices, and promoting public–private partnerships.³

Importantly, in 2012, the OSCE participating States agreed on the Consolidated Framework for the Fight Against Terrorism. It is in this Decision that the impetus of this *Technical Guide* can be found. The OSCE:

“will pursue its activities to enhance co-operation and build capacity at the national, regional and subregional levels to prevent and combat terrorism, *inter alia* in the areas of criminal justice, law enforcement, and border security and management, within a framework based on the rule of law and respect for human rights, in order to: [...] Improve the security of international transportation and of other critical infrastructure.”⁴

1.2 United Nations Mandate on Critical Infrastructure Protection from Terrorist Attacks

As a regional arrangement under Chapter VIII of the United Nations (UN) Charter, the OSCE contributes to the implementation of UN decisions including on counter-terrorism. Specific to the protection of CI, in 2017, the UN Security Council passed Resolution 2341 on the protection of CI against terrorist attacks. This resolution will be referenced multiple times in this *Technical Guide*.⁵

2 OSCE (2007), Ministerial Council Decision No. 5/07: Public-Private Partnerships in Countering Terrorism (MC.DEC/5/07). Available at: <https://www.osce.org/files/f/documents/3/e/29569.pdf> [accessed 14 May 2025].

3 OSCE (2012), Permanent Council Decision No. 1063: OSCE Consolidated Framework for the Fight against Terrorism (PC.DEC/1063). Available at: <https://www.osce.org/files/f/documents/7/5/98008.pdf> [accessed 14 May 2025].

4 OSCE (2012), Permanent Council Decision No. 1063: OSCE Consolidated Framework for the Fight against Terrorism (PC.DEC/1063), pp. 4–5. Available at: <https://www.osce.org/files/f/documents/7/5/98008.pdf> [accessed 14 May 2025].

5 UNSC (2017), Resolution 2341 (S/RES/2341). Available at: <https://documents.un.org/doc/undoc/gen/n17/038/57/pdf/n1703857.pdf> [accessed 5 May 2025].

Additionally, the UN Security Council's 2018 Addendum to the 2015 Madrid Guiding Principles on Foreign Terrorist Fighters provides guidance aimed at supporting the implementation of United Nations Security Council resolution 2341 (2017). These Principles and Addendum are also referenced in this *Guide*.⁶

Furthermore, in the UN Global Counter-Terrorism Strategy's eighth review in 2023, the UN General Assembly specifically calls for action on CIP in a counter-terrorism context:

"Further calls upon Member States to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect against, mitigate, investigate, respond to and recover from terrorist attacks, and emphasizes the need for States able to do so to assist in the delivery of effective and targeted capacity development, training and other necessary resources, and technical assistance, where it is needed, to enable all States to develop appropriate capacity to implement contingency and response plans with regard to attacks on critical infrastructure and public places ('soft' targets), and calls upon Global Counter-Terrorism Coordination Compact entities to continue providing capacity-building support to requesting Member States for the resilience of vulnerable targets".⁷

1.3 OSCE Project PROTECT Overview

In 2023, the OSCE Action against Terrorism Unit launched Project PROTECT, which seeks to enhance national approaches across the OSCE area on the protection of vulnerable targets from terrorist threats and other hazards. The term "vulnerable targets" refers to both CI and soft targets.⁸

6 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> [accessed 14 May 2025].

7 UN General Assembly (22 June 2023), *The United Nations Global Counter-Terrorism Strategy: eighth review*. Available at: <https://docs.un.org/en/A/RES/77/298> [accessed 12 May 2025].

8 There is no standard definition for a soft target at the OSCE. However, the United Nations Global Programme on Countering Terrorist Threats against Vulnerable Targets states: "Soft targets are broadly understood as being vulnerable sites – such as stadiums, shopping malls, theatres, religious institutions, pedestrian areas – that are easily accessible and open to the public and, for these reasons, have purposefully no or limited security measures in place. This feature, coupled with the large crowds that often gather therein, makes them appealing targets for terrorist actors bent on causing mass casualties and/or extensive destruction, without the need for significant planning, training or resources, but yielding disproportionate media coverage. The notion of soft targets escapes any precise definition also because of the extreme heterogeneity of the places that are commonly associated with it. Soft targets may be indoor or outdoor facilities, permanent or temporary spaces; and may vary in size, function, physical features, locations and users' profiles." See UN Office of Counter-Terrorism (UNOCT) (2022), *Protecting vulnerable targets from terrorist attacks: Good Practices Guide: Introduction*. Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod1-introduction_final-web.pdf [accessed 12 May 2025].

The Project is a multi-faceted initiative designed to build both national capacity and regional networks focused specifically on protecting vulnerable targets through three pillars:

- ▶ **Pillar 1:** Consolidating and disseminating specialized guidance and good practices on the protection of CI from across the OSCE area. This *Technical Guide* is a deliverable under this Pillar.
- ▶ **Pillar 2:** Enhancing national capacity to effectively protect vulnerable targets from terrorist attacks and other hazards through in-country awareness-raising and training.
- ▶ **Pillar 3:** Facilitating regional co-operation and dialogue among participating States and other stakeholders on the effective protection of vulnerable targets, including through public–private partnerships and engagement with civil society.

1.4 Structure of this *Technical Guide*

Effective physical security at CI facilities requires buy-in and commitment at the site level, the CI owner/operator’s corporate level, as well as from government policymakers. This *Technical Guide* provides guidance to these different actors, at both the senior and practitioner levels.

While often not the direct implementers of physical security measures at a site level, government policymakers provide the legal and strategic framework around which effective physical security is built. They draft and pass national legislation on CI protection, have the capability of regulating the activities of private sector CI owners/operators, and hold ultimate responsibility for the safety and security of their citizens. For this audience, Chapter 2, **Strategic and Legal Frameworks for Critical Infrastructure Protection** presents the various approaches taken by OSCE participating States by reviewing relevant laws, strategies and policies, and identifying several key commonalities, including the CI identification process, risk management approaches, emergency and crisis management, as well as international co-operation components. Chapter 3, **Human Rights Considerations**, follows by presenting human rights as a vital component of the effective protection of CI from terrorist attacks. CIP often involves private actors from CI owners/operators to private security providers, and thus **Public–Private Partnerships** are addressed in Chapter 4, with guidance provided on establishing common baseline values for such partnerships and sharing information on sensitive matters.

The second audience for this *Technical Guide* consists of the practitioners responsible for the security of CI facilities. The remainder of the *Guide* is designed for such practitioners. Nonetheless, it is highly recommended that they also review the three above-mentioned chapters.

Chapter 5, **Terrorism Threat and Risk Assessment**, provides a high-level overview of how the terrorist threat manifests at CI facilities and provides guidance on ways to manage terrorism risk while aligning with an “all threats and all hazards” approach.

Physical Security Measures are the focus of Chapter 6, beginning with ways to conceptualize the physical security framework as part of a larger security system for a CI facility. Specific physical security measures are then expanded upon, including intrusion detection systems, security lighting, video surveillance systems, access control systems and structural measures for buildings.

Chapter 7, **Security Planning and Target Hardening**, presents a range of measures to address many of the ways in which terrorists can disrupt a CI facility, from explosives to firearms attacks. This chapter emphasizes the range of plans that CI owners/operators should consider as part of their physical security mission.

While not necessarily an immediately obvious physical security measure, **Insider Threat Management**, the focus of Chapter 8, is a vital component of addressing the terrorist threat to CI. This chapter presents different types of insiders, indicators of hostile insider activities, as well as organizational measures to respond to such threats.

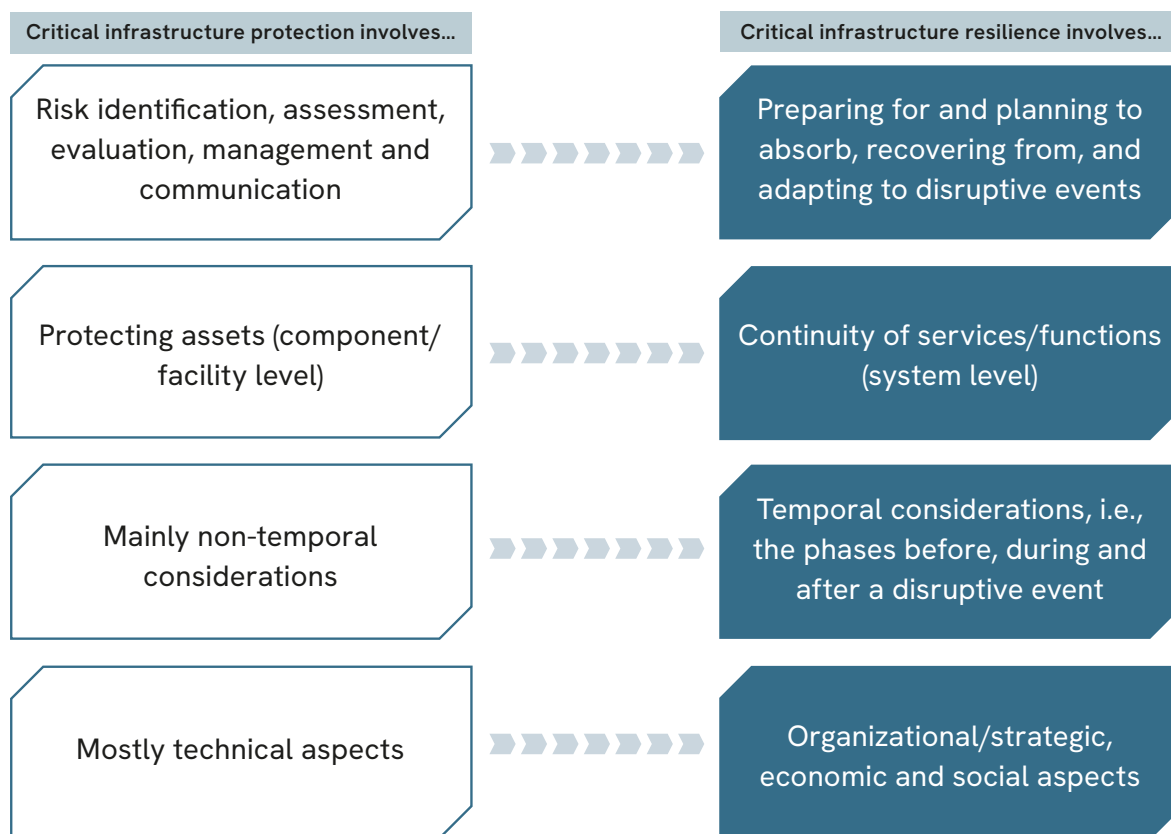
Chapter 9, **Training and Exercising**, underlines the importance of preparing a facility's workforce for security incidents, as well as the importance of exercising crises, including with local authorities. Doing so can ensure that in a real emergency, appropriate and possibly life-saving actions can be taken.

Since the terrorist threat itself is constantly evolving and involves both local and regional dynamics, CI owners/operators must be prepared to adapt their physical security measures in response. The final chapter of this *Technical Guide*, **Enhanced Threat Escalation Options**, expands on this concept.

1.5 Note on Critical Infrastructure Resilience

Efforts to enhance the physical security of CI are typically part of a broader approach by CI owners/operators and government actors to protect CI from a range of threats and hazards. One such threat is terrorism. In recent years CIP has increasingly been viewed by some policymakers as part of a broader approach to CI resilience. CI resilience incorporates many aspects of CIP, including physical security, but also provides a larger policy and operational framework that focuses on the continuity of CI services and functionality, rather than strictly CI asset protection. While this *Technical Guide* does not provide specific guidance on ways to enhance the resilience of CI facilities and sectors, if desired, its contents can be used by policymakers of participating States and others as a tool to contribute to greater CI resilience.

A useful way to conceptualize some differences between CI protection and CI resilience is presented below:⁹



⁹ Used with permission of Dr. Boris Petrenj: Petrenj, B., "Enhancing the Resilience of Critical Infrastructure to Terrorist Threats" [conference presentation, 22 November 2024]. See also: OSCE Critical Infrastructure Protection in Central Asia: Strengthening Resilience, Enhancing Security, Ashgabat 2024 [press release]. Available at: <https://www.osce.org/secretariat/581707> [accessed 12 May 2025].

The term CI resilience itself is defined differently by a range of stakeholders both within and outside the OSCE area:

Government/Organization	Resilience definition
Organisation for Economic Co-operation and Development (OECD)	"Resilience can be defined as the capacity of critical infrastructure 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". ¹⁰
United Nations Office for Disaster Risk Reduction	Resilience: "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." ¹¹
	"Infrastructure Resilience is the timely and efficient prevention, absorption, recovery, adaptation and transformation of national infrastructure's essential structures and functions, which have been exposed to current and potential future hazards. Implementing resilience across all disruption phases should be done through collaborative risk and uncertainty management, multi-hazard assessment, and methods that embrace the systemic nature of national infrastructure." ¹²
European Union's (EU) Directive on the resilience of critical entities	"[A] critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from incidents". ¹³
Australia ¹⁴	"[C]ritical infrastructure resilience refers to those aspects of organisational resilience that focus on measures to uplift the security and resilience of critical infrastructure owners, operators and supply-network stakeholders as a collective and across the whole economy." ¹⁵

Perhaps the clearest evidence of the aforementioned shift from CIP to CI resilience by policymakers is from the European Union (EU) in its 2022 EU Directive on the resilience of critical entities (2022/2557), known as the Critical Entities Resilience (or CER) Directive. In the preambular text of the Directive, which must be transposed into domestic legislation by all EU Member States, the previous EU Directive on CIP (2008/114/EC) was repealed and replaced with the CER Directive. A description of this process is below, which highlights the distinction between CIP and CI resilience:

"Council Directive 2008/114/EC [...] provides for a procedure for designating European critical infrastructure in the energy and transport sectors the disruption or destruction of which would have a significant cross-border impact on at least two Member States. That Directive focuses exclusively on the protection of such infrastructure. However, the evaluation of Directive 2008/114/EC conducted

10 OECD (2019), *Good Governance for Critical Infrastructure Resilience*. Available at: https://www.oecd.org/en/publications/good-governance-for-critical-infrastructure-resilience_02f0e5a0-en.html [accessed 11 March 2025].

11 UN Office for Disaster Risk Reduction (UNDRR) (2017), *The Sendai Framework Terminology on Disaster Risk Reduction*, Definition: Resilience. Available at: <https://www.undrr.org/terminology/resilience> [accessed 11 March 2025].

12 UN Office for Disaster Risk Reduction (UNDRR) (2017), *The Sendai Framework Terminology on Disaster Risk Reduction*, Definition: Resilience. Available at: <https://www.undrr.org/terminology/resilience> [accessed 11 March 2025].

13 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> [accessed 30 October 2024].

14 This definition is made only within the context of Australia's Critical Infrastructure Resilience Strategy.

15 Australian Government – Department of Home Affairs (February 2023), *Critical Infrastructure Resilience Strategy*. Available at: <https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf> [accessed 12 May 2025].

in 2019 found that, due to the increasingly interconnected and cross-border nature of operations using critical infrastructure, 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.”

Practice: United Nations Office for Disaster Risk Reduction’s Principles for Resilient Infrastructure (2022)¹⁶

In 2022, the United Nations Office for Disaster Risk Reduction (UNDRR) identified six principles, coupled with goals and guidance, for strengthening CI resilience and “improv[ing] the continuity of critical services provided by economic infrastructure systems”. The principles were designed to be used by “any level of government, institutions, donors, investors, owners, designers and contractors, service providers, and international organisations that are interested in implementing a set of actions that will improve national infrastructure resilience contributing to positive economic, social, and environmental outcomes.” The UNDRR published a handbook for implementing these principles in 2023.¹⁷

Principle	Description	Goal
1	Continuously learning	To develop and update understanding and insight into infrastructure resilience.
2	Proactively protected	To proactively plan, design, build and operate infrastructures that are prepared for current and future hazards.
3	Environmentally integrated	To work in a positively integrated way with the natural environment.
4	Socially engaged	To develop active engagement, involvement and participation across all levels of society.
5	Shared responsibility	To share information and expertise for co-ordinated benefits.
6	Adaptively transforming	To adapt and transform to changing needs.

Source: UNDRR

16 UNDRR (2022), *Principles for Resilient Infrastructure*. Available at: <https://www.undrr.org/publication/principles-resilient-infrastructure> [accessed 12 May 2025].

17 UNDRR (2023), *Handbook for Implementing the Principles for Resilient Infrastructure*. Available at: <https://www.undrr.org/publication/handbook-implementing-principles-resilient-infrastructure> [accessed 12 May 2025].

1.6 Note on Cybersecurity

Although this *Technical Guide* does not contain detailed references to cybersecurity, its importance as a part of a comprehensive approach to CIP must be acknowledged and emphasized. Many of the tools and services that facilitate the operation of CI – from industrial control systems to communications, heating, ventilation and air conditioning (HVAC) systems, and other technologies – are networked or connected to the internet and thus vulnerable to cyberattacks. As a result, local operations at a CI facility can be compromised by threat actors thousands of kilometres away. The International Security Ligue and Confederation of European Security Services (CoESS) acknowledge, “when devices in the field communicate back to network data centers, and computer systems are connected to the Internet, the attack surface expands exponentially.”¹⁸ While this *Technical Guide* does not address the cybersecurity challenge directly, as CI owners/operators adopt more emerging technologies to facilitate their operations, both physical and cyber risk management will become increasingly complex.



In many cases, OSCE participating States and security managers tasked with CIP approach CI security holistically – meaning their policies and practices account for and address both physical and cyber risks. Although the *Technical Guide* focuses on the physical security aspects of CI, this provides an opportunity to illustrate the importance and value of a holistic approach to security and resilience that identifies and integrates both cyber and physical measures. In 2023, the International Security Ligue and the CoESS stated:

¹⁸ International Security Ligue, CoESS (2023), *Cyber-Physical Security and Critical Infrastructure*. Available at: <https://www.bdswh.de/images/pdf/isl-coess-cyberphysicalsecurity-wp.pdf> [accessed 13 March 2025].

“Owners of critical infrastructure assets are embracing connected systems to enhance productivity and efficiency. Traditionally isolated devices in Supervisory Control and Data Acquisition systems and Industrial Control Systems now employ [the Industrial Internet of Things] to transmit data, from power plants to water treatment facilities. It is now common for computers and other technologies to be integrated into the design and function of physical infrastructure. Computers [...] are now integrated into physical infrastructure, which is most clearly observed in the development of ‘smart grid’ technology, where networked computers and communications technology work autonomously to resolve problems in the electric grid, manage energy use, and administer electricity generation. Automated traffic control has become part of transportation infrastructure and ‘smart’ water systems proactively monitor the health of their own physical infrastructure.”¹⁹

Physical and cybersecurity for CI facilitates are deeply intertwined: physical security at a CI facility can be compromised by a cyberattack, and cybersecurity at a facility can be impacted by a physical terrorist attack. This is referred to as the cyber-physical convergence and is an area of increasing concern to policymakers and CI owners/operators. The Cybersecurity and Infrastructure Security Agency (CISA) of the US Department of Homeland Security (DHS) provides examples of this phenomenon:

- ▶ “A security gap in access controls, such as unauthorized access to facilities or system permissions, can allow an individual to use a universal serial bus [...] device or other removable hardware to introduce a virus or malware into a network.
- ▶ Heating, ventilation and air conditioning (HVAC) systems can be virtually overridden, causing a rise in temperature that renders network servers inoperable.
- ▶ A cyber-attack on telecommunications can impair communication with law enforcement and emergency services, resulting in delayed response times.
- ▶ An unmanned aircraft system (UAS) can compromise sensitive information by gaining access to an unsecured network using wireless hacking technology.”²⁰

The interplay between physical and cybersecurity has been recognized at the policy level. 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”.²¹

19 International Security Ligue, CoESS (2023), *Cyber-Physical Security and Critical Infrastructure*. Available at: <https://www.bdsw.de/images/pdf/isl-coess-cyberphysicalsecurity-wp.pdf> [accessed 13 March 2025].

20 CISA (no date), *Cybersecurity and Physical Security Convergence*. Available at: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520and%2520Physical%2520Security%2520Convergence_508_01.05.2021.pdf [accessed 13 March 2025].

21 Council of the European Union (CoE), Council Directive 2008/114/EC 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), OJ L 333, para. 30. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555> [accessed 13 March 2025].

Thus while this *Technical Guide* focuses on the physical security threats associated with terrorist attacks, it encourages policymakers, CI owners/operators and other stakeholders to strengthen collaboration with their cybersecurity counterparts because “[w]hen security leaders operate in [cyber and physical security] siloes, they lack a holistic view of security threats targeting their enterprise”.²² Thus participating States and CI owners/operators may find value in breaking down silos between these communities and working towards a comprehensive approach to risk management at the facility, organizational and sector levels.

²² CISA (no date), *Cybersecurity and Physical Security Convergence*. Available at: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520and%2520Physical%2520Security%2520Convergence_508_01.05.2021.pdf [accessed 13 March 2025].

2

Strategic and Legal Frameworks for Critical Infrastructure Protection

ENHANCED
THREAT

TRAINING/
EXERCISING

INSIDER
THREAT

TARGET
HARDENING

PHYSICAL
SECURITY

RISK
ASSESSMENTS

PARTNERSHIPS

HUMAN RIGHTS

FRAMEWORKS

INTRODUCTION

//

Across the OSCE participating States, the basic concepts and approaches for infrastructure protection are most frequently defined in legal and policy instruments, within which physical security measures may be found.

//

2 Strategic and Legal Frameworks for Critical Infrastructure Protection

In United Nations Security Council (UNSC) Resolution 2341 (2017), the UN Security Council:²³

“Recogniz[es] that each State determines what constitutes its critical infrastructure, and how to effectively protect it from terrorist attacks, [...]”

“Calls upon Member States to consider developing or further improving their strategies for reducing risks to critical infrastructure from terrorist attacks, which should include, inter alia, assessing and raising awareness of the relevant risks, taking preparedness measures, including effective responses to such attacks, as well as promoting better interoperability in security and consequence management, and facilitating effective interaction of all stakeholders involved”.



In this chapter, different approaches taken by OSCE participating States are presented. They cover important dimensions of CIP, such as the CI identification process, risk management, emergency and crisis management, as well as international co-operation.

²³ UNSC (2017), Resolution 2341 (S/RES/2341). Available at: <https://documents.un.org/doc/undoc/gen/n17/038/57/pdf/n1703857.pdf> [accessed 5 May 2025].

It is important to note that this chapter does not cover all of the relevant strategic and legal frameworks that can affect CIP in a given country. For example, laws or regulations that permit or restrict the use of UAS (drones) impact who has access to this technology and for what purposes – all of which can affect CI security.

In many cases, these approaches provide a framework for CIP nationally. They represent a key part of the physical security puzzle and typically provide strategic-level guidance and instructions to relevant stakeholders. Facility-level physical security guidance (as presented in this *Technical Guide*), technical support to CI owners/operators, and the allocation of government funds all play a pivotal role in contributing to the effective implementation of these strategic and legal CIP frameworks.

As a note, many of the European practices referenced in this section may be subject to change since the entry into force in 2023 of the CER Directive, the European Union's Directive on the resilience of critical entities (2022/2557).

Across the OSCE participating States, the basic concepts and approaches for CIP are most frequently defined in legal and policy instruments providing the overarching framework for the protection of CI, within which physical security measures may be found. This begins with terminology defining CI itself, which ranges from critical infrastructure to “strategic objects”,²⁴ “vitally important installations”²⁵ and other terms.²⁶ Given this diversity, this *Technical Guide* does not attempt to provide a common definition for CI. This prerogative lies with each government, as affirmed in UNSC Resolution 2341 (2017).

In some cases, core components for CIP are found in dedicated cross-sectoral national strategies or action plans. These documents often set out the overarching parameters for the elaboration of detailed normative frameworks.

In other cases, basic principles for CIP are enshrined in dedicated legislative acts. The level of details contained in these laws varies significantly. For example, Slovenia's 2017 Critical Infrastructure Act²⁷ defines the notion of CI, regulates the criteria for its identification and designation, outlines the tasks of competent government agencies and CI owners/operators, and discusses information-sharing, data protection, as well as sanctions for failing to comply with the legal requirements. Luxembourg entrusts the task of regulating the designation of CI and determining the structure of owner/operators' security and business continuity planning to the executive wing of

24 Order of the Government of the Kyrgyz Republic No. 56/2015: About approval of Requirements to the mode of functioning and operation of strategic objects. Available at: <https://cis-legislation.com/document.fwx?rgn=73883> [accessed 12 November 2024] unofficial translation.

25 Code de la défense, Chapitre II : Protection des installations d'importance vitale, Articles R1332-1 à R1332-42 (2015, France). Available at: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006574323 [accessed 12 November 2024] unofficial translation. This practice may be subject to change following the entry into the force of the CER Directive.

26 In Estonia's National Defence Act, the phrase “national defence object related to the provision of a vital service” is used. See: National Defence Act (11 February 2015, Estonia). Available at: <https://www.riigiteataja.ee/en/eli/502042019010/consolide> [accessed 12 November 2024] unofficial translation. This practice may be subject to change following the entry into the force of the CER Directive.

27 Zakon o kritični infrastrukturi (22 December 2017, Slovenia). Available at: <https://pisrs.si/pregledPredpisa?id=ZAKO7106> [accessed 30 October 2024] unofficial translation. This practice may be subject to change following the entry into the force of the CER Directive.

government.²⁸ In some instances, the basic policy documents on CIP explicitly highlight physical security as a fundamental objective. In the national security strategy of the Netherlands, “ensuring a better protection of critical infrastructure” is a priority action for 2023–2027.²⁹

National Practice: Canada’s Strategic Emphasis on Cross-Sectoral Co-operation (2009)³⁰

A feature of Canada’s 2009 National Strategy for Critical Infrastructure is its focus on cross-sectoral approaches and initiatives. As Canada works to strengthen its approach to CI, promoting threat-informed cross-sector co-operation to advance shared objectives remains a key feature of Canada’s approach to CI security and resilience.

In line with this approach, Public Safety Canada – the governmental department responsible for matters of public safety, emergency management, national security and emergency preparedness – is working with key sectors to develop a robust, shared understanding of threats and interdependencies as the basis of effective cross-sector co-operation. One example of successful collaboration between sectors is a cross-sectoral study (led by the financial sector) to assess the level of interdependency of the financial, telecommunications and electricity critical infrastructure sectors. The study was jointly undertaken by experts from all three sectors, and it identifies opportunities for improved cross-sectoral resiliency, complete with actionable recommendations. Lessons learned from this success and others like it can encourage and inform future cross-sector collaborations.

Source: Public Safety Canada

Within the EU, a significant stimulus in legislative activity was initially provided by the 2008 Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.³¹ Building on the 2008 Directive, in Belgium, CIP-related legislation has been progressively expanded over the years, from its original scope limited to energy and transport (the two focus sectors of the 2008 Directive), to the areas of finance, health, water and critical information infrastructure.³² The EU’s 2008 Directive has also been transposed into national legislation by various EU candidate countries as part of their efforts to align with the EU legislative framework (known as the *acquis communautaire*). For example, Montenegro’s

28 Loi du 23 juillet 2016 portant création d’un Haut-Commissariat à la Protection nationale (29 July 2022, Luxembourg) Available at: <http://data.legilux.public.lu/eli/etat/leg/loi/2016/07/23/n1> [accessed 30 October 2024] unofficial translation. This practice may be subject to change following the entry into the force of the CER Directive.

29 Government of the Netherlands (3 April 2023) Security Strategy for the Kingdom of the Netherlands. Available at: <https://www.government.nl/documents/publications/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands> [accessed 5 May 2025].

30 Public Safety Canada (2009), *National Strategy for Critical Infrastructure*. Available at: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx#s0> [accessed 30 October 2024].

31 CoE Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345. Available at: <https://eur-lex.europa.eu/eli/dir/2008/114/oj> [accessed 30 October 2024].

32 Wet betreffende de beveiliging en de bescherming van de kritieke infrastructuur (15 July 2011, Belgium). Available at: https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2011070108&table_name=wet [accessed 30 October 2024] unofficial translation. This practice may be subject to change following the entry into the force of the CER Directive.

2019 legislation devotes a whole chapter that is designated “European Critical Infrastructure”.³³

Similar to the momentum generated by the 2008 Directive, the entry into force of the EU’s CER Directive in 2023 has sparked a wave of legislative reform across EU Member States.³⁴ The CER Directive repealed the aforementioned 2008 Directive and set a new foundation for CIP and resilience in the European Union and beyond. The CER Directive was adopted alongside a cybersecurity directive known as the NIS2 Directive.³⁵ The deadline for Member States to adopt and publish the measures necessary to comply with these two instrument was in October 2024. As an example, Germany’s parliament is in the drafting process of the “KRITIS³⁶ Umbrella Act”, which aims to implement the CER Directive by strengthening the resilience and physical protection of CI, complementing existing cybersecurity regulations.³⁷

In terms of the physical security of CI, the CER Directive’s Article 13 states:

“Member States shall ensure that critical entities take appropriate and proportionate technical, security and organizational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to [...] ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls”.³⁸

33 Zakon o određivanju i zaštiti kritične infrastrukture, Zakon o ZKI, 72/19 (30 January 2020, Montenegro). Available at: <https://www.gov.me/dokumenta/2585570a-cdff-420f-a7c4-0f67f19a6d8e> [accessed 28 November 2024] unofficial translation.

34 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> [accessed 30 October 2024].

35 EU (2022), Directive 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), OJ L 333. Available at: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng> [accessed 31 March 2025].

36 KRITIS stands for Kritische Infrastrukturen, German for “critical infrastructures”.

37 Some countries may experience institutional challenges in adopting cross-sectoral measures on CIP. In Switzerland, a recent opinion of the Federal Council highlighted that the presence of significant regulatory differences across CI subsectors in the country “is due in particular to the fact that the [federal level of government] does not have overall regulatory authority in this area. Such a competence should be created as part of a partial revision of the Federal Constitution”.

38 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> [accessed 30 October 2024].

From Critical Infrastructure Protection to Resilience: The European Union's Strategic Shift

In 2013, an evaluation of the status of implementation of the 2008 CI Directive revealed a number of challenges. It was observed, in particular, that “despite having helped foster European cooperation in the CIP process, the Directive [had] mainly encouraged bilateral engagement of Member States instead of a real European forum for cooperation. The sector-focused approach of the Directive likewise represents a challenge to a number of Member States, as in practice the analysis of criticalities is not confined to sectoral boundaries and follows rather a ‘system’ or ‘service’ approach (e.g., hospitals, financial services).”³⁹ Guided by the need to move from a sector-specific to a more systemic model, the European Commission led efforts to develop a new strategic approach.

The process resulted in the adoption of the CER Directive, which emphasizes the broad concept of “resilience”. This goes beyond the technical notion of “protection” by including overall operational continuity and the ability to prepare for, withstand, adapt to, and recover from various disruptions.

Basic approaches to CIP are also, in some cases, embedded within participating States’ broader frameworks on national security. For example, CIP takes central stage in the 2021 Slovak Republic’s Security Strategy,⁴⁰ and in Norway, a 2019 Act foresees a key co-ordinating role for the National Security Authority – a cross-sectoral professional and supervisory authority within the Ministry of Defence – in the implementation of the Act’s Chapter 7 “National critical objects and infrastructure”.⁴¹

As CI disruptions and their subsequent cascading effects can lead to situations of economic and societal paralysis or chaos, some participating States have entrenched CIP as a task in disaster- and emergency-related legislation. For example, in Poland, the legal basis for the national CIP programme is developed under the 2007 Crisis Management Act; the programme is updated every two years.⁴²

Across the OSCE area, a large number of CIP-related legal and policy frameworks implement an “all-hazard approach”, meaning they provide protective frameworks aimed at mitigating a range of threats and hazards to CI, whether these are of a natural (climate change, adverse weather, earthquakes) or human-induced (terrorism, criminal activity, negligence) origin. More information on this approach can be found below in Chapter 5, Terrorism Threat and Risk Assessment.

39 European Commission (2013), Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. Available at: https://home-affairs.ec.europa.eu/system/files/2020-09/swd_2013_318_on_epcip_en.pdf [accessed 19 May 2025].

40 Government of the Slovak Republic (2021), *Security Strategy of the Slovak Republic*. Available at: <https://www.mzv.sk/documents/30297/4638226/security-strategy-of-the-slovak-republic.pdf> [accessed 4 May 2025].

41 Government of the Kingdom of Norway (2019), Act relating to national security (Security Act). Available at: <https://lovdata.no/dokument/NLE/lov/2018-06-01-24> [accessed 30 October 2024].

42 Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 nr 89 poz. 590 (26 April 2007, Poland). Available at: <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20070890590> [accessed 30 October 2024] unofficial translation.

Other participating States structure CIP frameworks around a single type of threat, notably terrorism. For example, in the Kyrgyz Republic, the “Development and Implementation of Measures to Minimize the Consequences of Terrorist Acts for Strategic Objects” is a central pillar of its National 2023–2027 Counter-Terrorism Programme.⁴³

In analysing these various approaches for defining CIP by OSCE participating States’ governments, several basic principles can be extracted. These are presented in the table below.

Principle	Description
Shared responsibility	Safeguarding CI is a responsibility shared by public authorities (whether at the federal, state or local levels) and CI owners/operators.
Build partnerships	Strengthening CIP requires complementary and coherent action by all partners, from the private and the public sectors alike.
Continuous planning	CIP is based on an ongoing risk management process including threat assessment and mitigation.
Protection at all stages	Protective efforts should be ensured before, during and after CI disruptions in order for society to resist, manage, recover, and learn from incidents.
System-wide protection	The effectiveness of CIP depends on commitment from a range of stakeholders, including the public.
Proportionality	Protective measures should present an optimal balance between costs and perceived benefits.
Data exchange and data protection	Information sharing with relevant stakeholders and information protection are necessary and complementary prerequisites for CIP.

2.1 Critical Infrastructure Identification: Criteria and Processes

The process of identifying individual assets, systems and processes considered worthy of protection is complex and country-specific. In most cases, the criteria used to define specific sites and systems is highly sensitive and restricted. However, at the strategic level in many participating States, there is guidance on the process for identifying CI. As an initial step, many participating States determine or define CI sectors and sub-sectors.

⁴³ Cabinet of Ministers of the Kyrgyz Republic (15 March 2023), Programme of the Cabinet of Ministers of the Kyrgyz Republic on Countering Extremism and Terrorism for 2023–2027. Available at: <https://cbd.minjust.gov.kg/160032/edition/1241419/ru> [accessed 28 November 2024] unofficial translation.

Across many participating States there are often several CI sectors in common: energy, communication/information technology, transport, health, water management, food, finance and government.⁴⁴

Many of the European practices referenced in this section may be subject to change following the entry into the force of the CER Directive, in line with its Article 6 “Identification of critical entities”.

Overall, OSCE participating States employ different institutional processes for identifying and designating CI. Montenegro’s legislation allows the government to designate CI that does not fall within the pre-determined lists of critical sectors. The relevant ministries determine whether the systems, networks and facilities falling within their sectors meet the established criteria, and present their proposals to the state authority responsible for internal affairs. The latter submits the consolidated proposals to the government, which makes the final determination. CI owners/operators are required to inform the relevant ministries about changes affecting infrastructure that has been designated as critical, which may lead, following a governmental decision, to an amended national list of CI.⁴⁵ In Sweden, the process follows a collaborative, horizontal and non-hierarchical approach involving both central and local authorities. Responsibilities for identifying CI are assigned to municipalities, county councils, county administrative boards and national authorities based on their respective fields of responsibilities, including the geographical areas where the sites are located.⁴⁶ In France, the government does not identify CI directly. Instead, it designates “vital operators”, which are then in charge of identifying specific assets as critical.⁴⁷

44 Instead of generally identifying “government/public administration” as a critical sector, some countries choose to only highlight specific public services as being critical, as for example “emergency services” (in the Czech Republic, Germany, the Kyrgyz Republic, Poland, the United Kingdom, the United States). In Sweden, “social security” and “municipal technical services” are considered two autonomous critical sectors.

45 Zakon o određivanju i zaštiti kritične infrastruktura, Zakon o ZKI, 72/19 (30 January 2020, Montenegro) Available at: <https://www.gov.me/dokumenta/2585570a-cdff-420f-a7c4-0f67f19a6d8e> [accessed 28 November 2024] unofficial translation.

46 Swedish Civil Contingencies Agency (MSB) (2014), *Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure*. Available at: <https://www.msb.se/siteassets/dokument/publikationer/english-publications/action-plan-for-the-protection-of-vital-societal-functions--critical-infrastructure.pdf> [accessed 4 May 2025]. This practice may be subject to change following the entry into the force of the CER Directive.

47 Government of the French Republic (2015), Code de la défense, Chapitre II : Protection des installations d'importance vitale, Articles R1332-1 à R1332-42. Available at: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006574323 [accessed 12 November 2024] unofficial translation. This practice may be subject to change following the entry into the force of the CER Directive.

National Practice: France's Points of Vital Importance (2015)⁴⁸

In France, the steps for designating CI, known as “points of vital importance”, are outlined in the Defence Code:

- ▶ The Prime Minister develops a list of “sectors of vital importance” after consultation with an Interministerial Defence and Security Commission, and designates a “co-ordinating minister” for each identified sector.
- ▶ In each sector under their responsibility, the co-ordinating ministers notify infrastructure operators of their intention to designate them as “operators of vital importance”, based on the fulfilment of two conditions: i) their activity is carried out wholly or partly in a sector of vital importance; ii) they manage or use at least one establishment, structure or facility whose damage, unavailability or destruction as a result of malicious acts, sabotage or terrorism may have major consequences for the survival capacity of the nation or the health or life of the population.
- ▶ Notified operators have two months to present their observations. Once designated, they propose a list of “points of vital importance” as an annex to their security plans. The administrative authority then designates them as “points of vital importance”.

Source: Government of France

For the identification of individual assets, systems or processes as critical, many participating States apply both sectoral and cross-sectoral criteria. Sectoral criteria are typically determined by the ministries responsible for certain sectors and take into account the characteristics of those sectors. By contrast, cross-sectoral criteria are based on an assessment of the impact caused by a particular piece of infrastructure's disruption or destruction, usually in terms of “expected” casualties, economic effects or various social consequences (i.e., impact on public confidence, disruption of daily life, extent of environmental degradation). As two examples:

- ▶ Germany uses the “500,000 people threshold” as a benchmark. For example, a power plant is deemed critical if it has an installed net nominal capacity above 104 gigawatt, which equates to supplying over 500,000 people. The rationale is that outages affecting over 500,000 people cannot be adequately addressed with current emergency planning and operational capacities.⁴⁹
- ▶ In the Czech Republic, an executive order outlines the criteria used for CI identification in each critical sector. Under “water resource management”, for example, a source is considered critical if it is irreplaceable and provides water for at least 125,000 residents. In the health sector, the “criticality label” is assigned to, among others, medical facilities with a total number of at least 2,500 acute care beds.⁵⁰

48 Government of the French Republic (2015), Code de la défense, Chapitre II : Protection des installations d'importance vitale, Articles R1332-1 à R1332-42. Available at: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006574323 [accessed 12 November 2024] unofficial translation. This practice may be subject to change following the entry into the force of the CER Directive.

49 Government of the Federal Republic of Germany (2016), Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz. Teil 2: Berechnungsformeln zur Ermittlung der Schwellenwert. Available at: <https://www.gesetze-im-internet.de/bsi-kritisv/BSI-KritisV.pdf> [accessed 5 May 2025] unofficial translation. This practice may be subject to change following the entry into the force of the CER Directive.

50 Government of the Czech Republic (22 December 2010), Governmental Order No 432/2010 on the Criteria for the

As mentioned above, the criteria used by governments for CI identification purposes are not always in the public domain. In Croatia, these criteria represent classified information and are marked with the appropriate level of secrecy in accordance with special regulations on data secrecy.⁵¹

In addition to sectors and sub-sectors, some participating States have categories for CI that reflect different needs and administrative arrangements. Under Latvia's national security law, a key reason for distinguishing between Category A (deemed "Especially important CI") and Categories B and C (deemed "Important CI" and "CI", respectively) is to regulate which entity is in charge of implementing physical security measures.⁵² In the Netherlands, these distinctions are used as a guideline to prioritize the management of certain incidents and the development of capacities to increase resilience. Category A differs notably from Category B in that the former includes infrastructure for which disruption, damage or failure is expected to produce particularly severe economic, physical or social impact, as well as cascading effects.⁵³ In Estonia, CI is identified in Category B objects (deemed as providing a vital service); as a result the Ministry of Interior is defined as the entity in charge of co-ordinating protection efforts. By contrast, Category D objects (deemed as related to military operations) fall under the prerogative of the Ministry of Defence.⁵⁴

Identification of a Critical Infrastructure Element. Available at: https://nukib.gov.cz/download/publications_en/legislation/Order_432_2010_EN_v1.0_final.pdf [accessed 5 May 2025] non-binding English translation. This practice may be subject to change following the entry into the force of the CER Directive.

51 Zakon O Kritičnim Infrastrukturama (2 May 2013, Croatia). Available at: https://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1134.html [accessed 12 November 2024] unofficial translation. This practice may be subject to change following the entry into force of the CER Directive.

52 Latvia, Law on National Security (2000). Available at: <https://sab.gov.lv/files/uploads/2023/10/Law-on-National-Security.pdf> [accessed 18 May 2025] unofficial translation. For Category A, the implementing entities are determined by an individual Cabinet order. For Categories B and C, the implementation of physical security measures is borne by the CI operators. This practice may be subject to change following the entry into the force of the CER Directive.

53 Kingdom of the Netherlands, Ministry of Justice and Security, National Coordinator for Counterterrorism and Security (no date), Critical Infrastructure (protection) [webpage]. Available at <https://english.nctv.nl/topics/critical-infrastructure-protection> [accessed 23 July 2024]. This practice may be subject to change following the entry into the force of the CER Directive.

54 National Defence Act (11 February 2015, Estonia). Available at: <https://www.riigiteataja.ee/en/eli/502042019010/consolide> [accessed 12 November 2024]. This practice may be subject to change following the entry into the force of the CER Directive.

National Practice: Ireland's Methodology to Assess Infrastructure Criticality (2020)⁵⁵

As part of the Irish Department of Defence's Strategic Emergency Management Guideline on Critical Infrastructure Resilience, a "critical threshold" is "the level above which the impacts of loss are considered so severe that National Infrastructure falling into these levels should be considered CI." The Guideline further provides a six-step methodology that details the process for determining the level of an infrastructure's criticality:

Step 1

Consolidate "a list of essential services [...] which, if disrupted or destroyed would, [...] have the potential to have a significant impact on society."

Step 2

"Having identified essential services, document the assets 'essential' for service provision [...]. Each asset is now referred to as 'Examined Infrastructure'."

Step 3

"Identify other infrastructure which are connected with the Examined Infrastructure." For example, if an electric power station ("Examined Infrastructure") requires gas to produce power, that energy supplier is identified as "Required Infrastructure". If the electric power station produces power for water production, the water treatment plant is identified as a "Dependent Infrastructure".

Step 4

"Using a Scenario based approach, determine a [Reasonable Worst-Case Scenario] where a service is unavailable due to a disruptive shock."

Step 5

Evaluate the "criticality rating by assigning a score 1 to 5 for each impact factor". Impact factors include:

- ▶ Scope Impacts: People, concentration of people, geographical range
- ▶ Severity Impacts: Public, economic, environmental, dependence, political, psychological, international, "essential" services, security
- ▶ Time Related Impacts: Recovery time, duration of impact, impact peak

Step 6

After evaluating and assigning a score from 1 to 5 for each impact factor, calculate the Criticality Score by:

- ▶ Selecting "the single highest impact score from each Impact category (Scope, Severity and Time Related)."
- ▶ Multiplying "the highest score from each of the three Impact categories (i.e., Scope X Severity X Time Related). The calculated Criticality Score may range from 1 to 125."
- ▶ Plotting "the Criticality Score on the appropriate level to determine the overall Criticality Level of the infrastructure."

Source: Ireland's Department of Defence

⁵⁵ Department of Defence of Ireland (12 October 2020), Strategic Emergency Management Guideline 3 – Critical Infrastructure Resilience. Available at: <https://www.gov.ie/en/publication/7ff6f-strategic-emergency-management-sem-national-structures-and-framework/> [accessed 12 November 2024]. This practice may be subject to change following the entry into the force of the CER Directive.

In Germany's proposed law on CI (KRITIS-Dachgesetz), the government underlines that disruptions in specific CI sectors, in particular highly interconnected sectors with mutual dependencies, may lead to outages in many other sectors, potentially resulting in cascading service disruptions.⁵⁶ This example suggests that in every country, there is a small category of highly valuable CI sectors or facilities that are single points of failure, given the central role they play in complex interconnected CI networks. Even if they are not highlighted as a specific category in a country's legal or strategic framework, it is nonetheless important that every country identify such sectors and facilities and allocate appropriate measures for their protection and to ensure their resilience.

2.2 Policy Guidance on Risk Management

Risk management is a fundamental component of CIP, including physical security. This section presents policy guidance on aspects of risk management as defined in national strategic documents. More information on the risk management process can be found in Chapter 5, Terrorism Threat and Risk Assessment.

In the process of determining the nature and extent of threats against CI as part of the risk management process, legislation of various participating States envisages a role being played by CI owners/operators. This is reinforced by OSCE Ministerial Committee Decision 5/07 on public-private partnerships in countering terrorism, which "acknowledg[es] the usefulness of joint counter-terrorist efforts by government bodies and the private sector (civil society and the business community) in the form of voluntary co-operation [...] In this regard, efforts should particularly take due account of: [...] Identifying, prioritizing, and protecting critical infrastructure and addressing preparedness/consequence management issues".⁵⁷ Examples include:

- ▶ Under Slovenia's 2017 Law on Critical Infrastructure,⁵⁸ owners/operators prepare a risk assessment based on the methodology adopted by the Ministry of Defence, which acts as a co-ordinating agency in the field, as well as professional guidelines prepared by individual ministries in their respective fields of competence.
- ▶ In Estonia, the responsibility for determining the threat level for specific infrastructure sites lies with their owners/operators. However, owners/operators cannot set it at a lower level than the level established by the competent public authorities.⁵⁹

56 Deutscher Bundestag (27 November 2024), Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen, Drucksache 20/13961. Available at: <https://dserver.bundestag.de/btd/20/139/2013961.pdf> [accessed 5 May 2025] unofficial translation. This practice may be subject to change following the entry into the force of the CER Directive.

57 OSCE (30 November 2007), Ministerial Council Decision No. 5/07: Public-Private Partnerships in Countering Terrorism (MC.DEC/5/07). Available at: <https://www.osce.org/files/f/documents/3/e/29569.pdf> [accessed 5 May 2025].

58 Zakon o kritični infrastrukturi (Slovenia, 2017) Available at: <https://pisrs.si/pregledPredpisa?id=ZAKO7106> [accessed 28 November] unofficial translation. This practice may be subject to change following the entry into the force of the CER Directive.

59 Riigikaitseobjekti kaitse kord [Procedure for the protection of national defence objects] (Estonia, 27 April 2016). Available at: <https://www.riigiteataja.ee/akt/112032019033> [accessed 12 November 2024] unofficial translation. This practice may be subject to change following the entry into the force of the CER Directive.

At the CI owner/operator level, some participating States call for risk mitigation measures to be outlined in owner/operator-level security plans:

- ▶ Estonia's 2016 Procedure for the Protection of National Defence Objects sets minimum requirements specifically for the physical protection of CI.⁶⁰
- ▶ In the Kyrgyz Republic, detailed security requirements for owners/operators of strategic sites include access control measures – including physical measures – as well procedures for the timely detection of vulnerabilities and the identification of suspicious individuals seeking to enter protected premises.⁶¹

The laws of several participating States see training for CI owners/operators and relevant personnel as a key component in the risk management process:

- ▶ In Montenegro, the planning and delivery of training is the responsibility of the security co-ordinator appointed at the level of an individual CI facility.⁶²
- ▶ In Switzerland's 2023 National Strategy on CIP, training and exercises are identified within the "Resilience Cycle" as key tools to consolidate envisaged protection measures.⁶³

2.3 Emergency and Crisis Management

In relation to CI, emergency and crisis management procedures generally refer to the processes in place for responding to and managing disruptive events or major incidents at CI facilities that affect their services. Broadly speaking, three overarching legal approaches dealing with crises affecting CI have emerged across the participating States. Under the first approach, there are no crisis management provisions specifically aimed at CI. The legal framework generally applicable to emergency preparedness thus covers crisis scenarios affecting CI only indirectly.

60 Riigikaitseobjekti kaitse kord [Procedure for the protection of national defence objects] (Estonia, 27 April 2016). Available at: <https://www.riigiteataja.ee/akt/112032019033> [accessed 12 November 2024] unofficial translation. This practice may be subject to change following the entry into the force of the CER Directive.

61 Order of the Government of the Kyrgyz Republic No. 56/2015: About approval of Requirements to the mode of functioning and operation of strategic objects. Available at: <https://cis-legislation.com/document.fwx?rgn=73883> [accessed 12 November 2024] unofficial translation.

62 Zakon o određivanju i zaštiti kritične infrastrukture, Zakon o ZKI, 72/19 (30 January 2020, Montenegro). Available at: <https://www.gov.me/dokumenta/2585570a-cdff-420f-a7c4-0f67f19a6d8e> [accessed 28 November 2024] unofficial translation. This practice may be subject to change following the entry into the force of the CER Directive.

63 Nationale Strategie zum Schutz kritischer Infrastrukturen (16 June 2023, Switzerland). Available at: <https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2024/03/07/3159c04b-ffc8-4f4e-b72f-cba6b6a800e.pdf> [accessed 2 May 2025] unofficial translation.

National Practice: Sweden's System for Civil Emergency Planning⁶⁴

The Swedish system for civil emergency planning is co-ordinated by the Civil Contingencies Agency, which implements an “all-hazards” approach encompassing CI. This approach includes emergency planning, preparedness, response and recovery. To address CI interdependencies, the planning and resource allocation for peacetime emergency preparedness is built around the principle of stakeholders’ joint responsibility. This means that whichever entity is responsible for an activity in normal conditions should maintain that responsibility during emergencies and should also initiate any cross-sectoral co-operation.

Source: International Association of Emergency Managers

For example, Hungary’s Law on Disaster Prevention focuses on facility operators⁶⁵ – whether critical or not – dealing with hazardous substances. It requires them to develop internal protection plans, investigate the circumstances of any serious accidents, send incident reports to the industrial safety authority, and other tasks.

Under the second approach, provisions for CI crisis management are explicitly embedded in emergency/disaster preparedness legislation. For example, Estonia’s 2017 Emergency Act⁶⁶ defines the respective tasks of central and local authorities in managing the continuity of critical services, and establishes these authorities’ co-ordination, advisory and supervisory roles vis-à-vis CI owners/operators.

Under the third approach, the crisis management provisions applicable to CI are found in CIP-related laws in addition to other provisions dealing with, *inter alia*, CI identification and risk assessment. These norms often complement the text of general crisis management statutes, for instance by dealing with the division of labour between the agencies specifically in charge of CIP and those generally in charge of disaster management. For example:

- ▶ According to Serbia’s 2018 Law on Critical Infrastructure,⁶⁷ crisis management is undertaken by the Headquarters for Emergency Situations, while the Ministry of Internal Affairs – which acts as the co-ordinating entity for CIP – has a facilitating role providing professional support and needed data and information.
- ▶ The Annex to Poland’s National Programme on Critical Infrastructure Protection⁶⁸ provides detailed guidance on the preparation of business continuity and recovery plans. Practical advice includes storing CI plans in a safe and secure

64 International Association of Emergency Managers (IAEM) (no date), Civil Emergency Planning/Crisis Management in Sweden. Available at: <https://www.iaem.org/portals/25/documents/CivilEmergencyPlanningSweden.pdf> [accessed 5 May 2025].

65 2011. évi CXXVIII. Törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról (2011, Hungary). Available at: <https://njt.hu/jogszabaly/2011-128-00-00> [accessed 29 November 2024] unofficial translation.

66 Emergency Act (3 March 2017, Estonia). Available at: <https://www.riigiteataja.ee/en/eli/511122019004/consolide> [accessed 29 November 2024].

67 Zakon o kritichnoj infrastrukturi: 87/2018-41, Sluzhbeni glasnik RS, broj 87 od 13. novembra 2018 (13 November 2018, Serbia), Available at: <https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2018/87/8> [accessed 29 November 2024] unofficial translation.

68 Critical Infrastructure (26 April 2007, Poland). Available at: <https://archiwum.rcb.gov.pl/en/critical-infrastructure> [accessed 29 November 2024].

place, co-ordinating with other CI owners/operators regarding planned renovations and downtime of similar CI infrastructure, and periodically testing business continuity and recovery plans.

In some cases, CIP-related legislation requires that provisions on emergency planning and response be embedded in the security plans of CI owners/operators:

- ▶ Under Montenegro's legislation, owners/operators' security plans shall include, among other things, a description of measures aimed at ensuring the functioning of CI in the case of service disruption, as well as measures aimed at mitigating the consequences of such disruption.⁶⁹
- ▶ Latvia's government has approved guidelines⁷⁰ setting minimum requirements for planning the continuity of CI operations in case of a threat to national security. The guidelines discuss issues such as timelines and priorities for restoring critical services, the minimum human resources needed for ensuring critical functions, the identification of alternative working premises, and the type of support required from State authorities.

National Practice: The Kyrgyz Republic's Exercises on Emergency Planning and Management (2024)⁷¹

In 2024, the Kyrgyz government approved a regulation setting forth various types of mandatory exercises to be conducted at the CI site level. One type of exercise is designed to assess the level of preparedness for possible acts of terrorism. It requires that the competent security bodies surreptitiously penetrate the site either via regular checkpoints (i.e., using a forged accreditation document) or by gaining access outside the official entry points (i.e., exploiting a vulnerability in the external perimeter). For each exercise, the organizers develop a scenario that is not communicated to the site's security personnel. If necessary, following the exercise recommendations are sent to the heads of the concerned facilities to address detected weaknesses.

Source: Government of the Kyrgyz Republic

69 Zakon o određivanju i zaštiti kritične infrastrukture, Zakon o ZKI, 72/19 (30 January 2020, Montenegro) Available at: <https://www.gov.me/dokumenta/2585570a-cdff-420f-a7c4-0f67f19a6d8e> [accessed 28 November 2024] unofficial translation.

70 Procedures for Surveying Critical Infrastructure, including European Critical Infrastructure, and for Planning and Implementation of Security Measures and Continuity of Operation (Cab. Reg. No. 508) (6 July 2021, Latvia) Available at: <https://www.vvc.gov.lv/en/laws-and-regulations-republic-latvia-english/cab-reg-no-508-procedures-surveying-critical-infrastructure-including-european-critical-infrastructure-and-planning-and-implementation-security-measures-and-continuity-operation-amendments-08032022> [accessed 2 December 2024]. This practice may be subject to change following the entry into the force of the CER Directive.

71 Resolution 97/2024 of the Cabinet of Ministers of the Kyrgyz Republic: Approval of the regulations on educational, practical and preventive activities aimed at identifying the state of anti-terrorist protection of strategic sites vulnerable to terrorism (7 March 2024, the Kyrgyz Republic). Available at: https://online.zakon.kz/Document/?doc_id=35699774&show_di=1 [accessed 4 December 2024] unofficial translation.

National Practice: Ukraine's Passport for Critical Infrastructure Facility Protection (2023)⁷²

A Resolution of the Cabinet of Ministers of Ukraine lays out a procedure for CI owners/operators to develop a safety data sheet or "passport" for CI facilities and defines the official approval process. Each CI facility passport contains a title page, general characteristics of the facility, its protection plans and security assessment reports. Facility protection plans are subject to mandatory approval by the Ministry of Health, Ministry of Defence, State Service for Special Communications, State Emergency Service and National Police. Specifically for terrorist and other threats, additional approvals are required: "In the event of a threat of sabotage, terrorist acts, acts of cyberterrorism against control systems, operational and other systems of critical infrastructure facilities, emergencies or other dangerous events at critical infrastructure facilities, incidents related to violations of physical security and cybersecurity systems and other project threats at the national, sectoral and facility (if any) level and potential negative consequences for critical infrastructure facilities, protection plans are subject to mandatory approval by the State Security Service, the National Guard, and other state bodies."

Source: Government of Ukraine

National Practice: Kazakhstan's Passport for the Protection of Facilities Vulnerable to Terrorism (2023)⁷³

A Joint Order of Kazakhstan's Ministry of Internal Affairs and its Chairman of the National Security Committee establishes a standard data sheet or "passport" for the protection of facilities vulnerable to terrorism. The Order was adopted in June 2023 and tasks the Ministry of Internal Affairs with its implementation. The passport contains information about the facility in question: its characteristics (capacity, parking spaces, number of buildings/rooms), protective measures, security arrangements, building floor plans, etc.

Source: Government of Kazakhstan

72 Poriadok rozroblennia ta pogodzhennia pasporta bezpeki na ob'ekt kritichnoï infrastrukturi (4 August 2023, Ukraine) Available at: <https://zakon.rada.gov.ua/laws/show/818-2023-%D0%BF#n9> [accessed 4 December 2024] unofficial translation.

73 Ob utverzhdenii tipovogo pasporta antiterroristicheskoi zashchishchennosti obiektoiv, uiazvimykh v terroristicheskoe otnoshenie (29 June 2023, Kazakhstan). Available at: <https://adilet.zan.kz/rus/docs/V2300032950> [accessed 4 December 2024] unofficial translation.

Non-governmental actors also provide guidance on crisis management to private stakeholders, such as CI owners/operators.

Practice: American Petroleum Institute Oil and Natural Gas Industry Preparedness Handbook (2022)⁷⁴

The Handbook of the American Petroleum Institute provides information on how to prepare for a crisis at the State and local levels to support resilience and restoration of services:

- ▶ Know who does what: establish contacts and understand responsibilities in preparation;
- ▶ Know what not to do: do not share confidential or proprietary information during an event;
- ▶ Know what matters: understand the importance of assets and resources for the reliable operation of the system;
- ▶ Practice, practice, practice: test the process through drills and exercises in order to ensure that the correct relationships have been established, the correct information has been collected, and the correct mechanisms are in place.

Source: American Petroleum Institute

2.4 International Co-operation

The economies and societies of the OSCE's participating States are closely interconnected. This means that disruptions in CI, such as transportation networks, energy grids or financial systems, can have cascading effects – including across borders. This can occur not only when CI is physically shared by two or more countries, but also when CI that is entirely located in one country delivers a critical service to another. And yet, in only a few instances do domestic policies/legislation on CIP contain provisions for international co-operation. When they do, in most cases these provisions merely affirm in broad terms the need to strengthen protection efforts by reaching out and co-ordinating with foreign countries. For example, Ireland's governmental guidelines on CI resilience stress the importance of international collaboration to fully understand supply chain vulnerabilities, and to implement co-ordinated, non-competing global security and resilience measures.⁷⁵ Another example is the Security Strategy of the Netherlands, which emphasizes the need for international commitments for identifying and reducing dependencies in production chains, services and sectors. Such commitments are considered an integral part of risk assessments.⁷⁶

⁷⁴ American Petroleum Institute (Washington DC, 2022), *Oil and Natural Gas Industry Preparedness Handbook*, p. 24. Available at: <https://www.api.org/-/media/files/policy/safety/ong-industry-preparedness-handbook.pdf> [accessed 5 May 2025].

⁷⁵ Department of Defence of Ireland (2021), *Strategic Emergency Management: Guideline 3 - Critical Infrastructure Resilience (Version 2)*. Available at: <https://assets.gov.ie/90683/7d83eda8-4ff1-4a42-9c22-2d614c8a2d28.pdf> [accessed 5 May 2025]. This practice may be subject to change following the entry into the force of the CER Directive.

⁷⁶ Government of the Netherlands (3 April 2023), *Security Strategy for the Kingdom of the Netherlands*. Available at: <https://www.government.nl/documents/publications/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands> [accessed 4 December 2024].

The EU's CER Directive represents a notable effort to establish a co-operative framework on CIP at the EU level. The Directive introduces the notion of "critical entity of particular European significance" (CEPES), which is defined as an entity providing critical services to, or in, six or more EU Member States. As such, CEPES will be subjected to a regime of advisory missions (organized and financed by the European Commission) that aim to assess the measures that that critical entity has put in place to meet its obligations. When an entity does not qualify as a CEPES, the CER Directive still imposes an obligation to consult among Member States in relation to shared CI, or CI that provides critical services across borders, or CI that is connected with, or linked to, critical entities in other Member States. The CER Directive also sets up a regime for incident notification domestically and across Member States. The regime includes strict requirements for reporting timelines.

At the bilateral level, Canada and the United States are bound by a complex web of agreements, plans and procedures establishing various types and levels of mutual co-operation on CIP.⁷⁷ These arrangements attest to the incremental and pragmatic approach taken by these two countries in extending reciprocal support on a growing number of critical sectors and activities. Key instruments include:

- ▶ 2004 Agreement for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security (establishing a vehicle for the conduct of co-operative scientific and technological research and development);⁷⁸
- ▶ 2009 Agreement on Emergency Management Cooperation (setting up a Consultative Group);⁷⁹
- ▶ 2009 Framework for the Movement of Goods and People Across the Border During and Following an Emergency (including notably emergencies following an attack or threat of attack);⁸⁰
- ▶ 2010 Action plan for Critical Infrastructure (designing a comprehensive cross-border approach to CIP and resilience).⁸¹

77 US DHS & Public Safety Canada (2022), *Compendium of US - Canada emergency management assistance mechanisms*. Available at: https://www.dhs.gov/sites/default/files/2022-03/22_0329_us-canada-em-assistance-mechanism-compendium.pdf [accessed 5 May 2025].

78 Agreement Between the Government of the United States of America and the Government of Canada for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security (1 June 2004). Available at: https://www.dhs.gov/xlibrary/assets/agreement_us_canada_sciencetech_cooperation_2004-06-01.pdf [accessed 5 May 2025].

79 Agreement Between the Government of the United States of America and the Government of Canada on Emergency Management Cooperation (12 December 2008). Available at: <https://www.state.gov/wp-content/uploads/2019/02/09-707-Canada-Emergency-Management-Cooperation.pdf> [accessed 5 May 2025].

80 Canada-United States Framework for the Movement of Goods and People Across the Border During and Following an Emergency (17 May 2009). Available at: https://www.dhs.gov/xlibrary/assets/border_management_framework_2009-05-27.pdf [accessed 5 May 2025].

81 Canada-United States Action Plan for Critical Infrastructure (2010). Available at: <https://www.cisa.gov/sites/default/files/publications/ip-canada-us-action-plan-2010-508.pdf> [accessed 5 May 2025].

At the subregional level, one example of a cross-border mechanism is the memorandum of understanding (MoU) signed in 2006 by the Benelux countries.⁸² This instrument aims to enhance co-ordination in risk and crisis management, including public communication and the organization of joint exercises. The MoU applies to an “incident or accident occurring or threatening to occur in the territory of one of the Parties and having, or potentially having, cross-border consequences, whether the crisis is of natural, technical or human origin.” Although the Benelux MoU was signed before its signatories had adopted CIP-dedicated laws, it nevertheless applies to incidents affecting assets and networks that are commonly regarded as critical, particularly in the transport and energy sectors.

Regional Practice: Nordic participating States’ Collaborative Platform (2020)⁸³

In 2017, Finland, Norway and Sweden further developed their trilateral co-operation to prepare for potential disruptions to cross-border flows of critical goods and services. The result was a report covering the following “societal sectors”: communications and digital networks, energy, food, financial infrastructure, pharmaceuticals and transport.

The report identified various concrete actions aimed at informing the policymaking communities of the three countries. For example:

- ▶ In the energy sector, it was suggested to widen the informational base needed for improved policy coherence and to engage in joint undertakings to map cross-dependencies with other sectors.
- ▶ In the food sector, it was proposed to examine how Norway and Sweden might replicate how Finland had enhanced resilience in its food distribution channels by ensuring that more than three hundred retail shops would retain access to electricity during power outages or other disruptions.
- ▶ With regard to crisis management, the report recommended conducting a preliminary investigation assessing mutual availability in different kinds of emergencies of tank trucks, cargo containers and other transport infrastructure.

82 Memorandum van overeenstemming inzake de samenwerking op het terrein van de beheersing van crisissen met mogelijke grensoverschrijdende gevolgen tussen het Koninkrijk België, het Koninkrijk der Nederlanden en het Groothertogdom Luxemburg (1 June 2006). Available at: <https://wetten.overheid.nl/BWBV0003156/2012-03-01> [accessed 4 December 2024] unofficial translation.

83 Aula, I.; Amundsen, R.; Buvaro, P.; Harrami, O.; Lindgren, J.; Sahlén, V.; Wdebrand, C. (2020), *Critical Nordic Flows: Collaboration between Finland, Norway and Sweden on Security of Supply and Critical Infrastructure Protection*. Available at: <https://rib.msb.se/filer/pdf/29100.pdf> [accessed 4 December 2024].



Additionally, international co-operation as it relates to terrorism and criminality can be facilitated by international and regional organizations. For example, the International Criminal Police Organization (INTERPOL) “ensure[s] and promote[s] the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the Universal Declaration of Human Rights”.⁸⁴ Part of this mutual assistance takes place in the form of INTERPOL Notices, which are “international requests for cooperation or alerts allowing police in member countries to share critical crime-related information”.⁸⁵ Competent authorities within INTERPOL member countries are able to access these Notices, some of which may provide unique information useful to CIP. This may include information contained within an Orange Notice, used to “warn of an event, a person, an object or a process representing a serious and imminent threat to public safety”, or a Purple Notice, used to “seek or provide information on modus operandi, objects, devices and concealment methods used by criminals”.⁸⁶

84 Constitution of the ICPO-INTERPOL (2023). Available at: https://www.interpol.int/en/content/download/590/file/01%20E%20Constitution_2024.pdf [accessed 5 May 2025].

85 INTERPOL (no date), Notices. Available at: <https://www.interpol.int/en/How-we-work/Notices> [accessed 4 December 2024].

86 INTERPOL (no date), About Notices. Available at: <https://www.interpol.int/en/How-we-work/Notices/About-Notices> [accessed 4 December 2024].

INTERPOL's extensive network of police databases plays a crucial role in facilitating international co-operation and information sharing. INTERPOL manages 19 police databases containing a vast array of information on criminals and crimes,⁸⁷ including nominal data on individuals, details on terrorist organizations, and information on stolen and lost travel documents. These databases are accessible in real time to INTERPOL member countries,⁸⁸ enabling them to quickly and effectively share and retrieve critical information. This information can be used to inform risk assessments, develop targeted security measures, and enhance the overall physical security of CI, ultimately reducing the risk of a successful terrorist attack.

87 INTERPOL (no date), Databases. Available at: <https://www.interpol.int/How-we-work/Databases> [accessed 4 December 2024].

88 INTERPOL (no date), Databases. Available at: <https://www.interpol.int/How-we-work/Databases> [accessed 4 December 2024].



Human Rights Considerations

//

Terrorists represent a threat to the core functions of critical infrastructure. In facing this threat, States, critical infrastructure owners/operators, and private security providers must align with obligations under national as well as international law, including human rights law.

//

3 Human Rights Considerations

Terrorists represent a threat to the core functions of CI across the OSCE area. They are also “one of the most significant threats to peace, security and stability, as well as to the enjoyment of human rights and social and economic development, in the OSCE area and beyond.”⁸⁹ In facing this threat and designing the necessary CIP frameworks, States, CI owners/operators, and private security providers must align with obligations under national as well as international law, including human rights law. This is outlined in various international instruments, including the OSCE Commitments,⁹⁰ as well as numerous resolutions of the UN Human Rights Council,⁹¹ the UN General Assembly,⁹² and the UN Security Council.⁹³



89 OSCE (2007), Permanent Council Decision No. 1063: OSCE Consolidated Framework for the Fight against Terrorism (PC.DEC/1063), pp. 4–5. Available at: <https://www.osce.org/files/f/documents/7/5/98008.pdf> [accessed 5 May 2025].

90 See, e.g., OSCE (2007), Ministerial Council Decision No. 6/07: Public-Private Partnerships In Countering Terrorism (MC.DEC/5/07). Available at: <https://www.osce.org/files/f/documents/3/e/29569.pdf> [accessed 5 May 2025]. See also: OSCE (2015), Ministerial Declaration on Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism (MC.DOC/4/15), preambular paragraphs 5 and 7, para. 3, 2015. Available at: <https://www.osce.org/de/cio/212026> [accessed 5 May 2025].

91 See UN General Assembly (UNGA) Human Rights Council (2022), Resolution 51/24: Terrorism and human rights (A/HRC/51/24), preambular paragraphs 2, 5, 6, 7 and 8; paragraphs 2 and 4. Available at: <https://docs.un.org/en/A/HRC/RES/51/24> [accessed 5 May 2025].

92 See, e.g., UNGA (2018), Resolution 72/189: Protection of human rights and fundamental freedoms while countering terrorism (A/RES/72/180). Available at: <https://undocs.org/Home/Mobile?FinalSymbol=A%2F72%2F180&Language=E&DeviceType=Desktop&LangRequested=False> [accessed 5 May 2025]. See also UNGA (2006), Resolution 60/288: The United Nations Global Counter-Terrorism Strategy (A/RES/60/288). Available at: <https://documents.un.org/doc/undoc/gen/n05/504/88/pdf/n0550488.pdf> [accessed 5 May 2025].

93 See in particular, UNSC (2017), Resolution 2341 (S/RES/2341), preambular paragraph 5 on protecting critical infrastructure from terrorist attack. Available at: [https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2341\(2017\)&Language=E&DeviceType=Desktop&LangRequested=False](https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2341(2017)&Language=E&DeviceType=Desktop&LangRequested=False) [accessed 5 May 2025].

The Permanent Council of the OSCE “[r]eaffirm[ed] the participating States’ commitment to take the measures needed to protect everyone within their jurisdiction against terrorist acts and the need for all actions to be conducted in compliance with the rule of law and with all obligations under international law, including international human rights, refugee and humanitarian law”.⁹⁴ Thus navigating human rights obligations in the CIP context is an indispensable exercise to ensure effective State responses to terrorism based on the rule of law. Responses that are disproportionate to the terrorist threat or deprive people of their rights may push vulnerable individuals into the arms of terrorist recruiters.⁹⁵ To guard against such unintended consequences, human rights need to be considered both at the policymaker level, as well as by implementers such as CI owners/operators and private security providers.

Being a diverse body of law, human rights include procedural, investigative and fair trial guarantees to the right to privacy and to data protection and security. Each State has an obligation to respect, protect and fulfil human rights, including by regulating the conduct of non-State actors. The latter is of particular relevance in the context of CI, since State agencies will often be involved alongside private security providers in directing and implementing security and protective measures, or in providing responses to attacks on CI sites. A State may contract private entities for certain services (e.g., private security providers or data processing companies). And some CI sites may be wholly privately owned. The prevalence and prominence of private actors in this domain can thus complicate questions as to who is permitted to do what, or who carries responsibility, during a crisis situation such as a terrorist attack and its aftermath.

This chapter serves as an entry point for understanding the central importance of human rights obligations in the context of protecting CI from terrorist attacks, with some remarks on their relevance when considering physical security frameworks, public–private partnerships (PPPs) and other matters. The chapter explores three basic questions:

1. What are human rights and how do they apply to measures ensuring the physical security of CI?
2. What pressing human rights considerations should policymakers and CI owners/operators be aware of when constructing CIP frameworks?
3. How might human rights requirements apply differently to State and non-State personnel working at CI facilities?

This chapter is not a comprehensive or exhaustive account of the human rights considerations on this topic. Nonetheless, ongoing debates are noted and further references may be found in the footnotes. The primary lens of analysis in this section are the core UN human rights treaties,⁹⁶ since they form the common bedrock of legal

⁹⁴ OSCE (2007), Permanent Council Decision No. 1063: OSCE Consolidated Framework for the Fight against Terrorism (PC.DEC/1063), pp. 4–5. Available at: <https://www.osce.org/files/f/documents/7/5/98008.pdf> [accessed 5 May 2025].

⁹⁵ See UNDP (2023), *Journey to Extremism in Africa: Pathways to Recruitment and Disengagement*, pp. 17–18. Available at: <https://www.undp.org/sites/g/files/zskgke326/files/2023-02/UNDP-JourneyToExtremism-summary-2023-english.pdf> [accessed 5 May 2025]. It is reported here that nearly half of the individuals surveyed had experienced a specific trigger event that pushed them to join violent extremist groups, with 71 per cent describing that trigger as having been violence or injustice suffered at the hands of the government.

⁹⁶ See: United Nations (no date), *The Core International Human Rights Instruments and their monitoring bodies*. Available at: <https://www.ohchr.org/en/core-international-human-rights-instruments-and-their-monitoring-bodies> [accessed 4 December 2024].

obligation shared by all OSCE participating States. Where appropriate, jurisprudence, frameworks and guidance from other relevant mechanisms are also cited, including regional human rights mechanisms, international criminal tribunals and national courts. Finally, this chapter focuses on human rights law. As such, other bodies of law such as international humanitarian law are beyond its scope.⁹⁷

3.1 Human Rights and their Application

Human rights impose legal duties on States to protect individuals and guarantee certain standards of treatment and living. They are derived from several sources, most notably international/regional treaties that States have voluntarily signed and ratified, such as the International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights, or the Inter-American Convention on Human Rights. Human rights are also derived from customary law, which binds States regardless of their ratification of any treaty.⁹⁸ In both cases, States must ensure a domestic legal and policy framework that practically and effectively guarantees the enjoyment of human rights.

Commentators often describe States' human rights obligations as tripartite, comprised of a duty to protect, a duty to respect, and a duty to fulfil.⁹⁹ Put simply, this means each human right entails an obligation to:

- ▶ Respect: Refrain from taking actions that would interfere with or violate the enjoyment of human rights.
- ▶ Protect: Take all reasonable action to prevent human rights violations and abuses, including those caused by third parties (i.e., private enterprises).
- ▶ Fulfil: Take positive action such as "appropriate legislative, administrative, budgetary, judicial and other measures" to ensure the full enjoyment of human rights.¹⁰⁰

Human rights apply throughout the entire territory of a State, and whenever State agents exercise a certain level of control.¹⁰¹ For example, a State may be liable for a violation of the right to life or freedom from torture when the State's act is a "necessary link in a causal chain" that directly leads to a foreseeable risk of a violation

97 Irrespective of the applicable bodies of law, human rights scholars and UN experts counsel that terrorism "should primarily be seen as a serious form of crime and fought within a law enforcement paradigm," not within the framework of the law of armed conflict on the conduct of hostilities. Source: M. Scheinin (2022), "Terrorism", in *International Human Rights Law*, fourth edition, edited by Moeckli, D.; Shah, S.; Sivakumaran, S.; Harris, D. (Oxford: Oxford University Press), p. 608.

98 See, e.g., Schabas, W. (2021), *The Customary International Law of Human Rights* (Oxford: Oxford University Press).

99 See, e.g., UN Commission on Human Rights (1987), Report on the right to adequate food as a human right submitted by Mr. Asbjorn Eide, Special Rapporteur (E/CN.4/Sub.2/1987/23). Available at: <https://documents.un.org/doc/undoc/gen/g87/120/48/pdf/g8712048.pdf> [accessed 5 May 2025].

100 International Commission of Jurists (ICJ) (1997), Maastricht Guidelines on Violations of Economic, Social and Cultural Rights, para. 6. Available at: <https://www.refworld.org/policy/legalguidance/icjurists/1997/en/63964> [accessed 5 May 2025].

101 UN Human Rights Committee (2004), General comment no. 31 [80]: The nature of the general legal obligation imposed on States Parties to the Covenant (CCPR/C/21/Rev.1/Add.13), para. 10. Available at: <https://www.refworld.org/legal/general/hrc/2004/en/52451> [accessed 9 December 2024].

by a third party.¹⁰² States are also bound by international human rights law when implementing UN Security Council Resolutions.¹⁰³

Limitations and Derogations

Human rights protect everyone; this includes foreign nationals on the State's territory, as well as the State's own agents, such as armed forces, law enforcement or security personnel.¹⁰⁴ Though human rights law applies at all times, the body of law is flexible enough to account for diverse security exigencies States may face when protecting CI. The primary way this flexibility is realized is through lawful *limitation* of a non-absolute human right, which in certain circumstances reduces the application of a single right. Exceptionally, States may more broadly limit certain civil and political rights by means of a *derogation* during a state of emergency. Limitations and derogations are described in detail in the following two sections.

Limitations

Limitations are restrictions on human rights that are provided for by the right's relevant clause in an international treaty. For example, this might mean limiting the right to liberty and security when a law enforcement official effects a lawful arrest. Limitations, unlike derogations, do not require public declarations of a state of emergency. However, they do not provide *carte blanche* to restrict human rights. A lawful human rights limitation must be:

Proactively protected	Any limitation or interference with a human right must have a basis that is sufficiently clear, accessible and predictable in domestic law (known as the principle of legality).
Necessary/Justified	The State must establish that the limitation is necessary and justified in a democratic society to achieve a legitimate aim, such as the protection of national security, public order, public health or morals, or of the rights and freedoms of others (known as the principle of necessity).
Proportionate	The limitation must be proportionate to the legitimate aim. This means that it must be the "least intrusive measure" to achieve the legitimate aim (known as the principle of proportionality).
Non-discriminatory	Any limitation that has no objective of reasonable justification and is disproportionate is considered discriminatory. In a counter-terrorism context, particular attention must be given to ensure that measures are not adopted, and/or applied, that discriminate solely on grounds of race, religion, nationality or ethnicity.

¹⁰² See, e.g., UN Human Rights Committee (2009), *Mohammad Munaf v. Romania* (CCPR/C/96/D/1539/2006), para. 14.2. Available at: <https://www.refworld.org/jurisprudence/caselaw/hrc/2009/en/70157> [accessed 5 May 2025].

¹⁰³ *Kadi v. Council of the European Union and Commission of the European Communities*, C-402/05 P and C-415/05 P, European Union: Court of Justice of the European Union (CJEU), 3 September 2008. Available at: <https://www.refworld.org/jurisprudence/caselaw/ecj/2008/en/97735> [accessed 5 May 2025]; *Al-Jedda v. United Kingdom*, Application no. 27021/08, Council of Europe: European Court of Human Rights (ECHR), 7 July 2011. Available at: <https://hudoc.echr.coe.int/fre#%22itemid%22:%22001-105612%22> [accessed 18 May 2025]; *Nada v. Switzerland*, Judgement 12.9.2012 [GC], ECHR, August–September 2012. Available at: <https://hudoc.echr.coe.int/fre?i=002-6434> [accessed 5 May 2025].

¹⁰⁴ OSCE (1994), Code of Conduct on Politico-Military Aspects, para. 32, available at: [accessed 5 May 2025]; *Engel v. Netherlands*, ECHR, 8 June 1976, para. 54. Available at: <https://hudoc.echr.coe.int/eng?i=001-57479> [accessed 5 May 2025].

Limitations are an exceptional regime. Consequently, a limitation must not be applied in such a way as to make the enjoyment of a given right the exception rather than the rule. Further, some rights have no valid limitations listed in the treaty that establishes them, and as a result may only be restricted by means of a lawful derogation (see below). Other rights – for example the right not to be subjected to torture or other ill-treatment, the right to non-discrimination, and certain elements of the right to a fair trial, such as the presumption of innocence – are absolute rights and cannot be limited under any circumstances.

Derogations

In some limited circumstances, those working to protect CI may be able to act outside of strict human rights requirements. This is the result of a derogation, which is a public notice following a strict procedure of the temporary non-application of specific human rights protections.

A valid derogation may only be made during an exceptional situation created by an imminent public emergency that threatens the life of the nation.¹⁰⁵ This is a high bar. Involvement in an armed conflict, for example, is not per se a valid ground to derogate,¹⁰⁶ so a singular attack on CI may not necessarily provide grounds for a derogation. A derogation must be necessary and proportionate.

Furthermore, a derogation is a temporary measure. Rights may “only be suspended in order to [...] return to a situation of normalcy as soon as possible”.¹⁰⁷ For an entity to act in accordance with a valid derogation, it must be explicitly and publicly authorized to do so. Further, international human rights instruments explicitly state that some rights – such as the right to life, freedom from torture and other ill-treatment, the prohibition of slavery and the principle of no punishment without law – are non-derogable and therefore apply at all times, even during a public emergency.¹⁰⁸

Limitations and Derogations: Terrorist Attacks

When does a terrorist attack on CI provide grounds to limit or derogate from human rights law? Terrorism lacks a single, commonly accepted definition in international law; in any case, the “terrorist” character of an attack does not alter the human rights obligations of a State and its agents.¹⁰⁹ The criteria for assessing the lawfulness of a

¹⁰⁵ It is difficult to determine categorically what is, or is not, “a public emergency threatening the life of the nation”, since this requires a comprehensive and case-by-case assessment. However, international judicial mechanisms consider, *inter alia*, the following criteria: (1) The likelihood, imminence and severity of the harm; (2) Whether the emergency or its consequences affects the entire population; (3) Whether the proposed measures are strictly necessary to address the emergency. See, e.g., “The Greek Case” (Denmark, Norway, Sweden and the Netherlands v. Greece), ECHR, 1967. Available at: <https://hudoc.echr.coe.int/eng/?i=001-167795> [accessed 5 May 2025].

¹⁰⁶ Human Rights Committee (2001), General Comment No. 29: States of Emergency (Article 4) on derogations during a state of emergency (CCPR/C/21/Rev.1/Add.11) para. 3. Available at: <https://digitallibrary.un.org/record/451555?ln=en&v=pdf> [accessed 5 May 2025].

¹⁰⁷ OSCE Office for Democratic Institutions and Human Rights (ODIHR) (2007), *Countering Terrorism, Protecting Human Rights: A Manual*, p. 87. Available at: <https://www.osce.org/files/f/documents/d/6/29103.pdf> [accessed 5 May 2025].

¹⁰⁸ See UNGA (1966), International Covenant on Civil and Political Rights, Treaty Series, 999, 171, Art. 4; European Court of Human rights, Council of Europe (1950), Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended), European Treaty Series – No. 5, Art. 15; UN Human Rights Committee (2001), General Comment No. 29, Article 4 on derogations during a state of emergency (CCPR/C/21/Rev.1/Add.11).

¹⁰⁹ ODIHR (2007), *Countering Terrorism, Protecting Human Rights: A Manual*. Available at: <https://www.osce.org/files/f/documents/d/6/29103.pdf> [accessed 5 May 2025].

limitation or derogation remain the same, regardless of the nature of the threat. Any proposed restriction to international human rights law will therefore require a case-by-case assessment of the likelihood, imminence and severity of harm, as well as the legality, necessity and proportionality of the proposed response of the State.

However, an attack on CI may provide legitimate grounds for the limitation of some rights. For example, if there is an imminent threat to life, responders may be able to use lethal force in self-defence. Derogations, by contrast, require a higher burden of threat. For example, France made a derogation through the ICCPR and the European Court of Human Rights (ECHR) following the attack on the Bataclan Theatre in 2015.¹¹⁰ The initial derogation was for three months, and was instated to increase powers available to law enforcement, gendarmes and the military to combat a perceived immediate threat of further attacks. The United Kingdom made a derogation to the right to be free from arbitrary detention following the 11 September 2001 terror attacks in the United States, anticipating a similar attack in the United Kingdom. This derogation was considered invalid by British courts.¹¹¹ This was because the attack in the United States did not, absent specific intelligence regarding an impending attack on the United Kingdom, establish the necessity of such a drastic response.¹¹²

110 See Council of Europe (1950), Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005). Available at: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=005> [accessed 5 May 2025]; Decree No. 2015-1475 of 14 November 2015, to apply Act No. 55-385 of 3 April 1955 on the state of emergency in France. Available at: <https://treaties.un.org/doc/Publication/CN/2015/CN.703.2015-Eng.pdf> [accessed 5 May 2025].

111 See: A and others v. Secretary of State for the Home Department, United Kingdom House of Lords, 2005, UKHL 71, 2004. Available at: <https://publications.parliament.uk/pa/ld200506/ldjudgmt/jd051208/aand-1.htm> [accessed 11 May 2025]. See also: A. and Others v. United Kingdom, ECHR, 2009. Available at: <https://hudoc.echr.coe.int/eng?i=002-1647> [accessed 11 May 2025].

112 See: A and others v. Secretary of State for the Home Department, United Kingdom House of Lords, 2005. Available at: <https://publications.parliament.uk/pa/ld200506/ldjudgmt/jd051208/aand-1.htm> [accessed 11 May 2025]. See also: A. and Others v. United Kingdom, ECHR, 2009, paragraphs 19–34. Available at: <https://hudoc.echr.coe.int/eng?i=002-1647> [accessed 11 December 2024].

3.2 Involvement of Third Parties in Protecting Critical Infrastructure

The protection of CI is an area of public governance that is closely interlinked with the private sector.¹¹³ This is recognized in the OSCE's Ministerial Council Decision 5 of 2007 on public-private partnerships when countering terrorism:

The OSCE participating States "[a]cknowledg[e] the usefulness of joint counter-terrorist efforts by government bodies and the private sector (civil society and the business community) in the form of voluntary co-operation, based upon the principles of partnership and mutual trust, in order to provide better security and clear benefits to all parties. In this regard, efforts should particularly take due account of: [...] Identifying, prioritizing, and protecting critical infrastructure and addressing preparedness/consequence management issues."¹¹⁴



States may contract with private security providers to guard CI facilities, engage a business to conduct background checks for prospective facility personnel, maintain surveillance of a site, or store or process surveillance data. Some CI sites may be partially or wholly privately owned and staffed. The proliferation and prominence of non-State actors in this space raises questions of which responsibilities the State may delegate, and who is ultimately responsible in the event of a breach of human rights.

¹¹³ See, e.g., references made to public-private partnerships in the preambular paragraphs, as well as operative paragraph 5 of UNSC (2017), Resolution 2341 (S/RES/2341). Available at: [https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2341\(2017\)&Language=E&DeviceType=Desktop&LangRequested=False](https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2341(2017)&Language=E&DeviceType=Desktop&LangRequested=False) [accessed 5 May 2025]; OSCE (2007), Ministerial Council Decision No. 5/07: Public-Private Partnerships in Countering Terrorism (MC.DEC/5/07). Available at: <https://www.osce.org/files/f/documents/3/e/29569.pdf> [accessed 11 May 2025]; OSCE (2012), Permanent Council Decision No. 1063: OSCE Consolidated Framework for the Fight Against Terrorism (PC.DEC/1063), para. 6, 12, 17. Available at: <https://www.osce.org/pc/98008> [accessed 11 May 2025].

¹¹⁴ OSCE (2007), Ministerial Council Decision No. 5/07: Public-Private Partnerships in Countering Terrorism (MC.DEC/4/07). Available at: <https://www.osce.org/files/f/documents/3/e/29569.pdf> [accessed 11 May 2025].

State Responsibility

General international law elaborates the specific circumstances in which a State has responsibility for a breach of the law. For example, a State is always responsible for a breach by one of its agents, even those acting outside the scope of their lawful mandate.¹¹⁵ A State will likewise always have responsibility for an actor that is exercising elements of government authority (for example, a private security provider that has been delegated law enforcement powers in defence of CI).¹¹⁶

Human rights law creates additional parameters for State responsibility. International human rights law creates a presumption of State responsibility for all acts that occur within its territory or subject to its jurisdiction. Generally, the State is responsible for breaches by third parties unless it has taken reasonable steps to “prevent, investigate, punish and redress” such abuses.¹¹⁷ This means the State must take reasonable steps to stop and prevent human rights violations, for example by building a domestic law and policy framework that “establish[es] clear boundaries on any potential use of force”,¹¹⁸ and ensures that those working at CI sites are subject to background checks and that they receive human rights based training and appropriate equipment. These CIP frameworks should also be regularly assessed and strengthened with regard to their human rights compliance in an evidence-based, transparent and participatory manner to ensure that they do not contribute or lead to human rights violations, or to exclusion, prejudice or bias in a broader sense.

Secondly, the State must independently and impartially investigate alleged violations. Where a breach is established, the State must provide for an effective remedy.¹¹⁹ If the State fails to take measures to protect and ensure human rights standards, it becomes liable for the actions of third parties.

Delegation of State Powers

There is nothing under international law that explicitly prevents the State from delegating its powers to private entities, including those relating to the lawful use of force.¹²⁰

However, delegation of prerogatives is not equivalent to delegation of responsibility. The State remains liable for violations, abuses and/or misconduct of third parties if it

¹¹⁵ International Law Commission (November 2001), Draft articles on Responsibility of States for internationally wrongful acts, Supplement No. 10 (A/56/10), chp.IV.E.1, article 4. Available at: <https://www.refworld.org/legal/otherinstr/ilc/2001/en/20951> [accessed 11 May 2025].

¹¹⁶ International Law Commission (November 2001), Draft articles on Responsibility of States for internationally wrongful acts, Supplement No. 10 (A/56/10), chp.IV.E.1, article 6. Available at: <https://www.refworld.org/legal/otherinstr/ilc/2001/en/20951> [accessed 11 May 2025]. See also: UN Human Rights Committee (2019), General Comment No. 36, para. 15. Available at: <https://www.undocs.org/en/CCPR/C/GC/36> [accessed 11 May 2025].

¹¹⁷ See: UN (2011), *Guiding Principles on Business and Human Rights, Principle 1*. Available at: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf [accessed 11 May 2025].

¹¹⁸ See: Geneva Centre for Security Sector Governance (DCAF) (2019), *Regulating the Use of Force by Private Security Providers: A Guidance Tool for States: Basic Principles and Requirements for State Regulatory Frameworks on the Use of Force by Private Security Providers*, p. 5. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_Toolkit_Use%20of%20Force.pdf [accessed 11 May 2025].

¹¹⁹ See, e.g., UN Commission on Human Rights (2005), *Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law* (E/CN.4/2005/L.48). Available at: <https://digitallibrary.un.org/record/545961?v=pdf> [accessed 11 May 2025]; ECHR (2025), *Guide on Article 13 of the European Convention on Human Rights*. Available at: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_13_eng [accessed 11 May 2025].

¹²⁰ DCAF (2019), *Regulating the Use of Force by Private Security Providers: A Guidance Tool for States: Basic Principles and Requirements for State Regulatory Frameworks on the Use of Force by Private Security Providers*. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_Toolkit_Use%20of%20Force.pdf [accessed 11 May 2025].

has not taken the measures detailed above. Given the prevalence of private entities in the management and protection of CI, the State has a significant duty of due diligence to ensure the lawfulness of third party activities, especially when an entity is directly contracted for service provision by the State.

Some powers of the State demand human rights standards that are commonly ensured by the State. Examples may include general law enforcement mandates encompassing arrest and detention. They must protect against arbitrary arrest, such as by providing the right to challenge the detention in a court of law, ongoing legal review, and access to legal counsel.¹²¹ Despite no explicit prohibition, in practice States are prohibited from delegating such powers. Thus, a CI security force that is provided by a private security provider would generally not be able to exercise general powers of arrest.

Responsibility of Private Actors

The direct applicability of human rights law to non-State actors is under debate.¹²² Nevertheless, there is an increasing trend across much of the OSCE area towards building frameworks for corporate responsibility for human rights violations, abuses and/or misconduct.¹²³ In line with the Due Diligence Guidance for Responsible Business Conduct of the Organisation for Economic Co-operation and Development (OECD), such frameworks generally require that an enterprise:

- ▶ Integrate human rights due diligence into its policies and management systems;
- ▶ Identify and assess actual or potential adverse human rights impacts of its activities;
- ▶ Cease, prevent and mitigate adverse human rights impacts;
- ▶ Track the implementation and results of such steps;
- ▶ Communicate how impacts are addressed; and
- ▶ Provide remediation when appropriate.¹²⁴

As such, irrespective of whether private enterprises are directly bound by international human rights law, they are increasingly bound to follow human rights standards indirectly through regional and domestic law. Failure to meet these standards can result

¹²¹ DCAF (2019), *Regulating the Use of Force by Private Security Providers: A Guidance Tool for States: Basic Principles and Requirements for State Regulatory Frameworks on the Use of Force by Private Security Providers*, p. 6. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_Toolkit_Use%20of%20Force.pdf [accessed 11 May 2025]; UN (1990), *Basic Principles on the Role of Lawyers*. Available at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-role-lawyers> [accessed 11 May 2025]; UN Human Rights Committee (16 December 2014), General comment No. 35, Article 9 (Liberty and security of person), CCPR/C/GC/35. Available at: <https://www.refworld.org/legal/general/hrc/2014/en/104763> [accessed 11 May 2025].

¹²² The UN's *Guiding Principles on Business and Human Rights*, for example, chooses to emphasize the "responsibilities" of businesses rather than their "obligations". Available at: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf [accessed 11 May 2025]. Cf., however, A. Clapham (2022), "Non-State Actors", in *International Human Rights Law, fourth edition*, edited by Moeckli, D.; Shah, S.; Sivakumaran, S.; Harris, D. (Oxford: Oxford University Press) p. 583; and B.D. Lepard (2019), "Why customary international law matters in protecting human rights", Voelkerrechtsblog. Available at: <https://voelkerrechtsblog.org/de/why-customary-international-law-matters-in-protecting-human-rights/> [accessed 11 December 2024].

¹²³ See, e.g., UK Parliament (2023–24), *Commercial Organisations and Public Authorities Duty (Human Rights and Environment) Bill* [House of Lords]. Available at: <https://bills.parliament.uk/bills/3527/publications> [accessed 11 May 2025]; EU (2024), *Directive on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859 (Directive 2024/1760)*. Available at: <https://eur-lex.europa.eu/eli/dir/2024/1760/oj> [accessed 14 May 2025].

¹²⁴ See OECD (2018), *OECD Due Diligence Guidance for Responsible Business Conduct*. Available at: <https://mneguidelines.oecd.org/due-diligence-guidance-for-responsible-business-conduct.html>; see also the Corporate Sustainability Due Diligence Directive (CSDDD) – Directive (EU) 2024/1760. Available at: <https://www.corporate-sustainability-due-diligence-directive.com> [accessed 11 May 2025].

in punitive fines¹²⁵ or criminal prosecution,¹²⁶ and can also carry broader impacts related to public perception.¹²⁷

Private actors, and particularly private security providers, are also increasingly taking voluntary measures to align their practice with international law. Examples include the codification of human rights practice in industry-standard code of conduct documents,¹²⁸ and the benchmarks of the International Organization for Standardization (ISO).¹²⁹ In pursuing voluntary frameworks for the protection of human rights, private entities have engaged with civil society for monitoring their work and providing technical capacity and assistance to ensure compliance with best practice human rights standards.¹³⁰

3.3 The Use of Force and the Rights to Life, Security and Humane Treatment

A core part of ensuring the physical security of CI is establishing a security team capable of responding to threats. This security team may be armed and, if necessary, required to use force to defend themselves, other people, or a CI asset. As such, training in the human rights framework regulating the use of force and the right to life is vital for all members of a security team.

The use of force is regulated primarily by the right to life and the right to security. The right to life has a negative legal element (whereby State agents are required to refrain from arbitrarily depriving life), as well as and several positive legal elements, whereby the State is required to ensure a legal and policy framework conducive to respect for the right to life, to train and equip its agents properly, to investigate and remedy breaches,

125 See e.g., EU (2024), Directive on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859 (Directive 2024/1760), article 27. Available at: <https://eur-lex.europa.eu/eli/dir/2024/1760/oj> [accessed 14 May 2025]; see also Doe v. Chiquita Brands International, US District Court for New Jersey, 2024. Available at: <https://earthrights.org/case/doe-v-chiquita-brands-international-en/#:~:text=On%20June%2010%2C%202024%2C%20a,murdered%20were%20awarded%20rightful%20compensation> [accessed 11 May 2025].

126 See, e.g., the ongoing case of Lafarge (French Court of Cassation, n°22-83.681). Available at: <https://www.courdecassation.fr/en/decision/6411793925b075fb02f1b072> [accessed 11 May 2025]; Cossart, S.; Chatelain, L. (2021), "Human Rights Litigation against Multinational Companies in France", in *Human Rights Litigation against Multinationals in Practice*, edited by R. Meeran and J. Meeran, (Oxford; online edn Oxford Academic, 18 Nov. 2021).

127 See, e.g., various research that has linked publicized human rights abuses with negative stock performance: Kreitmeir, D.; Lane, N.; Raschky, P. (2020), *The Value of Names: Civil Society, Information, and Governing Multinationals on the Global Periphery*; S. Stäbler (2020), "Corporate social irresponsibility and stock market reactions: the critical role of news media", Principles for Responsible Investment. Available at: <https://www.unpri.org/pri-blog/corporate-social-irresponsibility-and-stock-market-reactions-the-critical-role-of-news-media/6008.article> [accessed 11 December 2024]; Kappel, V.; Schmidt, P.; Ziegler, A. (2009), "Human Rights Abuse and Corporate Stock Performance - An Event Study Analysis", *SSRN Electronic Journal*. Available at: https://www.researchgate.net/publication/256000444_Human_Rights_Abuse_and_Corporate_Stock_Performance_-_An_Event_Study_Analysis [accessed 11 May 2025].

128 See, e.g., International Code of Conduct Association (ICoCA), The International Code of Conduct for Private Security Service Providers [webpage]. Available at: <https://icoca.ch/the-code/> [accessed 11 May 2025]; Voluntary Principles on Security and Human Rights [website]. Available at: <https://www.voluntaryprinciples.org> [accessed 11 December 2024].

129 See, e.g., International Organization for Standardization, ISO 18788:2015 Management system for private security operations – Requirements with guidance for use. Available at: <https://www.iso.org/obp/ui/en/#iso:std:iso:18788:ed-1:v1:en> [accessed 11 December 2024].

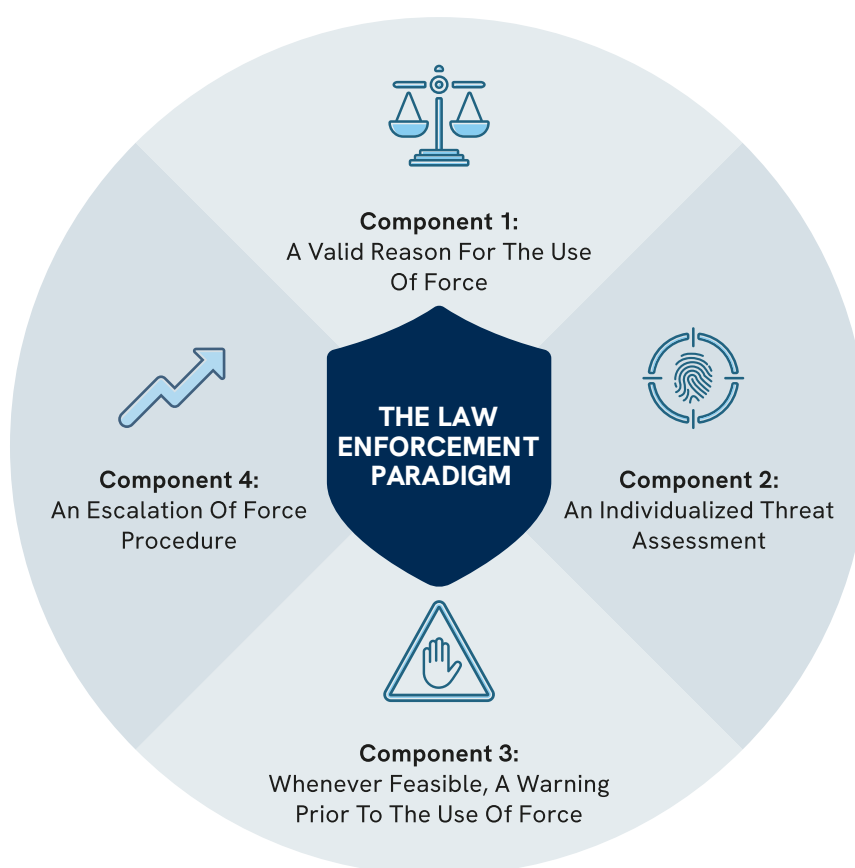
130 ICoCA, Capacity Building [webpage]. Available at: <https://icoca.ch/what-we-do/capacity-building/> [accessed 11 December 2024]; DCAF, Managing Security and Protecting Rights [webpage]. Available at: <https://www.dcaf.ch/index.php/managing-security-and-protecting-rights> [accessed 11 December 2024].

and to hold violators to account.¹³¹ The right to life requires that force only be used in the most exceptional circumstances when it is strictly unavoidable to protect life; such force is subject to stringent safeguards. The right to life is non-derogable, which means it cannot be suspended temporarily in times of crisis.

When a security team is responding to a security threat, its use of force must always be governed by three overriding principles: necessity, proportionality and precautions.¹³² The content of these principles, outside of situations of armed conflict, is provided by the law enforcement paradigm.

The Law Enforcement Paradigm

The law enforcement paradigm (LEP) protects everyone's right to life. This includes the target of a use of force. In practice, this means that responders must generally follow a strict framework that attempts, wherever possible, to avoid the use of force. Consequently, the LEP requires four key components at the tactical level:



¹³¹ In legal terms, a negative obligation is one that requires an actor to refrain from a certain behaviour, while a positive obligation is one that requires an actor to do a specific act.

¹³² Geneva Academy of International Humanitarian Law and Human Rights (2016), *Use of Force in Law Enforcement and the Right to Life: The Role of the Human Rights Council*, p. 6. Available at: https://www.geneva-academy.ch/joomlatools-files/docman-files/in-brief6_WEB.pdf [accessed 11 May 2025].



Component 1: A valid reason for the use of force

Security personnel may have to use force for a variety of reasons, such as in self-defence or as State agents effecting a lawful arrest. Lower levels of force such as physical restraint may be authorized when they are absolutely necessary in order to achieve a legitimate law enforcement objective. This may include, for example, detaining an intruder until law enforcement arrive at the scene.¹³³

The use of more significant levels of force including firearms is more tightly regulated under human rights law. The UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (“UN Basic Principles”) provide for three situations in which firearms may be used to stop or apprehend an individual. These three situations are:

- ▶ Self-defence or the defence of others against the imminent threat of death or serious injury. Imminence in this context refers to a threat that will manifest in “seconds, not hours”;¹³⁴
- ▶ Prevention of the perpetration of a particularly serious crime involving a grave threat to life;
- ▶ In the arrest of a person presenting such a danger and resisting authority, or to prevent their escape.¹³⁵

Note that all three situations require a clear threat of grave injury or death to an identifiable person.¹³⁶ This means in effect that firearms may never be used solely to defend property.

Moreover, the above situations apply only to circumstances in which the intent is to “stop”, not “kill” the target. The use of intentional lethal force is further restricted. For example, an escapee, even one perceived to be violent and dangerous, who does not pose an immediate and specific threat to life may not be killed. In the view of the European Court of Human Rights and UN Experts, this is the case “even if a failure to use lethal force may result in the opportunity to arrest the fugitive being lost”.¹³⁷

133 UN (1990), Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, principle 4. Available at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-use-force-and-firearms-law-enforcement#:~:text=4,use%20of%20force%20and%20firearms> [accessed 11 May 2025]; UN, Code of Conduct for Law Enforcement Officials (UNGA Res 34/169) with Commentary (1979), art. 3. Available at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/code-conduct-law-enforcement-officials> [accessed 11 May 2025].

134 C. Heyns, UN Human Rights Council, Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions (A/HRC/26/36), para. 50. Available at: <https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F26%2F36&Language=E&DeviceType=Desktop&LangRequested=False> [accessed 12 May 2025].

135 See: *M.D v. Turkey*, ECHR, 1997. Available at: <https://hudoc.echr.coe.int/eng?i=001-113441> [accessed 11 May 2025]. Here the shooting of a suspected bomber was considered lawful, since the officers were not “shooting to kill” but rather to immobilize.

136 See: UN (1990), Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, principle 9. Available at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-use-force-and-firearms-law-enforcement> [accessed 11 December 2024]. See also: UN, Code of Conduct for Law Enforcement Officials (UNGA Res 34/169) with Commentary (1979). Available at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/code-conduct-law-enforcement-officials> [accessed 11 December 2024].

137 *Nachova and others v. Bulgaria*, ECHR, 2005, para. 95. Available at: <https://hudoc.echr.coe.int/tur?i=001-69630> [accessed 12 May 2025]. See also: UN (2006), Report on Civil and Political Rights, Including the Question of Disappearances and Summary Executions, E/CN.4/2006/53/Add.4, para. 47. Available at: <https://documents.un.org/doc/undoc/gen/g06/106/40/pdf/g0610640.pdf> [accessed 12 May 2025].

Together, these principles mean that a CI facility's guarding force would be allowed to use firearms to respond lethally to an active shooter who is attacking facility personnel, but not to prevent the escape of someone who has infiltrated a facility and who is destroying objects or escaping without posing an immediate threat to people. If a suspect is peacefully retreating, security personnel may only use appropriate non-lethal force to prevent their escape. Lethal force may only be used when strictly unavoidable in order to protect another life.¹³⁸

A situation that initially gave rise to lawful grounds for the use of force may change over time. If the grounds that gave rise to the imminent threat to life no longer exist, the use of force, and especially lethal force, may become unlawful. Examples may include attackers surrendering or becoming incapacitated.



Component 2: An individualized threat assessment

Human rights law requires that an individual be afforded an individual assessment of the imminent threat they pose.¹³⁹ This means that an individual may not be targeted simply because they are part of an armed group engaged in an attack on CI. If, for example, intelligence suggests that only two out of four individuals involved in an attack are armed, security personnel may not shoot at all four based solely on their involvement in the same group, or due to a “balance of probabilities” that they each pose a threat. An individual must pose a direct and imminent threat for the use of force to be authorized against them. In mixed crowds, force must be limited precisely to those who pose such a threat.



Component 3: Whenever feasible, a warning prior to the use of force

The use of force by security personnel should be preceded, whenever feasible, by a warning and the opportunity to surrender. A warning is unfeasible if it would put the security agent at undue risk, would create a risk of death or serious harm to other people, or would be manifestly pointless (for example, if the target is already firing his/her weapon).¹⁴⁰

138 UN (1990), Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, principle 9. Available at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-use-force-and-firearms-law-enforcement> [accessed 11 December 2024]; principle 9 read in conjunction with principles 4, 5 and 10. See also: C. Heyns, UN Human Rights Council, Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions (A/HRC/26/36), para. 46–47. Available at: <https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F26%2F36&Language=E&DeviceType=Desktop&LangRequested=False> [accessed 12 May 2025].

139 OHCHR (1997), *Human Rights and Law Enforcement: A Manual on Human Rights Training for Law Enforcement Officials*, Chapter 9. Available at: <https://www.ohchr.org/sites/default/files/Documents/Publications/training5en.pdf> [accessed 12 May 2025].

140 UN Office on Drugs and Crime (UNODC) (2017), *Resource Book on the Use of Force and Firearms in Law Enforcement*, p. 98. Available at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/resource-book-use-force-and-firearms-law> [accessed 12 May 2025].

A warning should be verbal, make clear the identity of the security agent, give clear instructions and indicate what will occur in the event of non-compliance.¹⁴¹ For a warning to be effective, there must be sufficient time given for the target to comply with the security agent's demands. Warning shots are not an effective warning, as they do not meet these criteria and may be misinterpreted as an attack. In any case, warning shots should be prohibited in most circumstances due to the risk of causing incidental damage and injury.¹⁴² The requirement to give a warning whenever feasible is well-established and applies even to targets who are considered armed and dangerous.



Component 4: An escalation of force procedure

Under the LEP, security personnel may only use as much force as is strictly necessary and proportionate to end the threat to life. Non-lethal force must be the primary mode of response. This does not preclude scenarios where lethal force may be used immediately, as for example in lawful self-defence against an imminent or ongoing attack. However, this does mean that non-lethal and less-lethal responses should be attempted first whenever possible. The use of firearms is an extreme measure, and the intentional use of lethal force should always be a last resort. Even in high-risk operations, an escalation of force procedure may include an initial, controlled deployment of disorientation devices such as flash-bang grenades, riot control agents,¹⁴³ malodorants or sonic weapons.¹⁴⁴

The Right to Life: Positive Legal Elements

The positive elements of the right to life fall into two categories: those that require the State to take action prior to the use of force, and those that require action after a use of force.

Policy and Planning: The State must create a legal and policy framework that reflects its obligations under international human rights law. This includes, for example, establishing frameworks regulating security personnel that reflect the LEP, and establishing adequate oversight, investigation and remedy procedures.

Operational planning must also respect the right to life. This means that those involved in planning a response to a terrorist attack must consider at all times whether the use of force is strictly necessary, and if so, what type of force.

141 UN (1990), Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, principle 10. Available at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-use-force-and-firearms-law-enforcement#:~:text=4,use%20of%20force%20and%20firearms> [accessed 11 December 2024].

142 UNODC (2017), *Resource Book on the Use of Force and Firearms in Law Enforcement*, p. 98. Available at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/resource-book-use-force-and-firearms-law> [accessed 12 May 2025]. See also: Amnesty International (2015), *Use of Force: Guidelines for Implementation of the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials*. Available at: https://www.amnesty.org.uk/files/use_of_force.pdf [accessed 12 May 2025].

143 As referred to in the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons (Chemical Weapons Convention). Available at: <https://www.opcw.org/chemical-weapons-convention> [accessed 12 May 2025].

144 OHCHR (2020). *United Nations Human Rights: Guidance on Less-Lethal Weapons in Law Enforcement*. Available at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/united-nations-human-rights-guidance-less> [accessed 12 May 2025]; cf. also ODIHR (2021). *Guide on Law Enforcement Equipment Most Commonly Used in the Policing of Assemblies*. Available at: <https://www.osce.org/odihr/491551> [accessed 12 May 2025].

The right to life also applies to security personnel themselves. The State may be liable for a breach of the right to life or the right to personal security if it is grossly negligent in the planning, training or equipping of security personnel to face a particular threat, with that negligence resulting in the death or injury of a State's agent.¹⁴⁵

Training and Equipment: The training of security personnel should draw upon relevant international standards, especially the UN Code of Conduct for Law Enforcement Officials, and the UN Basic Principles on the Use of Force and Firearms by Law Enforcement officials.¹⁴⁶ Moreover, security personnel should be trained in de-escalation techniques and methods of interdiction that may reduce the need to resort to force.

Security personnel, including CI facility personnel, must also be appropriately equipped. Providing security personnel with protective equipment such as helmets, shields and body armour may reduce threats posed by attackers, or may even deter an attack, thus limiting the need for a recourse to force.¹⁴⁷ Certain "offensive" equipment, such as firearms, by contrast, may be more likely to lead to a right's violation. Security personnel should therefore have access to "less lethal" alternatives to firearms, such as foam bullets, paintballs, tasers, truncheons or incapacitating aerosols.¹⁴⁸ In any case, where there are mixed crowds of valid targets and other persons, security personnel must use methods and means that are most likely to guarantee the safety of those persons who are not valid targets.

Nonetheless, less-lethal weapons may still cause significant injury or even death, both to their targets and those around them. Therefore, access to such weapons should be restricted to those who have regularly undergone specific training. Operationally, less lethal weapons should only be deployed in situations where other less harmful measures appear ineffective to address a clear threat.¹⁴⁹

¹⁴⁵ See, e.g., *Smith and others v. United Kingdom*, Supreme Court of the United Kingdom, 2013. Available at: <https://www.supremecourt.uk/cases/uksc-2012-0249> [accessed 12 May 2025]. This case is related to friendly fire during a military operation in Iraq. Since the court found liability in a more complex extra-territorial situation, an *a fortiori* argument is made that the case will apply to domestic situations as well.

¹⁴⁶ UN Human Rights Committee (2018), General comment No. 36, para. 13. Available at: <https://docs.un.org/en/CCPR/C/GC/36> [accessed 12 May 2025].

¹⁴⁷ UNDOC (2018), The promotion and protection of human rights in the context of peaceful protests (A/HRC/RES/38/11), para. 15. Available at: <https://documents.un.org/doc/undoc/gen/g18/213/58/pdf/g1821358.pdf> [accessed 12 May 2025].

¹⁴⁸ OHCHR (2020), *United Nations Human Rights: Guidance on Less-Lethal Weapons in Law Enforcement*, p. iii. Available at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/united-nations-human-rights-guidance-less> [accessed 12 May 2025].

¹⁴⁹ UN Human Rights Committee (2018), General comment No. 36 (CCPR/C/GC/36) para. 14. Available at: <https://docs.un.org/en/CCPR/C/GC/36> [accessed 12 May 2025].

3.4 The Rights to Privacy, Data Security and Protection



Technology-aided data collection is a key component of ensuring the physical security of CI. Common data collection practices include property surveillance networks such as video surveillance systems, collection of biometric data for authentication, security vetting of personnel, and insider threat mitigation practices (for more information, see Chapter 8, Insider Threat Management). These measures are likely to impact the privacy of either the general public, facility personnel, or both.

Since 2013, there has been significant normative development of the right to privacy under international law.¹⁵⁰ Today, the right to privacy encompasses not just private and family life, home, and correspondence, but broader robust personal data privacy and protection measures.¹⁵¹ Anything under the right to privacy's scope, including personal data, is protected from "arbitrary or unlawful interference" from "State authorities or from natural, or legal persons".¹⁵²

The UN and OSCE have identified expanded communications monitoring, general purpose surveillance systems and targeted digital surveillance as some of the largest threats to the right to privacy today.¹⁵³ However a State's interference with the right

¹⁵⁰ Nyst, C.; Falchetta, T. (2017), "The Right to Privacy in the Digital Age". *Journal of Human Rights Practice* 9(1), pp. 104–118. Available at: https://www.researchgate.net/publication/317774145_The_Right_to_Privacy_in_the_Digital_Age [accessed 12 May 2025].

¹⁵¹ See the successive resolutions of the UN General Assembly and Human Rights Council: UN General Assembly (2018), The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights, (A/HRC/39/29). Available at: <https://digitallibrary.un.org/record/1640588?v=pdf&ln=en> [accessed 12 May 2025]; UN General Assembly (14 December 1990) (45/95), Guidelines for the regulation of computerized personal data files. Available at: <https://digitallibrary.un.org/record/105299?v=pdf> [accessed 12 May 2025]; UN General Assembly (2022), Right to Privacy (A/77/196). Available at: <https://documents.un.org/doc/undoc/gen/n22/594/48/pdf/n2259448.pdf> [accessed 12 May 2025]. In the author's view, the latter may be a study of sufficient breadth to gauge State practice and opinio juris regarding a customary right to privacy.

¹⁵² UN Human Rights Committee (1988), General comment No. 36: Article 17 (Right to Privacy), para. 1. Available at: <https://www.refworld.org/legal/general/hrc/1988/en/27539> [accessed 12 May 2025].

¹⁵³ See: UNGA (2018), The right to privacy in the digital age: Report of the United Nations High Commissioner for

to privacy may be permissible if it is for a clearly identifiable purpose such as national security, and if it is necessary and proportionate, i.e., if it is carried out in accordance with data protection principles, such as data minimization (limiting data collection to that strictly necessary for the original purpose) and retention (deleting data after it is no longer needed).¹⁵⁴ For example, data collection about an individual in order to ascertain whether he/she may hold security clearance, or may access a facility, is generally a valid limitation of the right to privacy, assuming the data is limited in scope by the principles of necessity and proportionality.¹⁵⁵

Likewise, the European Court of Human Rights notes that a security guard monitoring a video surveillance system covering a public scene constitutes generally a lawful interference with privacy.¹⁵⁶ The Venice Commission concluded that surveillance at the workplace nevertheless requires respect for the rights of employees' privacy. This means avoiding the use of cameras in toilets, personnel lounges or other areas where a person expects to be unmonitored, and that any secret surveillance of personnel, for example for insider threat mitigation, must be necessary, proportionate and deployed on a temporary basis.¹⁵⁷ More invasive or wide-ranging methods of data collection require a greater justification for their use, and greater protections against misuse.

Human Rights (A/HRC/39/29). Available at: <https://digitallibrary.un.org/record/1640588?v=pdf&ln=en> [accessed 12 May 2025]. See also: OSCE ODIHR (2021), *Border Management and Human Rights: Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context*. Available at: <https://www.osce.org/files/f/documents/f/a/499777.pdf> [accessed 12 May 2025].

154 For the full “ten principles” identified by the UN Special Rapporteur on privacy, see UN General Assembly (2024), Report of the Special Rapporteur on the right to privacy, Ana Brian Nougères, A/79/173. Available at: <https://docs.un.org/A/79/173> [accessed 12 May 2025].

155 UK Parliament (2024), *National Security Vetting: Your Questions Answered*. Available at: <https://www.parliament.uk/globalassets/mps-lords--offices/offices/pass-office/psd-national-security-vetting-booklet.pdf> [accessed 30 October 2024]. See also: Michael Schwars v. Stadt Bochum, CJEU, 2013, C-191/12, paragraphs 63–64 for an EU perspective on the deletion of biometric data otherwise validly collected and processed in airports.

156 P.G and J.H v. The United Kingdom, ECHR, 2001, para. 57.

157 European Commission for Democracy through Law (Venice Commission) (2007), Opinion on Video Surveillance by Private Operators in the Public and Private Spheres and by Public Authorities in the Private Sphere and Human Rights Protection, para. 53–54. Available at: [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2007\)027-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2007)027-e) [accessed 12 May 2025].



The use of UAS (drones) allows for loitering reconnaissance capabilities that may target an individual, or viewing of a wide area where individuals may have no reasonable perception of being surveyed. UN human rights experts have noted that UAS generally require a high level of legal regulation to avoid misuse, more so than traditional surveillance technology, such as ground-based video surveillance systems.¹⁵⁸

Similarly, the collection and processing of biometric data,¹⁵⁹ such as data from facial recognition technology, likely requires a far stronger justification and legal protections to be permitted. This new technology is also triggering a fast evolving area of law.¹⁶⁰

Both State actors and private entities must be particularly careful when collecting, processing and storing data to ensure they are not arbitrarily or unlawfully interfering with the right to privacy. While there may be a presumption that State agents performing legitimate security duties in accordance with the law are not unduly interfering with the right to privacy, it is not clear that the same presumptions and calculations of necessity and proportionality apply to private actors. Examples for privacy rights-compliant data collection by non-State actors are based primarily on receiving the “free, specific and informed consent” of the data subject, or compliance with national law.¹⁶¹

¹⁵⁸ See, e.g., Ní Aoláin, F. (2022), Remarks of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedom while countering terrorism at the International Expert Meeting on the Protection of Vulnerable Targets and Unmanned Aircraft Systems. Available at: <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/2022-10-18/SR-CT%2520-HR-Drones-Remarks-6-Oct-2021.docx> [accessed 12 May 2025].

¹⁵⁹ For additional information, see: OSCE ODIHR (2021), *Border Management and Human Rights: Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context*. Available at: <https://www.osce.org/files/f/documents/f/a/499777.pdf> [accessed 12 May 2025].

¹⁶⁰ Murray, D. (2023), “Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework”, *Modern Law Review* 87(4), pp. 833–863. Available at: <https://doi.org/10.1111/1468-2230.12862> [accessed 12 May 2025].

¹⁶¹ See, e.g., EU, General Data Protection Regulation (GDPR) 2016, Article 6(1), OJ L 119. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679> [accessed 12 May 2025]. See also: GDPR Recital 47: Overriding legitimate interests (available at: <https://gdpr-info.eu/recitals/no-47/> [accessed 12 May 2025]), and its clarification in *Meta Platforms Inc. and Others v. Bundeskartellamt*, Case C-252/21, CJEU, 2023; and Venice Commission (2007), *Opinion on Video Surveillance by Private Operators in the Public and Private Spheres and by Public Authorities in the Private Sphere and Human Rights Protection*, para. 50. Available at: [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2007\)027-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2007)027-e) [accessed 12 May 2025].

Some States may consider data storage facilities to fall within their definition of CI.¹⁶² While this *Technical Guide* does not detail good practices in cybersecurity, cyber and physical security are closely interlinked. For example, while robust data protection practices such as data encryption and access control may reduce the likelihood of unauthorized access to data, these will be undermined if personnel are not sufficiently trained in cybersecurity, or if the data is physically stored in a place where threat actors can access it.

Considerations of physical access to data are particularly important when data analysis or storage is contracted out to private enterprises or other third parties. States must ensure that a contractor's facilities and training meet minimum standards regarding data protection, physical security and cybersecurity. Additionally, private entities may transfer, store, backup or cache data across networks that may include nodes in foreign jurisdictions. States should seek to maintain data sovereignty over personal or high-risk data. Where this is not possible, States should ensure that the other jurisdiction involved adheres to robust data protection regulations. This helps ensure compliance with and direct application of human rights obligations, including those related to unauthorized access, to mitigate complications regarding third State data protection or data sharing laws.

The sharing of data between States and private entities regarding groups and individuals considered to pose a threat to CI is increasingly being considered as part of the prevention and preparedness plans for the protection of CI.¹⁶³ However, "data-sharing is a black box of international law practice, with little information available on [...] what type of data is exchanged, the content of data-sharing agreements" and whether they integrate human rights standards.¹⁶⁴ States and private entities must ensure that data is only shared when necessary and proportionate, and in a manner that respects human rights obligations, including the right to privacy.¹⁶⁵

Given that such systems of sharing necessarily operate without the consent of the data subject, the sharing of biometric data such as facial or fingerprint data will require higher burdens in proving necessity, such as the presence of an immediate and identifiable threat, as well as safeguards against abuse.¹⁶⁶

162 See, e.g., Australian Government Department of Home Affairs, Cyber and Infrastructure Security Centre (CISC) (5 Dec. 2023), SOCI Act 2018 for data storage and processing. Available at: <https://www.cisc.gov.au/information-for-your-industry/data-storage-and-processing/legislation-regulation-and-compliance/soci-act-2018> [accessed 12 May 2025].

163 See UNSC, Counter-Terrorism Committee Executive Directorate (2017), *CTED Trends Report: Physical Protection of Critical Infrastructure Against Terrorist Attacks*. pp. 11–12. Available at: <https://www.un.org/securitycouncil/ctc/sites/www.un.org/securitycouncil.ctc/files/cted-trends-report-march-2017-final.pdf> [accessed 12 May 2025].

164 UNGA (2023), Human rights implications of the development, use and transfer of new technologies in the context of counterterrorism and countering and preventing violent extremism (A/HRC/52/39), para. 26. Available at: <https://documents.un.org/doc/undoc/gen/g23/020/43/pdf/g2302043.pdf> [accessed 12 May 2025].

165 For further guidance, see Huszti-Orbán, K.; Ní Aoláin, F. (2020), *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?* Human Rights Center, University of Minnesota (2020). Available at: <https://law.umn.edu/sites/law.umn.edu/files/2020/07/21/hrc-biometrics-report-july2020.pdf> [accessed 12 May 2025]. See also: UNGA (2023), Human rights implications of the development, use and transfer of new technologies in the context of counterterrorism and countering and preventing violent extremism (A/HRC/52/39). Available at: <https://docs.un.org/A/HRC/52/39> [accessed 12 May 2025].

166 For further guidance, see OSCE ODIHR (2021), *Policy Brief: Border Management and Human Rights*, pp. 16–20. Available at: <https://www.osce.org/files/f/documents/f/a/499777.pdf> [accessed 12 May 2025]. See also: UNSC Counter-Terrorism Committee Executive Directorate and UNOCT (2018), *United Nations Compendium of Recommended Practices for the Responsible Use & Sharing of Biometrics in Counter-Terrorism*, particularly pp. 37–38. Available at: https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf [accessed 12 May 2025].



Public–Private Partnerships



//

While ownership structures for critical infrastructure sites vary, a key reality is that many private infrastructure owners/operators are responsible for protecting their assets. Therefore engagement between the public and private sectors is increasingly seen as a good, if not essential, practice.

//

4 Public–Private Partnerships

Across the OSCE area, the private business community has a central role in owning, operating and protecting CI. It thus plays a key role in preparing for and responding to terrorist attacks on CI sites. While ownership structures of CI sites vary among the OSCE participating States, a key reality is that many private CI owners/operators are responsible for protecting their CI assets/systems. This is the case even if the service they provide (such as electricity, drinking water, or transportation) is intended for public consumption. In many cases, protective duties are outsourced to a private security provider. As a result, in the event of a terrorist incident at a CI site, private stakeholders, including private security companies, play a vital role. Therefore engagement between the public and private sectors is increasingly seen as a good, if not essential, practice.

Public–private partnerships (PPPs) are formal or informal co-operation arrangements between public authorities and private companies. PPPs aim to share work and promote collaboration between private partners and public authorities, whereby the private partner takes on the responsibility for providing an efficient service, and the public authority ensures that the goals being pursued are in the public interest. Public authorities anticipate that a partnership with the private economy will relieve pressure on public budgets because the private company must provide some or all of the funds itself, which means it will strive to ensure that the projects are cost-effective.¹⁶⁷

This chapter presents the international framework for PPPs within a CIP context, and explores how shared baseline values can support strong PPPs. The chapter ends with a focus on information-sharing arrangements within PPPs, a factor that is central to countering terrorist threats to CI.

4.1 OSCE and United Nations Frameworks for Public–Private Partnerships to Protect Critical Infrastructure

The OSCE has a near two-decade history of acknowledging and encouraging public–private partnerships, specifically in efforts to protect CI from terrorist attacks. In 2007, through Ministerial Council decision 5, the OSCE participating States affirmed the:

“usefulness of joint counter-terrorist efforts by government bodies and the private sector (civil society and the business community) in the form of voluntary co-operation, based upon the principles of partnership and mutual trust, in order to provide better security and clear benefits to all parties.”¹⁶⁸

¹⁶⁷ OSCE (2013), *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*. Available at: <https://www.osce.org/files/f/documents/4/b/103500.pdf> [accessed 12 May 2025].

¹⁶⁸ OSCE (2007), Ministerial Council Decision No. 5/07: Public-Private Partnerships in Countering Terrorism (MC. DEC/5/07). Available at: <https://www.osce.org/files/f/documents/3/e/29569.pdf> [accessed 12 May 2025].

In this regard, they called for efforts which take due account of, “identifying, prioritizing, and protecting critical infrastructure and addressing preparedness/consequence management issues”.¹⁶⁹

This position has been since reinforced in the OSCE Ministerial Council Decision 6 of 2007 on critical energy infrastructure protection from terrorist attacks,¹⁷⁰ and the OSCE’s 2012 Consolidated Framework for the Fight against Terrorism.¹⁷¹

The United Nations General Assembly and its Security Council have affirmed similar views regarding public–private partnerships within the framework of protecting CI from terrorist attacks. In the eighth review of the Global Counter-Terrorism Strategy,¹⁷² the United Nations General Assembly:

“Encourages the Office of Counter-Terrorism and the Global Counter-Terrorism Coordination Compact entities to work closely with Member States and relevant international, regional and subregional organizations to identify and share best practices to prevent terrorist attacks on particularly vulnerable targets, including critical infrastructure and public places (‘soft’ targets), and recognizes the importance of developing public–private partnerships in this area.”

Through United Nations Security Council 2341 (2017), the Security Council:

“Recogniz[es] that preparedness for terrorist attacks includes prevention, protection, mitigation, response and recovery with an emphasis on promoting security and resilience of critical infrastructure, including through public-private partnership as appropriate.”

“Further calls upon States to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks”.¹⁷³

Additionally, the 2018 Addendum to the Madrid Guiding Principles provides valuable guidance on PPPs from the UN Security Council. The 2015 UN Security Council Madrid Guiding Principles on Foreign Terrorist Fighters¹⁷⁴ were designed as “a practical tool

169 OSCE (2007), Ministerial Council Decision No. 5/07: Public-Private Partnerships in Countering Terrorism (MC.DEC/5/07). Available at: <https://www.osce.org/files/f/documents/3/e/29569.pdf> [accessed 12 May 2025].

170 OSCE (2007), Ministerial Council Decision No. 6/07: Protecting Critical Energy Infrastructure from Terrorist Attack (MC.DEC/6/07). Here the Ministerial Council “[e]ncourages participating States to further promote public-private partnership with business communities with a view to increasing critical energy infrastructure protection against terrorist attack and to effectively address preparedness/consequence management issues in this field”. Available at: <https://www.osce.org/files/f/documents/4/5/29482.pdf> [accessed 12 May 2025].

171 OSCE (2007), Permanent Council Decision No. 1063: OSCE Consolidated Framework for the Fight against Terrorism (PC.DEC/1063), II, para. 6. Available at: <https://www.osce.org/files/f/documents/7/5/98008.pdf> [accessed 12 May 2025].

172 UNGA (2023), The United Nations Global Counter-Terrorism Strategy: eighth review (A/RES/77/298). Available at: <https://documents.un.org/doc/undoc/gen/n23/189/01/pdf/n2318901.pdf> [accessed 12 May 2025].

173 UNSC (2017), Resolution 2341 (S/RES/2341). Available at: <https://documents.un.org/doc/undoc/gen/n17/038/57/pdf/n1703857.pdf> [accessed 5 May 2025].

174 UNSC (2015), Letter dated 15 December 2015 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/2015/939).

for use by [UN] Member States in their efforts to combat terrorism and, in particular, to stem the flow of foreign terrorist fighters in accordance with resolution 2178 (2014).” In 2018, an Addendum to these Guiding Principles was released, which includes additional Guiding Principles. Two of these provide specific guidance on PPPs in a counter-terrorism context.¹⁷⁵

Guiding Principle	Official Text
Guiding Principle 50	“In their efforts to develop and implement measures to protect critical infrastructure and soft targets from terrorist attacks, Member States, acting in cooperation with local authorities, should: [...] Develop, implement and practice strategies and action plans for reducing the risks of terrorist attacks on critical infrastructure and soft targets that integrate and leverage the capabilities of relevant public and private stakeholders; Establish or strengthen mechanisms to share information, expertise (such as tools and guidance) and experience among public and private stakeholders to investigate and respond to terrorist attacks on such targets.”
Guiding Principle 51	“In their further efforts to protect critical infrastructure and soft targets from terrorist attacks, Member States, acting in cooperation with local authorities, should also consider: [...] Putting in place national frameworks and mechanisms to support risk-based decision-making, information-sharing and public-private partnering for both Government and industry, including with a view to working together to determine priorities, and jointly developing relevant products and tools, such as general guidelines on surveillance or specific protective measures suggested for different types of facilities (for example, stadiums, hotels, malls or schools); Establishing processes for the exchange of risk assessments between Government, industry and the private sector, to promote and increase situational awareness and strengthen soft target security and resilience; Promoting public-private partnerships by developing cooperation mechanisms, supporting business owners and operators and infrastructure managers and by sharing plans, policies and procedures, as appropriate.”

4.2 Common Values as the Baseline for Public–Private Partnerships

PPPs between governments and CI owners/operators exist in different shapes and sizes. Effective PPPs that achieve specific pre-defined objectives require a common set of values shared by all parties. In 2016, the Meridian Process, a forum for the exchange of ideas on critical information infrastructure protection and for collaboration among senior government policymakers, identified a series of factors that sustain effective PPPs:

- **Trust:** Since PPPs often deal with sensitive subjects, it is essential to create an atmosphere of trust in which all involved organizations show awareness of each

Available at: <https://documents.un.org/doc/undoc/gen/n15/448/85/pdf/n1544885.pdf> [accessed 12 May 2025].

175 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> [accessed 12 May 2025].

other's need for discretion. Clear membership guidelines regarding operating rules may support efforts to build trust.

- ▶ **Value:** PPPs need to produce benefits to sustain participants' enthusiasm and motivation over time.
- ▶ **Respect:** Each involved entity must recognize the added value that the other entities bring to the collaborative endeavour.
- ▶ **Code of conduct:** It is necessary to have clear, specific and predictable rules that are not open to interpretation and that prevent any conflict of interest.
- ▶ **Awareness of each other's capabilities and restrictions:** This prevents conflict based on misjudging reasons for negative responses, and allows for an optimum return on the efforts undertaken. This implies that each entity should be familiar with the business of the other entities involved.
- ▶ **Realistic expectations:** Involved entities have to take into consideration resource affordability, development budgets, and other factors to enable realistic expectations from the PPP in question.¹⁷⁶

Spotlight: The Importance of Trust

While trust has already been referred to as a factor that sustains effective PPPs, its central importance to the success of PPPs cannot be understated. Willingness to share information within any relationship is closely linked to the level of trust between the involved parties. Information of value is almost always sensitive to the holder of that information. For private CI owners/operators and their private security providers (where relevant), this may be information about facility vulnerabilities, vital infrastructure nodes, site security arrangements, trade secrets or intellectual property. For government actors, this can be sensitive information or intelligence related to recent or ongoing criminal investigations, terrorist or criminal threats (including threat actors, modus operandi, capabilities) or intelligence sources. For both parties, sharing such sensitive information may jeopardize the sources or methods by which it was collected, reveal strengths or weaknesses of a critically important facility, and/or allow information to be misused to build or erode competitive advantage.

At the core of efforts to overcome these sensitivities – efforts such as entering into formal legal arrangements, providing security clearances for private sector representatives, or other measures – is trust. Parties in a PPP must trust that all involved will use shared information for its intended purpose and will protect it from misuse. Trust can be built in many ways, including routine face-to-face engagement.

¹⁷⁶ Global Forum on Cyber Expertise (2017), *The GFCE-Meridian Good Practice Guide on Critical Information Infrastructure Protection for government policy-makers*. Available at: <https://thegfce.org/wp-content/uploads/gfce-meridian-gpg-to-ciip-1.pdf> [accessed 12 May 2025].

Practice: OSCE – Eight Steps for Pursuing Effective Public–Private Partnerships (2013)¹⁷⁷

The below eight steps have been extracted from the *OSCE Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*, published in 2013. They are, however, relevant for a broader range of CI sectors, as well as for addressing physical threats such as terrorism.

Step 1

Analyse and identify the motivation of each partner who will be part of a CIP partnership, in order to clarify mutual expectations and contributions.

Step 2

Define aspirations and objectives of the CIP partnerships based on relevant national CIP goals; clarify the purpose of CIP partnerships and the tasks to be accomplished by the participating organizations.

Step 3

Review the existing regulatory framework relevant for each critical infrastructure sector; identify mandatory requirements; assess the adequacy of the existing regulatory framework relating to expected risks and existing preparedness levels; discuss how to close possible gaps.

Step 4

Provide mechanisms, protections, and legal certainty to facilitate the exchange of CIP-related information between stakeholders. In addition, provide mechanisms to allow the development and exchange of best practices, consultation and dialogue to ensure ongoing and effective partnerships.

Step 5

Set up an institutional structure that fosters cross-organizational co-operation and partnership working, and which facilitates information exchange; the roles and contributions of each partner (for example, government agencies, owners and operators of critical infrastructure, product suppliers, associations) should be clarified; identify single points of contact for each partner; establish guidelines for co-operation between all parties involved.

Step 6

Start small by focusing on one or two critical infrastructure sectors first of all to identify and resolve issues; after this, grow steadily while building on the readiness of all stakeholders to co-operate and consider threat levels.

Step 7

Define critical milestones to review what has been achieved and identify potential next steps. It is important to undertake this review process to find out what has worked and what has not.

Step 8

Provide for a constant review process to revisit and update partnerships to ensure continual progress commensurate with the overall risk landscape and the safety and security measures that are needed to provide an optimal level of protection.

Source: OSCE

¹⁷⁷ OSCE (2013), *Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*. Available at: <https://www.osce.org/files/f/documents/4/b/103500.pdf> [accessed 12 May 2025].

4.3 Information-Sharing within Public–Private Partnerships

Governments, particularly their intelligence and law enforcement authorities (at both a national and local level), have a significant role in ensuring that threat information is appropriately disseminated and understood across government and within CI sectors, including private stakeholders. If threat information is not shared with stakeholders outside government, it may lead a CI owner/operator or its security provider to conduct an inaccurate or incomplete assessment of a CI facility's vulnerability. Similarly, CI owners/operators and private security providers are well positioned to share information on site-specific security arrangements, areas of particular interest to threat actors, suspicious activities, and incidents of concern. When this information is combined, with due respect and alignment with local laws, all stakeholders have a clearer picture of the current threat situation and can take action accordingly. As a result, across the OSCE area, many CI owners/operators and government actors engage in PPPs with information-sharing provisions.

Information-sharing can also take place between private sector actors, such as CI owners/operators within the same sector or even across sectors. Across the OSCE area, there are multiple sector-specific and industry-led associations and groups that provide an additional avenue for learning and sharing expertise and experience, as for example the United States' National Council of Information Sharing and Analysis Centers,¹⁷⁸ the CoESS,¹⁷⁹ and the European Utilities Telecom Council.¹⁸⁰

UNSC Resolution 2341 (2017) provides a strong foundation for promoting information-sharing between private and public actors to protect CI from terrorist attacks. In this resolution, the Security Council,

"4. Calls upon [UN] Member States to explore ways to exchange relevant information and to cooperate actively in the prevention, protection, mitigation, preparedness, investigation, response to or recovery from terrorist attacks planned or committed against critical infrastructure."

"8. Affirms that regional and bilateral economic cooperation and development initiatives play a vital role in achieving stability and prosperity, and in this regard calls upon all States to enhance their cooperation to protect critical infrastructure, including regional connectivity projects and related cross-border infrastructure, from terrorist attacks, as appropriate, through bilateral and multilateral means in information sharing, risk assessment and joint law enforcement."¹⁸¹

178 National Council of Information Sharing and Analysis Centers (ISACs) (no date), About ISACs [webpage]. Available at: <https://www.nationalisacs.org/about-isacs> [accessed 25 March 2025].

179 CoESS (no date) [website]. Available at: <https://www.coess.org/> [accessed 25 March 2025].

180 European Utilities Telecom Council (EUTC) (no date) [website]. Available at: <https://eutc.org/> [accessed 25 March 2025].

181 UNSC (2017), Resolution 2341 (S/RES/2341). Available at: <https://documents.un.org/doc/undoc/gen/n17/038/57/pdf/n1703857.pdf> [accessed 5 May 2025].

The United Nations 2022 *Compendium of Good Practices for the Protection of Critical Infrastructure Against Terrorist Attacks* highlighted three categories for information-sharing between government authorities and CI owners/operators:

- ▶ **“Threat assessments:** Law enforcement bodies and intelligence services should provide CI operators with national threat assessments affecting specific critical assets and processes and critical sectors. This information needs to be fed into the risk assessments that CI operators are expected to conduct, often in compliance with regulatory requirements mandating them to prepare and share CI-level security plans. Conversely, it is essential for individual CI operators to share their own threat assessments with the competent government authorities for these latter to be able to paint an accurate picture of the threat, both within a given CI sector and at the cross-sectoral level.
- ▶ **“Suspicious activities:** CI operators have a critical role to play in observing and reporting unusual activities taking place within or around the assets and processes of which they are in charge. This task should be the responsibility not only of those specifically in charge of security, but also those who get into contact with CI assets, processes and systems as employees, contractors, suppliers, and other stakeholders. Appropriate awareness-raising programmes and training activities should be in place to ensure that those people are in a position to recognize suspicious behaviour and know to whom to report it.
- ▶ **“Incident-related data and perspectives:** Lessons learned from past incidents (including successful practices and interventions and failures) offer important insights into ways of preventing the same situation from reoccurring. This, in turn, provides a basis for more effective risk management and recovery action.”¹⁸²

Some of the above points may also be valuable for private security providers involved in protecting a given CI facility.

Importantly, given the sensitivity of information relevant to the protection of CI, the following key points should be considered as part of any PPP:

- ▶ Relevant information should not be used other than for the purpose of protecting CI.
- ▶ Any personnel handling classified or sensitive information should have an appropriate level of security vetting from the relevant government authorities to ensure the information is treated with due care.
- ▶ Stakeholders within a PPP should recognize that certain information shared, even if unclassified, may still be sensitive and therefore needs to be treated with care.
- ▶ If the relevant information includes personal data, the collection, processing, storage and transfer must be carried out in accordance with the national legal framework and international standards.

¹⁸² UNOCT, UNSC Counter-Terrorism Committee Executive Directorate (2022), *The protection of critical infrastructures 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 [accessed 3 May 2025].

Information exchange between organizations is addressed in the International Organization for Standardization's Standard No. 22396:2020: "Security and resilience – Community resilience – Guidelines for information exchange between organizations".¹⁸³

National Practice: United States Protected Critical Infrastructure Information Program (2022)¹⁸⁴

The Protected Critical Infrastructure Information Program was created by the United States Congress in 2002. The goal of the Program is to "protect information voluntarily shared with the government on the security of private and state/local government critical infrastructure". The Program established uniform procedures for the receipt, validation, handling, storage, marking and use of CI information voluntarily submitted to CISA of the US DHS. It also provides protection for CI owners/operators, which has led to enhanced voluntary sharing of information with the government. It also gives CI owners confidence that any shared information will not compromise sensitive or proprietary data to public exposure.

Source: US DHS CISA

¹⁸³ ISO (2020), *Security and resilience — Community resilience — Guidelines for information exchange between organizations* (ISO Standard No. 22396:2020). Available at: <https://www.iso.org/standard/50292.html> [accessed 12 May 2025].

¹⁸⁴ Cybersecurity & Infrastructure Security Agency (no date), Protected Critical Infrastructure Information (PCII) Program [website]. Available at: <https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program> [accessed 25 August 2024].



Terrorism Threat and Risk Assessment

//

A nuanced assessment of extant threats and risks to a given critical infrastructure facility is central to protecting it from terrorist attacks.

//

5 Terrorism Threat and Risk Assessment

CI comprises sectors and facilities that are integral to daily life and support the critical services and functions necessary for the safety, security, economic stability, human rights and overall well-being of society. As such, CI is an appealing target for terrorists due to the widespread disruption, fear, and economic damage such attacks can cause. Terrorists choose targets based on a broad mix of strategic, symbolic and operational factors, which are then combined with the characteristics, motivations and objectives of their terrorist organization.¹⁸⁵ It can therefore be extremely difficult to know exactly who, what and where terrorists will aim to strike, particularly since many States face simultaneous threats from multiple terrorist organizations of different ideological persuasions.

In this chapter, a review of the methods terrorists employ to attack CI is presented, as well as the basics of the risk assessment process, which is a vital preliminary step for determining physical security arrangements for any CI site. Particular attention is paid to the importance of pursuing an all threats and all hazards approach to CIP, in line with UNSC Resolution 2341 (2017).

There are several interconnected reasons why attacking CI facilities might be attractive to terrorist organizations. Several of these are presented below.



Symbolic Value

Terrorists may seek targets of symbolic value to their adversaries. In some cases, this may be CI such as oil/gas pipelines, transportation infrastructure or government facilities.



Economic Damage

Damage to and/or destruction of CI assets can cause extensive financial loss due to repair costs, economic disruptions and loss of productivity. Extended disruptions caused by attacks of this nature can lead to long-term economic instability, weakening a nation's economy, resilience and investment framework.



Psychological Impact

Terrorists target CI in part to create a pervasive sense of vulnerability and fear among the public. A successful attack on CI may lead members of the public to believe authorities are unable to protect critical services, which in turn can damage public confidence in government and its ability to maintain security and order.

¹⁸⁵ Schmitt, K. (no date), Targets of Terrorists, US Department of Justice, NCJ Number 63429. Available at: <https://www.ojp.gov/ncjrs/virtual-library/abstracts/targets-terrorists> [accessed 12 May 2025].

Propaganda Value

Terrorists may select a target based upon a specific message they wish to deliver or to advance a particular narrative. Successful attacks on CI also serve as a recruitment tool for terrorist organizations, enhancing their attractiveness to prospective new members by demonstrating their capabilities and commitment to a cause.

Retaliation

Terrorist organizations may select a specific CI target as part of a wider retaliatory strategy in response to previous incidents or operations carried out against them.

Media Attention

Terrorists typically target a location likely to attract media attention, which amplifies their message and spreads fear. Attacks on CI can garner significant media attention due to their widespread impact.

Long-term Consequences

Attacks on CI can force governments to divert significant resources towards CI protection and restoration, which can strain budgets and make it harder for authorities to manage the immediate aftermath of an attack. Prolonged disruptions of CI – such as a widespread blackout – can lead to social unrest, political instability, and increased polarization within society, aspects that in turn can act as drivers of radicalization to terrorism and violence.

Maximizing Casualties

Terrorist organizations may target areas with large concentrations of people (such as public transportation systems) to maximize their impact. Such incidents also draw significant media attention. As a result, terrorists may plan attacks to coincide with events or periods where more people are likely to be present, such as rush hour on a metro system.

5.1 How Do Terrorists Attack Critical Infrastructure?

This *Technical Guide* is focused on physical security for CI facilities, with an emphasis on terrorist attacks. This section details the modus operandi used by terrorists to conduct attacks. While it does not provide an exhaustive list, it does cover many of the key categories. In some cases, terrorists also combine the modus operandi described here, such as a terrorist attack using both vehicles and explosives.

	Explosives Explosives and improvised explosive devices (IEDs) are commonly used by terrorists as an attack method due to their destructive power, relative ease of construction, and potential to cause mass casualties. IEDs can be made from readily available materials, making them accessible to a wide range of groups, regardless of their resources. They can be deployed in various ways: person-borne IEDs, vehicle-borne IEDs, water-borne IEDs, roadside bombs, or hidden and activated as radio controlled IEDs. This allows for flexible targeting of both civilians and CI. The unpredictability and potential for high casualties make explosives and IEDs a highly effective tool for instilling fear, disrupting societies, and drawing attention to terrorists’ causes.
	Firearms Firearms are a consistent attack method for terrorists due to their accessibility, ease of use, and lethal effectiveness. They allow attackers to inflict significant casualties quickly, particularly in crowded or confined spaces. Firearms can be obtained through both licit and illicit channels, and they require minimal training compared to more complex weapons. The mobility and control offered by firearms enable terrorists to carry out co-ordinated attacks, target specific individuals or groups, and sustain assaults over a longer period to increase their impact. Additionally, firearm attacks often attract significant media attention, which can contribute to reinforcing the terrorists’ message.
	Vehicles Terrorists use vehicles as weapons because they are easy to access, require minimal planning, and can cause significant casualties, particularly in crowded urban areas. Vehicles can be turned into deadly tools by driving them into groups of people, making them effective for spontaneous or low-cost attacks. This method requires little technical skill or preparation, which makes it attractive to lone actors or small groups. The unpredictability of vehicle attacks makes them difficult to prevent.

	Arson Terrorists can deliberately set critical infrastructure assets (fences, structures, storage facilities, etc.) on fire in order to damage or destroy them. Since this is a relatively low-cost attack method, it is possible for anyone to use it at any facility. Arson can also be combined with other attack methods listed here, including firearms and/or kidnapping/hostage-taking.
	Kidnapping/Hostage-taking Kidnapping and hostage-taking are used by terrorists to exert pressure, gain leverage, and attract media attention. Such tactics allow terrorists to demand ransoms, secure the release of imprisoned members of their group, or force political concessions from governments. Hostage situations create intense fear and uncertainty, as well as public and media interest. The prolonged nature of such incidents can disrupt societies, strain security forces, and create a powerful psychological impact.
	Unmanned Aircraft Systems Unmanned aircraft systems (UAS), also known as drones, are increasingly being used as an attack method by terrorists due to their growing accessibility, decreases in their cost, and their potential ability to bypass traditional security measures.¹⁸⁶ Since UAS can be easily purchased, the potential ability for attackers to target CI, public gatherings or military installations from a distance with minimal risk to themselves marks UAS as a technology of concern. Additionally, UAS can be operated remotely, making it difficult to trace or intercept perpetrators.
	Chemical, Biological, Radiological, Nuclear Materials Terrorists may use chemical, biological, radiological, and nuclear (CBRN) materials as an attack method because of their potential to cause mass casualties, widespread fear, and long-term disruption. CBRN weapons can be incredibly lethal and challenging to detect or defend against. The use of such materials can contaminate large areas, overwhelm medical systems, and have devastating psychological effects on populations. The mere threat of a CBRN attack can cause significant panic and strain on governments.
	Enabler: Cultivation of Insiders Terrorists use “insiders” due to their authorized access to CI facilities, sensitive information, and security protocols, all of which can be exploited to plan and execute more effective attacks. Insiders can help terrorists bypass security measures, provide intelligence on targets, and even directly participate in sabotage or attacks, increasing their chances of success while minimizing the risk of detection. While not a strict modus operandi used to attack CI facilities, the cultivation of insiders may be seen as an enabler of attacks and therefore has been placed in this list.

¹⁸⁶ For information on the threat posed by the use of UAS by terrorists, see, e.g., UNSC (2023), Guiding principles for Member States on countering the use of new and emerging technologies for terrorist purposes (S/2023/1035). Available at: <https://docs.un.org/en/S/2023/1035> [accessed 13 May 2025].

5.2 Threat and Risk Assessments: Considerations and Differences

A nuanced assessment of extant threats and risks to a given CI facility is central to protecting that facility from terrorist attacks. Such assessments drive the range of security responses, including physical security measures. If these assessments are incomplete or inaccurate, it can put CI facilities, personnel or processes in danger.

Threat: The United Nations Security Management System defines a threat as “a potential cause of harm initiated by deliberate actions”.¹⁸⁷ Threats can be direct (i.e., a clear, defined expression of intent to target a given facility) or generalized (i.e., a broad expression of intent to target a sector, religious group or entire country). Both should be taken seriously when identifying and assessing threats to a given CI facility. When doing so, there are several key intelligence questions one can consider, including:

WHO	Which threat actor might launch an attack?
WHAT	What assets may the threat actor attempt to attack? What might they use to carry out an attack?
WHY	What is the purpose of an attack?
WHERE	What may be the location of an attack?
WHEN	At what point in time might an attack occur? Note: The more specific the response, the better: i.e., hour, day, month, year.
HOW	How might attackers carry out an attack? What would be potential attack methods? What is the probability of an attack occurring? What is the probability of an attack succeeding?

Considering such questions contributes to the development of a threat assessment that also includes features about possible attack methods. Another way to approach threat is to visualize it as a calculation:

$$\text{threat} = \text{intentions}^{188} \text{ of threat actors} \times \text{their capabilities}^{189}$$

Conducting a threat assessment allows those responsible for the security of a CI facility to understand and assess potential threat actors and threat scenarios, and in turn, to develop a sound foundation for an effective risk assessment. It is vitally important that a threat assessment is conducted before carrying out a risk assessment, since threat is a key component of risk (as shown in the risk calculation below).

¹⁸⁷ UN Department of Safety and Security (2017), *United Nations Security Management System: Security Policy Manual*. Available at: https://b2315f08-09cf-4a7a-b224-5b9df6403e51.usrfiles.com/ugd/b2315f_59d25533484d4430aede6ad4558aea66.pdf [accessed 12 May 2015].

¹⁸⁸ Defined as “[t]he motivation or disposition of a threat actor to cause the threat event as described” in: United Nations Department of Safety and Security (2017), *United Nations Security Management System Security Policy Manual*. Available at: https://b2315f08-09cf-4a7a-b224-5b9df6403e51.usrfiles.com/ugd/b2315f_59d25533484d4430aede6ad4558aea66.pdf [accessed 12 May 2015].

¹⁸⁹ Defined as “[t]he capacity or ability of threat actors to cause the threat event as described” in United Nations Department of Safety and Security (2017), *United Nations Security Management System Security Policy Manual*. Available at: https://b2315f08-09cf-4a7a-b224-5b9df6403e51.usrfiles.com/ugd/b2315f_59d25533484d4430aede6ad4558aea66.pdf [accessed 12 May 2015].

Risk: Risk is defined by the United Nations as “the likelihood of a harmful event occurring and the impact of the event if it were to occur”.¹⁹⁰ Risk can also be visualized as a calculation. One example is the following:

$$risk = threat \times vulnerability^{191} \times impact^{192}$$

In order to develop an understanding of risk to a given CI facility and ways to manage it, the following questions and considerations are important:

Component	United Nations Definition ¹⁹³	Core Question	Considerations
Threat	“A potential cause of harm initiated by deliberate actions”	What could threaten the operation?	▶ Past threat events ▶ Threat patterns (local, regional, global) ▶ Threat modelling and forecasts
Vulnerability	“A weakness that can allow a threat or hazard to cause harm”	How susceptible is the facility to being disrupted by the threat?	▶ Assessment of current conditions ▶ Recent security improvements ▶ Lessons learned from previous disruptions (local, regional, global)
Impact (often referred to as Consequence)	“A rating of the assessed potential harm that an event would have (if it were to occur) on the Organization”	If the facility is disrupted, what would be the impact?	▶ Interdependency analyses ▶ Impact assessments ▶ Resilience policies and business continuity plans

¹⁹⁰ United Nations Department of Safety and Security (2017), *United Nations Security Management System Security Policy Manual*. Available at: https://b2315f08-09cf-4a7a-b224-5b9df6403e51.usrfiles.com/ugd/b2315f_59d25533484d4430aede6ad4558aea66.pdf [accessed 12 May 2015].

¹⁹¹ Defined as “a weakness that can allow a threat or hazard to cause harm” in United Nations Department of Safety and Security (2017), *United Nations Security Management System Security Policy Manual*. Available at: https://b2315f08-09cf-4a7a-b224-5b9df6403e51.usrfiles.com/ugd/b2315f_59d25533484d4430aede6ad4558aea66.pdf [accessed 12 May 2015].

¹⁹² Often also referred to as “consequence”.

¹⁹³ United Nations Department of Safety and Security (2017), *United Nations Security Management System Security Policy Manual*. Available at: https://b2315f08-09cf-4a7a-b224-5b9df6403e51.usrfiles.com/ugd/b2315f_59d25533484d4430aede6ad4558aea66.pdf [accessed 12 May 2015].

5.3 The Importance of an “All Threats and All Hazards Approach”

To meet the challenges of both the current and future threat environment, in 2017 the United Nations Security Council encouraged countries to undertake a national approach to CIP that considers a range of threats and hazards impacting CI owners/operators and broader communities. As stated in UNSC Resolution 2341 (2017),¹⁹⁴ which focuses on the protection of CI from terrorist attacks, a consideration of all threats and all hazards¹⁹⁵ to CI is central to its protection from terrorist attacks:

“Recognizing in this regard that the effectiveness of critical infrastructure protection is greatly enhanced when based on an approach that considers all threats and hazards, notably terrorist attacks, and when combined with regular and substantive consultation and cooperation with operators of critical infrastructure and law enforcement and security officials charged with protection of critical infrastructure, and, when appropriate, with other stakeholders, including private sector owners.”

In practice, this means incorporating terrorism as a threat to CI in addition to other threats and hazards, such as natural disasters (extreme heat, volcanic eruptions, earthquakes, drought), cybersecurity incidents, technical failures, chemical spills, unintentional explosions, power outages, industrial espionage, fires, criminal activity, civil unrest, etc.

5.4 Assessing Risk

In UNSC Resolution 2341 (2017), the UN Security Council,

“[c]alls upon Member States to consider developing or further improving their strategies for reducing risks to critical infrastructure from terrorist attacks, which should include, inter alia, **assessing and raising awareness of the relevant risks, taking preparedness measures**, including effective responses to such attacks, as well as promoting better interoperability in security and consequence management, and facilitating effective interaction of all stakeholders involved”.¹⁹⁶

Given the sensitive nature of the risk assessment process, few national good practices will be cited in this section. Rather, it provides guidance on assessing general risks, guidance that can be used to support existing processes for participating States and CI owners/operators. For more detailed and targeted guidance on risk management, CI owners/operators may wish to refer to the guidelines on risk management of the

194 UNSC (2017), Resolution 2341 (S/RES/2341). Available at: <https://documents.un.org/doc/undoc/gen/n17/038/57/pdf/n1703857.pdf> [accessed 5 May 2025].

195 A hazard is defined as “a potential cause of harm resulting from non-deliberate actions” in United Nations Department of Safety and Security (2017), *United Nations Security Management System Security Policy Manual*. Available at: https://b2315f08-09cf-4a7a-b224-5b9df6403e51.usrfiles.com/ugd/b2315f_59d25533484d4430aede6ad4558aea66.pdf [accessed 13 May 2025].

196 UNSC (2017), Resolution 2341 (S/RES/2341). Available at: <https://documents.un.org/doc/undoc/gen/n17/038/57/pdf/n1703857.pdf> [accessed 5 May 2025].

International Organization for Standardization (ISO 31000:2018).¹⁹⁷ It is important to note that risk assessment is only one part of the risk management process. Once risks have been assessed in a clearly-defined process, the next step is referred to as risk treatment,¹⁹⁸ in which organizational responses to identified risks are designed and implemented.

Risk assessments related to terrorist attacks are not an exact science. Each individual involved in such an assessment may interpret the process differently. It is important to ensure that the team conducting a risk assessment are given quality data (including information about threat actors, their intentions and capabilities, and previous incidents) as well as a structured model or template.

Some governments and actors bring together a range of stakeholders as part of the risk assessment process. For example, the United Kingdom's annual National Security Risk Assessment (NSRA) evaluates risks (such as terrorism, accidents and systems failures, natural and environmental hazards, etc.) across seven broad dimensions: impact on human welfare, behavioural impacts, impact on essential services, economic damage, environmental impact, impact on security, international impacts. The NSRA is used as a basis for the elaboration of Sector Resilience Plans, which are developed by each of the governmental departments in charge of the United Kingdom's 13 critical sectors.¹⁹⁹

Additionally, given the high degree of private security used in the CI sector, the highest quality risk assessments are typically those that benefit from public–private partnerships, such as between law enforcement and those responsible for the security of a CI facility. For more information on how to establish effective partnerships, see Chapter 4, Public–Private Partnerships.

¹⁹⁷ ISO (2018), *Risk management – Guidelines* (ISO Standard No. 31000:2018). Available at: <https://www.iso.org/standard/65694.html> [accessed 13 May 2025].

¹⁹⁸ ISO (2018), *Risk management – Guidelines* (ISO Standard No. 31000:2018). Available at: <https://www.iso.org/standard/65694.html> [accessed 13 May 2025].

¹⁹⁹ HM Government (2023), *National Risk Register 2023*. Available at: https://assets.publishing.service.gov.uk/media/64ca1dfe19f5622669f3c1b1/2023_NATIONAL_RISK_REGISTER_NRR.pdf [accessed 13 May 2025].

5.5 Managing Risk

Although there are a range of different models for risk management across the OSCE area, in line with ISO 31000:2018 it typically consists of the following phases, best viewed as an iterative and cyclical process: customizing the process, risk assessment, risk treatment, monitoring and review.²⁰⁰



The risk management cycle is best carried out routinely in order to capture evolving threats, security improvements and other developments that may change the risk profile of a given facility. In most cases, senior leadership at CIs will be responsible for the risk management process and thus their involvement throughout is vital.

A CI owner/operator's risk management process should be documented and managed by security professionals with experience in risk management who are familiar with the CI facility, with the support of competent authorities and other authorized partners. ISO 3100:2018 also encourages reporting the risk management process and its outcomes throughout an organization, as needed, and to other relevant stakeholders as part of an organization's governance framework.

²⁰⁰ ISO (2018), *Risk management – Guidelines* (ISO Standard No. 31000:2018). Available at: <https://www.iso.org/standard/65694.html> [accessed 13 May 2025].

**National Practice: United Kingdom Health and Safety Executive's Risk Assessment
Template for Businesses²⁰¹**

Organisation:						
Assessment carried out by:						
Date of next review:						
Date assessment was carried out:						
What are the hazards?	Who might be harmed and how?	What are you already doing to control the risks?	What further action do you need to take to control the risks?	Who needs to carry out the action?	When is the action needed by?	Done?

Source: UK Health and Safety Executive

Customizing the Risk Management Process: Each CI owner/operator will need to tailor the risk management process to their unique situation and needs. In this phase, decisions are made about relevant risk criteria, the scope of risk management activities, the objectives of the risk management process, and other key parameters.

Risk Assessment: The phase of risk assessment involves identifying and assessing potential risks that could affect the CI facility and its operations. It includes gathering information on all possible internal and external threats such as those described above. Methods used in this phase might include open-source research, focus group sessions, interviews with key stakeholders, historical data analysis, industry reports and consultation with local and national security services. One goal is to create a comprehensive list of threats and threat scenarios that could impact the CI facility. Once threats are identified, the probability of each threat scenario occurring and the severity of its impact (or consequence) is analysed. Risks are then evaluated against existing risk criteria with a view towards decision-making and the CI owner/operator's risk appetite (i.e., the level of risk a CI owner/operator is willing to accept). Tools such as risk matrices can be employed to help prioritize risks, which can reveal risks requiring immediate attention and those that can be monitored over time.

Risk Treatment: Strategies are then developed and implemented to mitigate, or treat, identified risks. Mitigation measures can be preventive, such as installing security measures or adopting new policies, or corrective, such as developing incident response

²⁰¹ This sample risk assessment matrix was extracted from the UK government Health and Safety Executive, produced for businesses within the United Kingdom. Health and Safety Executive (2019), Risk assessment template [webpage]. Available at: <https://www.hse.gov.uk/simple-health-safety/risk/risk-assessment-template-and-examples.htm> [accessed 16 December 2024].

plans and training programmes to better prepare personnel for such incidents. Ultimately, a key objective for a CI owner/operator is to make informed decisions about what to do regarding specific risks, using practical and cost-effective solutions.

Monitoring and Review: This phase of the risk management cycle involves monitoring risks and reviewing the implementation of risk treatment strategies to ensure they are functioning as intended. This includes evaluating the success of mitigation measures, the accuracy of risk assessments, and the efficiency of the monitoring processes. Tools for monitoring risks can include audits and inspections by external experts. Regular reviews, often conducted annually or after significant incidents, ensure that the resultant risk management output (often in the form of a risk management plan) remains relevant and effective. Feedback from this phase is used to enhance and develop future risk management efforts, creating a continuous feedback loop that enables consistent improvements.



Physical Security Measures

//

It is clear that terrorist actors have a range of attack methodologies at their disposal, ranging from explosives, firearms, unmanned aerial systems, CBRN materials, and vehicles, to kidnapping or hostage-taking. This means that devising effective physical security measures is vitally important for the protection of any critical infrastructure facility.

//

6 Physical Security Measures

There are a variety of malicious actors, including terrorists, who pose physical threats to CI facilities with the intention of rendering them inoperable (either in full or in part) by destroying or damaging them. Understanding the nature of the terrorist threat to a specific CI facility requires a comprehensive assessment of the intent and capability presented by terrorist organizations and the risks they pose, as detailed above in Chapter 5, Terrorist Threat and Risk Assessment. It is clear that terrorist actors have a range of attack methodologies at their disposal, ranging from explosives, firearms, UAS,²⁰² CBRN material, and vehicles, to kidnapping or hostage-taking. This means that devising effective physical security measures is vitally important for the protection of any CI facility. In Chapter 5, the concept of risk was presented as a calculation of *threat* x *vulnerability* x *impact*. In this chapter, potential measures to reduce the vulnerability of CI facilities are explored, with a focus on physical security.



The importance of security enhancements at CI facilities has been recognized by both the UN and the OSCE. The OSCE Consolidated Framework for the Fight Against Terrorism, adopted in December 2012, states that the OSCE should enhance co-operation and build capacity to prevent and combat terrorism, including in relation to improving “the security of international transportation and of other critical infrastructure.”²⁰³ Specific to critical energy infrastructure, in 2007 the OSCE Ministerial

²⁰² Additional guidance on measures to prevent terrorists from acquiring weapons, such as explosive devices, UAS and firearms, can be found in the *Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017) and related international standards and good practices on preventing terrorists from acquiring weapons*, published by the UNOCT, UNSC Counter-Terrorism Executive Directorate, UN Institute for Disarmament Research, and the UN Global Counter-Terrorism Coordination Compact.

²⁰³ OSCE (2012), Permanent Council Decision No. 1063: OSCE Consolidated Framework for the Fight Against Terrorism (PC.DEC/1063). Available at: <https://www.osce.org/files/f/documents/7/5/98008.pdf> [accessed 13 May 2025].

Council called on all participating States “to consider all necessary measures at the national level to ensure an adequate protection of critical energy infrastructure from terrorist attack”.²⁰⁴ And the UN Security Council, in its Resolution 2341 (2017), has recognized that the many efforts needed to protect CI must include “physical protective measures.”²⁰⁵

This chapter examines the various ways physical security can be improved and the steps needed to develop a security system (including examples of different national approaches and models). It will then explore a range of physical security measures that form the constituent parts of a physical security system, including intrusion detection systems, lighting, video surveillance systems, perimeter security, access control systems, security screening, and the use of restricted areas. Finally, it will look at design and construction techniques that can enhance the physical security of CI facility buildings, including construction materials, installation of secure street furniture, and the form and location of different security measures.

The implementation of physical security measures should also be supported by proper personnel and procedural measures to ensure that they are executed by authorized individuals and regularly tested. Such measures should be enforced by properly vetted and trained personnel. They must also be supported by comprehensive contingency and security plans developed at the CI operator level, and be fit for deployment within a CI facility. These plans should be exercised on a regular basis and updated when required (see Chapter 9, Training and Exercising).

204 OSCE (2007), Ministerial Council Decision No. 6/07: Protecting Critical Energy Infrastructure from Terrorist Attack (MC.DEC/6/07). Available at: <https://www.osce.org/files/f/documents/4/5/29482.pdf> [accessed 13 May 2025].

205 UNSC (2017), Resolution 2341 (S/RES/2341). Available at: <https://documents.un.org/doc/undoc/gen/n17/038/57/pdf/n1703857.pdf> [accessed 5 May 2025].

National Practice: Finland's National Emergency Supply Agency's General Contingency Measures Recommended for Companies (2022)²⁰⁶

Finland's National Emergency Supply Agency provides the following recommendations for the protection of companies' critical infrastructure:

- ▶ Check access control, locks, surveillance, physical protection and other measures depending on the needs of physical objects.
- ▶ In particular, review cybersecurity protection measures and incident management practices for critical core business functions.
- ▶ Ensure sufficient reliable telecommunications connections for critical operations from the perspective of operational resilience.
- ▶ Ensure the energy supply of critical operations, i.e., by ensuring the availability of substitute energy sources and by examining the ability of operations to withstand interruptions in energy supply.
- ▶ Review the organization's continuity management and preparedness measures and plans.
- ▶ Encourage staff to be vigilant and ensure that employees receive up-to-date information.
- ▶ Notify the authorities and the network of observations at a low threshold in order to obtain an overall picture of the situation and initiate possible support measures if necessary.

Source: Finland National Emergency Supply Agency

6.1 Conceptualizing Physical Security

The aim of physical security systems is to protect CI facilities, including equipment and occupants, from unauthorized physical intrusion, damage, destruction, or disabling of functionality. Physical security can consist of both active and passive measures designed to deter intruders and to safeguard assets²⁰⁷ against a range of threats, including unauthorized access, theft and damage. Both CI owner/operators and relevant national authorities are responsible for determining the make-up of physical security systems.

The United Nations 2022 *Compendium of Good Practices for the Protection of Critical Infrastructure Against Terrorist Attacks* lists example physical security measures, including:

- ▶ Delineation of CI area perimeters and protection of these by physical barriers;
- ▶ Patrols and surveillance by law enforcement and CI operators, with a view to quickly identifying suspicious activity occurring around a critical site (such as hostile reconnaissance) and reporting it to the relevant authorities;

²⁰⁶ National Emergency Supply Agency (12 October 2023), Companies have many ways to protect critical infrastructure [webpage]. Available at <https://www.huoltovarmuuskus.fi/en/a/companies-have-many-ways-of-protecting-critical-infrastructure> [accessed 13 May 2025].

²⁰⁷ E.g., personnel, equipment, installations, materials and information.

- ▶ Access control, with security features used to increase its performance or effectiveness (such as barbed wire topping on fences, perimeter intrusion detection systems, lighting or a closed-circuit television system);
- ▶ Use of technology such as screening and other security controls (i.e., conventional or high-definition X-ray equipment, explosive detection dogs, hand-held metal detectors, and explosives trace detection technology).²⁰⁸

National Practice: Norwegian National Security Authority Physical Security Guidance (2020)²⁰⁹

In 2020 the National Security Authority of Norway released public, non-binding basic principles for physical security. Targets for this guidance are businesses across all sectors wishing to protect their assets from a range of intentional as well as unintentional threats. The guidance is not limited to critical infrastructure sectors or companies. The National Security Authority presents four basic principles of physical security: (1) identify and map, (2) protect, (3) maintain and detect, and (4) manage and recover. The principles cover a range of measures such as lighting and visible security deterrents (fences, barriers, signage), as well as recommended procedures such as evacuation, lockdown and whistleblowing. The National Security Authority recommends regular training exercises for facility personnel, as well as a concerted focus on the ongoing maintenance of the security framework, including both measures and policies.

Source: Norway's National Security Authority

The Physical Security Program of the US Department of Defense characterizes physical security as employing “tangible protective and procedural security measures in combination with active or passive systems, technologies, devices, and security personnel used to protect assets from possible threats.”²¹⁰ The Program identifies key components for security systems as follows:

- ▶ Security forces and personnel under the control of the owner or user;
- ▶ Physical barriers, facility hardening, and active delay or denial systems;
- ▶ Secure locking systems, containers and vaults;
- ▶ Electronic security systems, such as intruder detection systems, radio frequency detectors, or electronic emissions detectors;
- ▶ Assessment of surveillance systems (i.e. closed-circuit television, thermal imagers, millimetre wave radar);
- ▶ Protective lighting;

²⁰⁸ UNOCT, and UNSC Counter-Terrorism Committee Executive Directorate (2022), *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices*. Available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf [accessed 13 May 2025].

²⁰⁹ Norwegian National Security Authority (NSM) (2 October 2020), Grunnprinsipper for fysisk sikkerhet [webpage]. Available at: <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-fysisk-sikkerhet/introduksjon> [accessed 30 October 2024] unofficial translation.

²¹⁰ US Department of Defense (2007), *Physical Security Program: US Dept of Defense, DoD Manual 5200.08-R (Incorporating Change 2, October 19, 2020)* (Washington, DC: US Department of Defense).

- ▶ Credential technologies, access control devices, biometrics, material or asset tagging systems, and contraband detection equipment;
- ▶ Dogs with licensed handlers (i.e., explosive detection dogs, patrol dogs, etc.).²¹¹

National Practice: Swiss Federal Office for Civil Protection Examples of Physical Security (2018)²¹²

The Swiss Federal Office for Civil Protection has developed a guide for the protection of critical infrastructure that provides points to consider for CI owners/operators when building and protecting their facilities, including:

Perimeter security	▶ Fencing (gapless, breakthrough-proof, minimum height requirements, protected against crossing over or under [i.e., barbed wire], video surveillance) ▶ Puncture-proof doors and gates ▶ Technical access control (intercom, video technology, staggered entry systems, identification card readers, keypads, etc.) ▶ Automatic electronic detection (alarm fences and gates, video technology with sensors, secured wall tops, radar observation, high frequency light barriers, alarms)
Building protection	▶ Protection of security areas (electronic, mechanical, access controls, special surveillance) ▶ Barred windows ▶ Safety glass in security areas ▶ Window protection (penetration resistant glaze, impact resistant laminated safety glass, lockable hinges, bolted retaining strips) ▶ Limited number of exterior doors ▶ Protection of main entrance (card or chip reader, couplable/self-locking locks, electric security door openers, automatic door closures, intercom with video, staggered entry systems, separation of entrance and exit) ▶ Protection of emergency exits (self-locking, automatic door closure, alarm doors) ▶ Provision of keys only for authorized persons ▶ Secure storage of back-up keys
Personnel safety measures	▶ For personnel (internal and external): ▶ Security check for internal and external employees ▶ Personnel adherence to laws, obligations, provisions, internal regulations, etc. ▶ Sensibilization of personnel concerning security (courses, exercises, seminars, team training, etc.) ▶ Security aware recruitment: experience, knowledge, background check (criminal records, etc.), integrity, reference check ▶ Ensuring security upon separation (return of all documents, office materials, keys, passwords, badges, etc.; non-disclosure agreements, etc.) ▶ Protection of staff (personal security etc.)
Outside personnel	▶ Registration: sign-in and -out visitor log ▶ Quick identification of visitors (i.e., through visitor badges) ▶ Ensuring that visitors are accompanied/supervised ▶ Control of delivery services and goods

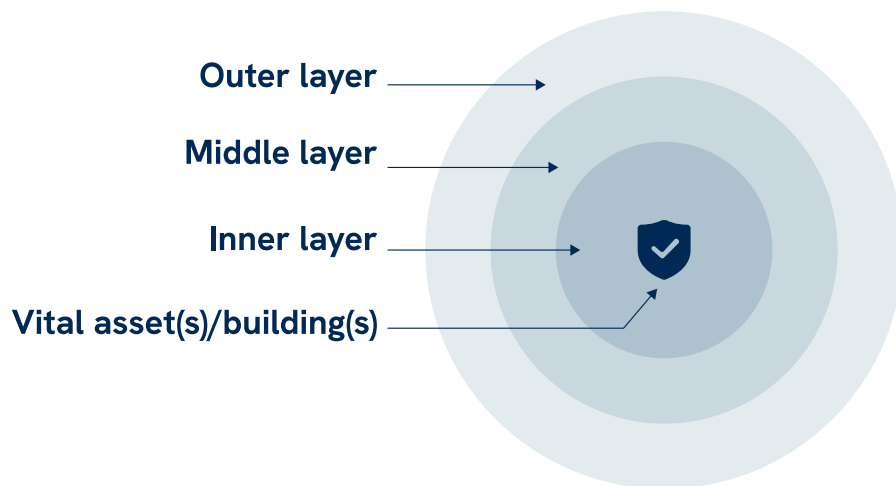
Source: Switzerland's Federal Office for Civil Protection

²¹¹ US Department of Defense (2007), *Physical Security Program. US Dept of Defense, DoD Manual 5200.08-R (Incorporating Change 2, October 19, 2020)* (Washington, DC: US Department of Defense).

²¹² Swiss Federal Office for Civil Protection (BABS), *Leitfaden Schutz kritischer Infrastrukturen* (Bern: BABS, 2018). Available at: <https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/27228b5a-2d7c-4c17-9df6-42e105197465.pdf> [accessed 13 May 2025] unofficial translation.

6.2 Defensive Layers or Defence-in-Depth

Physical security can be achieved through a variety of different approaches and technologies. One effective approach is the defence-in-depth concept, which consists of multiple consecutive layers of different security measures forming an intrusion detection system (IDS), guided by the underlying principle that the overall security of a facility is not significantly compromised by the loss of any single layer in and of itself. A key advantage of adopting this approach with its consecutive security layers, each more difficult to penetrate, is that it provides additional time for detection, assessment and response by a security team, and it gives facility personnel time to move to safe areas in the facility in case escape is not an option.²¹³



Layers can be seen as beginning from the outer perimeter of a given CI site or facility and moving inward to the building(s) with the greatest need for protection. Alternatively, layers can be seen in reverse: starting from what requires the most protection and working outwards.²¹⁴ Notably, if terrorist organizations use an “insider” to facilitate an attack, there is the potential to overcome some or all levels of security from the inside. More information can be found in Chapter 8, Insider Threat Management.

²¹³ UNOCT, and UNSC Counter-Terrorism Committee Executive Directorate (2022), *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices*. Available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf [accessed 13 May 2025].

²¹⁴ US DHS (2011), *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings: FEMA-426/BIPS-06/ October 2011. Edition 2*. Available at: <https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf> [accessed 13 May 2025].

National Practice: US Department of Homeland Security Defence-in-Depth Concept for the Protection of Buildings from Terrorist Attacks (2011)²¹⁵

1. First or Outer Layer: Natural or man-made barriers, usually at a property line or perimeter of a facility;
2. Second or Middle Layer: This typically extends from the perimeter of the site to the exterior face of the facility. Protective measures can consist of natural or man-made barriers, along with a site design strategy of keeping attackers away from key facilities.
3. Third or Inner Layer: Refers to the facade and/or inside the facility and separates unsecured from secured areas. The key concept of the third layer is building “hardening” or strengthening.

Source: US DHS

To strengthen layers of defence, CI stakeholders are increasingly implementing so-called “security-by-design” approaches at the stage of designing and constructing (or renovating) buildings. This helps minimize future physical security-related costs. An example of this approach is the handbook *Security by Design: Protection of Public spaces from Terrorist Attacks* published in 2022 by the European Commission’s Joint Research Centre.²¹⁶ Although the handbook focuses on the protection of public spaces, many of the security-by-design principles can also apply to CI.

6.3 Developing a Security System

Implementing physical security measures at a CI facility begins with the development of a security system tailored to that facility’s unique profile and needs. Security systems should involve components that work together seamlessly to provide an appropriate level of protection for a given facility and allow it to absorb, adapt to, and/or rapidly recover from a threat scenario, as for example, a terrorist attack. In nearly every case, a security system for a CI facility will incorporate more than just physical security measures.

For example, it may be valuable to consider personnel security a key component of a security system if it is aimed at reducing the risk of insider threats at a given facility (for more information, see Chapter 8, Insider Threat Management).

²¹⁵ US DHS (2011), *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings: FEMA-426/BIPS-06/ October 2011. Edition 2*. Available at: <https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf> [accessed 13 May 2025].

²¹⁶ Publications Office of the European Union (2024), *Security by Design: Protection of public spaces from terrorist attacks*. Available at: <https://publications.jrc.ec.europa.eu/repository/handle/JRC131172> [accessed 13 May 2025].

National Practice: US Department of Homeland Security's Five Component Parts of a Security System (2011)²¹⁷

1. *Security Policies, Plans, and Procedures*, including emergency action plans, security plans, training and testing procedures and responses, general procedure guidance, post-procedure guidance, and outside resources guidance.
2. *Security Operations and Intelligence*, which determine security needs and include security guard duties, intelligence and information sharing.
3. *Physical Barriers*, including fencing, gates and vehicle barriers.
4. *Security Systems and Equipment*, including electronic devices, computer systems and electronic access control.
5. *Cyber Security*, including measures that protect CI operating systems and data from cyber threats and unauthorized intrusions.

Source: US DHS

Security System Models

There are many different yet similar security system models, as for example:

International Atomic Energy Agency ²¹⁸	Deter, Detect, Delay, Respond
United Kingdom National Protective Security Authority ²¹⁹	Deter, Detect, Delay, Mitigate, Response
Australia ²²⁰	Deter, Detect, Delay, Respond, Recover
Singapore ²²¹	Deter, Detect, Delay, Deny, Respond

²¹⁷ US DHS (2011), *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings: FEMA-426/BIPS-06/ October 2011. Edition 2*. Available at: <https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf> [accessed 13 May 2025].

²¹⁸ International Atomic Energy Agency (IAEA) (2021), *Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities*. IAEA Nuclear Security Series No. 40-T. Available at: <https://www.iaea.org/publications/13459/handbook-on-the-design-of-physical-protection-systems-for-nuclear-material-and-nuclear-facilities> [accessed 13 May 2025].

²¹⁹ NPSA (2021), *Asset – Principles* [webpage, last updated 18 March 2021]. Available at: <https://www.npsa.gov.uk/asset-0> [accessed 12 January 2024].

²²⁰ Australian Government – Department of Home Affairs (2018), *Protective Security Policy Framework. Section 15: Physical security for entity resources*. V2018.3 (Belconnen: Department of Home Affairs).

²²¹ Joint Operations Group – Ministry of Home Affairs (no date), *Guidelines for Enhancing Building Security in Singapore*. Available at: <https://www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security> [accessed 13 May 2025].

Key to developing and implementing a security system and determining its model is defining each component. Example definitions for the above terms are:

Deter	Measures that lead “potential adversaries [to] regard a facility as an unattractive target and decide not to attack it because they estimate that their probability of success is too low or the risks for themselves are too high.” ²²²
Detect	Measures that “[begin] with sensing a potentially malicious or otherwise unauthorized act and that [are] completed with the assessment of the cause of the alarm.” ²²³
Delay	Measures that “[seek] to slow an adversary’s progress towards a target, thereby providing more time for effective response.” ²²⁴
Deny	Measures that “[ensure] that only authorized persons are allowed entry into protected areas.” ²²⁵
Mitigate	Measures that “[seek] to interrupt and neutralize an adversary to prevent the completion of any malicious act.” ²²⁶
Respond	Measures that “prevent, resist or mitigate an attack or event when it is detected.” ²²⁷
Recover	Measures that “restore operations to normal levels (as soon as possible) following an event.” ²²⁸

The structure of a given security system will be determined by the competent authorities and/or the CI owner/operator. As shown, there are various shapes and sizes for security systems. These should be tailored to a sector or facility’s threat environment and risk assessment. Important is defining a security system’s structure and using that structure as a basis for integrating all system components so they work towards the common goal of providing an appropriate level of protection for a given facility.

222 IAEA (2021), *Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities*. IAEA Nuclear Security Series No. 40-T. Available at: <https://www.iaea.org/publications/13459/handbook-on-the-design-of-physical-protection-systems-for-nuclear-material-and-nuclear-facilities> [accessed 13 May 2025].

223 IAEA (2021), *Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities*. IAEA Nuclear Security Series No. 40-T. Available at: <https://www.iaea.org/publications/13459/handbook-on-the-design-of-physical-protection-systems-for-nuclear-material-and-nuclear-facilities> [accessed 13 May 2025].

224 IAEA (2021), *Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities*. IAEA Nuclear Security Series No. 40-T. Available at: <https://www.iaea.org/publications/13459/handbook-on-the-design-of-physical-protection-systems-for-nuclear-material-and-nuclear-facilities> [accessed 13 May 2025].

225 Joint Operations Group – Ministry of Home Affairs (no date), *Guidelines for Enhancing Building Security in Singapore*. Available at: <https://www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security> [accessed 13 May 2025].

226 IAEA (2021), *Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities*. IAEA Nuclear Security Series No. 40-T. Available at: <https://www.iaea.org/publications/13459/handbook-on-the-design-of-physical-protection-systems-for-nuclear-material-and-nuclear-facilities> [accessed 13 May 2025].

227 Australian Government – Department of Home Affairs (2018), *Protective Security Policy Framework*. Section 15: *Physical security for entity resources*. V2018.3 (Belconnen: Department of Home Affairs).

228 Australian Government – Department of Home Affairs (2018), *Protective Security Policy Framework*. Section 15: *Physical security for entity resources*. V2018.3 (Belconnen: Department of Home Affairs).

6.4 Intrusion Detection Systems



Regardless of the security system model selected for a facility, managing and detecting authorized and unauthorized entry will always be a key component. This is achieved through an intrusion detection system (IDS). Using surveillance measures, the IDS detects changes in a target environment, such as an intruder, and then announces the unauthorized intrusion (through alarms). In addition to surveillance and alarm capabilities, an effective IDS is complemented by monitoring and response capabilities either on- or off-site.

An IDS typically includes internal and external alarm triggering devices such as motion detectors and door contacts. As part of its general functionality, an IDS monitors activities such as the opening/closing of access doors, or personnel movements in a target area. It may also extend to monitoring the target area's surrounding environment, such as the facility perimeter or other assets. This would enable the IDS, for example, to detect an attempt to cut the perimeter fence by a malicious actor.

When an unauthorized intrusion is detected, an IDS will generate an alarm, either at an on-site security point or at a remote monitoring centre for a follow-up response by designated security personnel. Given the sensitive nature of CI facilities and their protection, CI owners/operators may consider building in redundancies for their alarm communication channels, as well as back-up power sources to ensure systems still function, for example, in a power outage.²²⁹

²²⁹ Association of Banks in Singapore (2018), *Physical Security Guidelines for Financial Institutions*. Available at: <https://abs.org.sg/docs/library/abs-scps-guidelines.pdf> [accessed 13 May 2025].

As part of an IDS, facilities may implement standard measures for normal periods of operation, as well as additional measures for a period of enhanced threat. This may include additional surveillance measures and escalation plans guiding facility personnel on appropriate behaviour in the event of a threat being detected.

Intrusion Detection Technologies

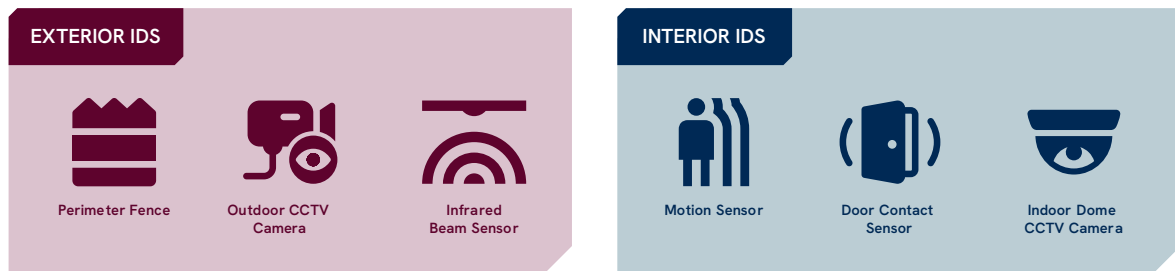
IDS can incorporate a range of technological measures to detect authorized and unauthorized movements. In many cases, the technologies selected by CI owners/operators may be based on local, national or industry performance standards, or guidance from competent authorities. The technological measures available to CI owners/operators will vary across the OSCE area. However, the United Kingdom's Centre for the Protection of National Critical Infrastructure (now the National Protective Security Authority [NPSA]) has presented a succinct list of the core categories of available detection technologies as part of the Authority's voluntary guidance on IDS for CI security managers, presented in the table below:²³⁰

Technology	Operating Principle
Passive infrared motion detection	Passive infrared detectors detect the presence of an intruder by sensing heat (infrared) emissions from the human body.
Microwave motion detection	Microwave motion detectors emit electromagnetic "radio" waves. When the microwaves come in contact with an object, some of the waves are absorbed, some are reflected and scattered in all directions, and some are reflected back to the detector.
Combined detectors	Detectors incorporating two or more detection technologies in a single housing (i.e., passive infrared combined with microwave) have become popular because of their increased stability in the service environment. The combination of differing technology types provides the benefit of increased resistance to false alarms, compared with detectors of only a single technology.
Glass break detectors	When glass breaks it generates a wide range of frequencies. Depending on type, glass break detectors use the frequencies in one or more of these bands to detect the breakage.
Vibration and shock detectors	Vibration and shock detectors are used in applications in which an expected intrusion attempt will result in the penetration of a planar surface (e.g., a wall) or another type of barrier. Intrusion techniques may include drilling, impacting with a sledgehammer, pick axe or similar tool, cutting with a saw or grinder or oxyacetylene torch/rope, or blasting with explosives.
Seismic detectors	Seismic vibration detectors are able to detect a wide range of forcible attacks, from high intensity shock impulses down to minute vibration tremors.
Inertia detectors	Inertia detectors are designed for general purpose use. They can provide a reliable and cost-effective solution for detecting most methods of forcible entry.
Shock sensors	Shock sensors typically respond to vibrations caused by forcible entry styles of attack such as ramming a door and removing it from its hinges.
Protective switches	Protective switches are used to sense when a door or window or other type of aperture is opened.
Active infrared detectors	Active infrared detectors provide one or more beams of infrared that can be aligned to create a "detection barrier" invisible to the human eye. If the beams are interrupted, for example by an intruder passing through them, the loss of infrared signal at the receiver is detected and an alarm created.

230 Centre for the Protection of National Infrastructure (2013), *Intrusion Detection Systems: Guidance For Security Managers*, pp. 59, 70, 75, 81, 86–88, 91, 96. Available at: <https://www.npsa.gov.uk/resources/intrusion-detection-systems-guidance-security-managers> [accessed 13 May 2025].

Types of Intrusion Detection Systems

To detect unauthorized intrusions at a CI facility, IDS have two different applications: exterior and interior. Each application comes with its own system requirements and different technological solutions. When designing exterior IDS, which potentially carry out the surveillance of persons who are not CI facility personnel, it is important to consider the human rights impacts of such activities, including data collection and storage (for more information, see Chapter 3, Human Rights Considerations). A general good practice for the protection of a CI facility is to incorporate both exterior and interior IDS elements. A description of each application is provided in the following.



Exterior IDS: The outer layers of a security system are often the most important component, since they provide for the earliest detection and reaction. As a general principle, the farther the exterior IDS layer is from the target (for example, a CI facility entrance or perimeter), the better. This means that exterior IDS are typically used to detect intrusions at or outside the perimeter of a target. However, NATO's 2020 Directive on Physical Security acknowledges that exterior IDS "are inherently prone to false alarm and should therefore normally only be used with an alarm verification system such as CCTV [closed-circuit television]."²³¹ Thus a security system that incorporates an exterior IDS should allow for rapid verification of trigger alarms to verify if malicious or authorized activity is indeed taking place.

Interior IDS: Interior IDS typically include a blend of sensors and video surveillance designed to detect unauthorized intrusions into a facility or target. When contrasted with exterior IDS, interior IDS are considered less costly since they are often better protected, including from inclement weather. The specific sensor or blend of sensors selected as part of an IDS will be determined by security managers and competent authorities, and based on relevant guidance and performance standards. They often include boundary-penetration sensors that function by detecting successful or attempted penetration into a given target through its perimeter.²³²

²³¹ Criscuolo, M. (2020), Directive on Physical Security, NATO document AC/35-D/2001-REV3 (Brussels: North Atlantic Treaty Organization).

²³² US DHS (2011), *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings: FEMA-426/BIPS-06/* October 2011. Edition 2. Available at: <https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf> [accessed 13 May 2025].

National Practice: US Department of Energy Physical Protection Program – Physical Protection Baseline Requirements: Select Requirements for Testing Interior IDS (2021)²³³

The US Department of Energy guidelines are designed to establish baseline requirements for the physical protection of assets under the control of the US Department of Energy. The following are requirements for testing interior IDS:

- ▶ A perimeter intrusion detection and assessment system (PIDAS) must be capable of detecting an individual crossing the detection zone by walking, crawling, jumping, running, rolling, and/or climbing the fence at any point in the detection zone, with a detection probability of 90 per cent and confidence level of 95 per cent.
- ▶ The IDS must be performance tested when installed and annually (at least every 12 months) thereafter to validate that it meets detection probability and confidence level requirements.
- ▶ Any time the IDS falls below the required probability of detection, the IDS must be repaired and retested.
- ▶ When calculating detection probability for multiple sensor systems, detection is assumed if any of the sensors report an intrusion.
- ▶ Performance testing must be conducted to determine the proper settings for high detection rates with the lowest possible nuisance alarm report.
- ▶ Tests must be performed with a low-profile target (crawling) as well as higher velocity profile targets (walking, running, fast crawl, rolling).
- ▶ The tests must be conducted under the sort of weather and lighting conditions that are common to the local environment.

Source: US Department of Energy

²³³ US Department of Energy, Physical Protection Programme, DOE O 473.1A, Attachment 2: Physical Protection Baseline Requirements. Available at: <https://www.directives.doe.gov/directives-documents/400-series/0473.1-BOrder-a/@images/file> [accessed 13 May 2025].

6.5 Lighting



Lighting at a CI facility (both interior and exterior) is a core component of effective physical security. The use of lighting for security purposes is summarized in the 2008 OSCE *Handbook of Best Practices on Conventional Ammunition*:

“Security lighting aids the detection and assessment of threats, and the security response to the threat. It may also serve as a deterrent to intruders/hostiles. Security lighting increases the effectiveness of guards and CCTV by increasing the visual range during periods of darkness, or by illuminating an area where natural light is insufficient. Exterior security lighting is typically located along exterior perimeters and entry points to an installation.”²³⁴

Specific lighting requirements will be different for each CI facility based on need and the assessed threats it faces. In some cases, international or national standards offer valuable guidance, such as ISO 8995-1:2002 on the Lighting of Workplaces, or the US Department of Defense Unified Facilities Criteria on Interior and Exterior Lighting Systems (UFC 3-530-01 (C4-2019)).²³⁵ Lighting systems should not be designed independently from other aspects of a CI facility's security system. For example, the US DHS emphasizes that lighting systems should be designed to support the operation of video surveillance systems, or guard posts, which typically require higher levels of lighting.²³⁶

²³⁴ OSCE (2008), *OSCE Handbook of Best Practices on Conventional Ammunition* (Vienna: OSCE). Available at: <https://www.osce.org/files/f/documents/5/5/33371.pdf> [accessed 13 May 2025].

²³⁵ US Department of Defense (2023), *Unified Facilities Criteria (UFC): Interior and Exterior Lighting Systems*. Available at: https://www.wbdg.org/FFC/DOD/UFC/ufc_3_530_01_2023_c1.pdf [accessed 13 May 2025].

²³⁶ US DHS (2011), *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings. FEMA-426/BIPS-06/ October 2011. Edition 2*. Available at: <https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf> [accessed 13 May 2025].

Considering different lighting strategies for specific parts of a CI facility is seen as a good practice. The Illuminating Engineering Society, in its 2016 *Guide for Security Lighting for People, Property, and Critical Infrastructure*, states: “When planning or evaluating security lighting, designers will find it useful to divide the facility into zones such as perimeter, pedestrian, building, vehicle, storage, equipment, and restricted areas. During the planning process, designers may title and plan for various other zones for evaluation of specific security lighting, as the project requires. Each zone may require consideration of a different set of vulnerability and response factors.”²³⁷

Lighting strategies must also include protection measures against malicious activities, such as tampering with or damaging lights. Security managers may mount lights high and out of reach of potential attackers, and ensure that lights are protected through vandal-resistant materials such as wire mesh or metal/plastic casing.

Finally, ensuring standby power supplies for the most essential security lighting systems at a CI facility is considered good practice, with the control panel for such systems placed in a secure area with controlled access.

Types of Security Lighting

As stated above, lighting requirements will be different for each CI facility based on need and the assessed threats it faces. Security lighting comes in multiple different forms, as summarized by the US DHS below:²³⁸

Continuous lighting	Continuous lighting is the most common security lighting system. It consists of a series of fixed lights arranged to flood a given area continuously during darkness with overlapping cones of light.
Standby lighting	Standby lighting has a layout similar to continuous lighting; however, the lights are not continuously lit, but are either automatically or manually turned on when suspicious activity is detected or suspected by security personnel or alarm systems.
Movable lighting	Movable lighting consists of manually operated, movable searchlights that may be lit during hours of darkness or as needed. The system is normally used to supplement continuous or standby lighting. Movable lighting is also used to assist in vehicle inspection in temporary and permanent vehicle inspection areas.
Emergency lighting	Emergency lighting is a backup power system of lighting that may duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies that render the normal system inoperative. It depends on an alternative power source, such as installed or portable generators or batteries. Emergency backup power for security lighting should be considered.

²³⁷ Illuminating Engineering Society (2016), *Guide for Security Lighting for People, Property, and Critical Infrastructure*. Available at: https://cdn.fedweb.org/fed-96/2/IES%2520Security%2520Lighting%2520G-1_web.pdf [accessed 13 May 2025].

²³⁸ US DHS (2011), *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings: FEMA-426/BIPS-06/* October 2011. Edition 2. Available at: <https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf> [accessed 13 May 2025].

6.6 Video Surveillance Systems

Part of an IDS is a video surveillance system (VSS), which is typically strategically placed throughout a CI facility to monitor activity for suspicious behaviour and other considerations. The European Data Protection Supervisor defines video surveillance as “monitoring of a specific area, event, activity, or person by means of an electronic device or system for visual monitoring”.²³⁹ The Association of Banks in Singapore describes a VSS as “an integral part of security monitoring as it provides information for investigative work when the need arises. The CCTV surveillance system can also deter threat actors if they perceive that their actions are being monitored and recorded.”²⁴⁰ A VSS should comply with local laws on data collection, storage and protection, and be necessary and proportionate (see Chapter 3, Human Rights Considerations). Similar to other parts of this *Technical Guide*, in some cases, international or national standards offer valuable guidance, for example European Norm 50132-1 “Alarm systems – CCTV surveillance systems for use in security applications – Part 1: System requirements”.

When used properly, VSS are a valuable aid to security personnel in verifying incidents and activating both interior and exterior IDS. However, the effectiveness of a VSS depends on the types of cameras used and their installation, as well as the process for monitoring VSS feeds.



²³⁹ European Data Protection Supervisor (no date), Video-surveillance [webpage]. Available at: https://www.edps.europa.eu/data-protection/data-protection/glossary/v_en#video_surveillance [accessed 30 November 2024].

²⁴⁰ Association of Banks in Singapore (2018), *Physical Security Guidelines for Financial Institutions*. Available at: <https://abs.org.sg/docs/library/abs-scps-guidelines.pdf> [accessed 13 May 2025].

Camera Deployment Locations

A VSS involves a series of cameras strategically placed to provide surveillance capabilities for an intended location. They can be deployed at access points to a CI facility, perimeter points, areas of critical business operations, and/or areas containing high-value or critical assets. The proper placement of cameras should be based on a pre-defined function.

National Practice: Example Functions for Video Surveillance from the UK NPSA²⁴¹

- ▶ Deter an attempted intrusion by causing an adversary to reconsider the site due to enhanced probability of detection;
- ▶ Detect an attempted intrusion to the site using video analytics;
- ▶ Verify and further investigate an alarm event from a perimeter IDS;
- ▶ Tracking of an intruder when they have breached the perimeter;
- ▶ Recording of digital image evidence suitable for use in an investigation or court proceedings;
- ▶ Overlooking access control areas.

Source: UK NPSA

National Practice: Categories for Fields of View from the Video Surveillance System Standard for Buildings from the Singapore Police Force (2022)²⁴²

Field of View Category	Description
Detect	A figure occupies at least 10% of the available screen height and the scene portrayed is not unduly cluttered. Following an alert an observer can, after a search, ascertain with a high degree of certainty whether or not a person is visible in the pictures displayed to him (or more than 40mm per pixel).
Observe	A figure should occupy between 25% and 30% of the screen height. At this scale, some characteristic details of the individual, such as distinctive clothing, can be seen, whilst the view remains sufficiently wide to allow some activity surrounding an incident to be monitored (or more than 16mm per pixel)
Recognize	When the figure occupies at least 50% of screen height, viewers can say with a high degree of certainty whether or not an individual shown is the same as someone they have seen before (or more than 8mm per pixel). ²⁴³
Identify	With the figure now occupying at least 120% of screen height, picture quality and detail should be sufficient to enable the identity of an individual to be established beyond reasonable doubt (or more than 4mm per pixel).

Source: Singapore Police Force

241 NPSA (no date), CCTV. Overview [webpage]. Available at: <https://www.npsa.gov.uk/cctv> [accessed 30 November 2024].

242 Singapore Police Force (2022), *Video Surveillance System Standard (VSS) for Buildings, Version 2.0*. Available at: <https://www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security> [accessed 13 May 2025].

243 The Singapore Police Force makes the additional comment: "It should be noted at this point that when these guidelines were first developed, the systems all made use of the common fully analogue [Phase Alternate Line] system with a fixed resolution of 576 lines for video capture and display. Since the influx of digital systems to the [Video Surveillance System] market, we have more options to capture, recording and display in higher resolutions. So a 'Recognise' requirement can no longer be simply equated to a 50% screen height. For instance, through the use of megapixel cameras and high-resolution displays, it is now possible to provide the same image resolution as before using a much smaller physical percentage of the screen."

Types of Cameras

A VSS is made up of a series of cameras placed at strategic locations to serve a pre-defined desired function. Based on the function, different cameras can be used. For example, cameras can be fixed (immobile) or flexible (capable of being pointed in different directions). Cameras can have zoom functions, which provide close-up or wide-angle views, and can integrate additional technologies allowing, for example, license plates and other information to be recorded. As part of a comprehensive security system, it is vital to consider synergies between lighting, camera placement and camera selection.

Monitoring Video Surveillance Systems

In addition to cameras, another core component of a VSS is its monitoring capability. Unless a camera feed is being monitored by security personnel, it is possible that pre-attack hostile surveillance or criminal activity may go undetected, or the response to an incident is delayed.

VSS monitoring capabilities are typically housed within a control room at a CI facility that is staffed by security personnel trained for a range of incidents, including armed intrusions, bomb threats, explosive incidents and others. This training should be accompanied by written policies that support these actors in times of emergencies and allow them to alert all necessary stakeholders on- and off-site, including local law enforcement and first responders.

National Practice: Video Surveillance System Standard for Buildings from the Singapore Police Force (2022)²⁴⁴

- ▶ The VSS live images (video feed) should be monitored by operators in the Security Control Room, Fire Command Centre or other locations (VSS viewing facilities) in the building.
- ▶ Within the VSS viewing facility, the operator should be able to select any camera picture for display on any monitor at any time or to set up a scanning sequence with the desired dwell time.
- ▶ The camera selection control system should allow rapid selection of any camera views using minimum manual effort and be consistent across the VSS network.
- ▶ In event of any incident, each monitor within the VSS viewing facility should be able to view any of the cameras within the building's VSS. The system should allow multi-view display on VSS monitors.
- ▶ Any one user selecting a live image (feed) should not preclude other users selecting that live image (feed), or any other live images (feed) on the same system.
- ▶ All camera pictures displayed on monitors should include a single superimposition showing the camera identification codes, date and time.
- ▶ To facilitate general surveillance of building's safety and security and incident management, the labelling and numbering of cameras, and the associated recording sequence should be carefully planned to facilitate the rapid retrieval of recorded images.

Source: Singapore Police Force

²⁴⁴ Singapore Police Force (2022), *Video Surveillance System Standard (VSS) for Buildings, Version 2.0*. Available at: <https://www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security> [accessed 13 May 2025].

Monitoring VSS involves recording data, including data on facility personnel and visitors. The collection, retention, use and disclosure of VSS recordings should therefore be carried out in accordance with the relevant national data protection laws and policies.

Video Recording and Retention

Monitoring video surveillance feeds is important for immediate reaction, whereas video surveillance recording and retention supports investigative and other law enforcement actions. It is important to be able to retain video surveillance footage for security purposes. This should be compliant with national laws and procedures, including on data protection and privacy (for more information, see Chapter 3, Human Rights Considerations). All cameras that are part of a VSS should have the capability to record and retain images for a period specified in national laws and procedures. There is no established global standard for how long VSS footage should be retained; this relies heavily on the national context. For example, the UK NPSA recommends retention for 30 days,^{245, 246} whereas the Singapore Police Force recommends 31 days or more.²⁴⁷

6.7 Perimeter Security

Identifying and maintaining a secure perimeter around a CI facility is essential to its effective protection. It represents the outermost line of defence of a site's security system. It serves to control access for vehicles and people, delay unauthorized intrusion, and deter potential attackers. Perimeters may be comprised of fences, barriers (natural or human made), dense vegetation, or other installations.

²⁴⁵ Centre for the Protection of National Infrastructure (2020), *Storage and retention of recorded CCTV Images. Version 2.0*. Available at: <https://www.npsa.gov.uk/resources/storage-and-retention-recorded-cctv-images-2020> [accessed 13 May 2025].

²⁴⁶ HM Prison and Probation Service (no date), *Retention of CCTV Footage* [webpage]. Available at: <https://assets.publishing.service.gov.uk/media/619b92788fa8f503780c1b5f/annex-f-at-compliant-version-retention-cctv-footage.pdf> [accessed 13 May 2025].

²⁴⁷ Singapore Police Force (2022), *Video Surveillance System Standard (VSS) for Buildings, Version 2.0*. Available at: <https://www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security> [accessed 13 May 2025].

National Practice: Functions for a Properly Designed Perimeter from the UK NPSA (2011)²⁴⁸

A properly designed and implemented perimeter should:

- ▶ Help deter potential attacks;
- ▶ Facilitate authorized access to the site for both pedestrians and vehicles through intended access points;
- ▶ Deny unauthorized access through intended access points;
- ▶ Provide an enforceable stand-off to reduce the effectiveness of threats located at the perimeter, such as vehicle-borne improvised explosive devices;
- ▶ Assist in delaying, detecting and denying unauthorized attempts to breach site security;
- ▶ Provide appropriate facilities to enable security officers to carry out their duties, including protection in case of an attack;
- ▶ Help minimize the risk of collateral damage to people, facilities and infrastructure;
- ▶ Work effectively with other security measures in and around the site.

Source: UK NPSA

If hostile vehicle threats to a CI facility are deemed probable as part of its risk assessment, then consideration should be given to installing certified anti-ram fences around the perimeter. It is important to note that the cost of crash-rated hostile vehicle mitigation systems is much higher than normal fencing systems (for more information, see Chapter 7, Security Planning and Target Hardening).

Fencing and Barriers

A perimeter fence or barrier, while essential, can only delay a determined intruder for a period of time. The *OSCE Handbook of Best Practice on Conventional Ammunition* states that “fences (both with and without enhancements) offer delays of less than 1 minute against low level threats to as little as 3 to 8 seconds against highly trained intruders.”²⁴⁹



²⁴⁸ NPSA (2021): Building and Infrastructure [webpage]. Available at: <https://www.npsa.gov.uk/building-infrastructure> [accessed 30 November 2024].

²⁴⁹ OSCE (2008), *OSCE Handbook of Best Practices on Conventional Ammunition*. Available at: <https://www.osce.org/fsc/33371> [accessed 13 May 2025].

In most cases, a CI facility's perimeter will include security fencing designed to separate protected space from non-protected space. Such fencing may include metal chain link, mesh panels or other types of fencing, and can be topped with barbed wire or other physical deterrent measures. It is important that non-essential structures such as light posts or telephone poles, should be kept away from security fences since these may serve as climbing aids for a malicious intruder. Ideally, the bottom of a fence should be fixed below ground level. An IDS can also be integrated into security fencing, as for example, an alarm being activated if the fence is tampered with.

Barriers may also be used instead of security fencing for particular applications in line with a facility's needs and its environment. Barriers may consist of earthen mounds, poured concrete, or other human-made materials such as steel.

Where UAS threats are identified as relevant, the use of anti-UAS nets or fences as part of a building or perimeter structure should be considered.²⁵⁰ Counter-UAS technologies may also be considered in such cases.

Perimeter Gates

The security of a CI facility's gate(s) has a significant impact on the overall security of its perimeter, since gates are generally considered to be a perimeter's weakest point in terms of unauthorized access. Gates should be constructed to the same security standard as the perimeter itself, and they should have a form of access control in place.

As a general principle, the number of gates in a CI facility's perimeter should be kept to a minimum to reduce the resources required to patrol and monitor them. This is particularly relevant for parts of a perimeter located far away from the main access point where a permanent security team presence may be located.

It is important to monitor both the perimeter and its gates at all times by VSS in order to detect malicious activity.

6.8 Access Control Systems

Given that a key component of physical security is to prevent unauthorized access to a facility, CI owners/operators employ a range of access control measures. These can be located externally (at the perimeter of a facility) and internally (to ensure that only authorized individuals can access certain parts of the facility). They can include electronic access systems with specific procedures for sensitive parts of the facility. Importantly, all access control systems should comply with relevant health and safety regulations, including fire, to ensure the safety of CI facility personnel.

²⁵⁰ For further reading, see: European Commission Joint Research Centre (2023), Protection against Unmanned Aircraft Systems: Handbook on UAS Risk Assessment & Principles for Physical Hardening of Buildings and Sites. Available at: <https://publications.jrc.ec.europa.eu/repository/handle/JRC132967> [accessed 13 May 2025].

National Practice: Kazakhstan's Security Instructions for Critical Infrastructure Owners/Operators (1999/2023)²⁵¹

Based on Kazakhstan's 1999 Law on Countering Terrorism,²⁵² individual ministries have released instructions for the counter-terrorism protection of strategic sites under their purview. In 2023, the Minister of Industry and Infrastructure Development issued Order No. 508 targeting drinking water supply facilities. The instructions are divided into various thematic categories and chapters, including:

- ▶ Access control;
- ▶ Prevention and educational activities;
- ▶ Engineering and technical equipment (i.e., gates, fences, video-surveillance systems, checkpoints, vehicle inspection);
- ▶ Items and substances prohibited from being brought into the concerned facilities;
- ▶ Documents to be kept by facilities' managers (i.e., security plans, job descriptions for employees of the security unit);
- ▶ Training curricula on security matters relating to counter-terrorism;
- ▶ Checklists of actions in relation to different threat scenarios (i.e., discovery of suspicious objects, threat of hostage-taking, receipt of anonymous messages about an explosive device).

Source: Government of Kazakhstan

External Access Control

External access control measures around the perimeter of a facility are used to prevent access by unauthorized individuals, and to facilitate access for accredited personnel and authorized visitors. They also prevent IEDs or other harmful material and devices being carried into the facility by potential aggressors. Incoming packages and personal belongings can be controlled and checked at the entrance of a CI facility (i.e., by using X-ray machines). The level of external access control required for a given CI facility will vary depending on the facility's threat environment and risk assessment. However, consideration should be given to the development of standard external access control measures during periods of normal operation, such as those shown in the graphic below, and enhanced measures for periods of enhanced threat (for more information on this, see Chapter 10, Enhanced Threat Escalation Options).

²⁵¹ Ob utverzhenii instrukcii po organizacii antiterroristicheskoy zashity ob"ektov pit'evogo vodosnabzheniya naselennykh punktov, ujazvimykh v terroristicheskoy otnoshenii (20 July 2023, Kazakhstan). Available at: <https://adilet.zan.kz/rus/docs/V2300033119> [accessed 29 November 2024] unofficial translation.

²⁵² Zakon Respubliki Kazahstan ot 13 iul'ya 1999 goda № 416-І O protivodejstvii terrorizmu (13 July 1999, Kazakhstan). Available at: https://online.zakon.kz/Document/?doc_id=1013957&pos=3;-106#pos=3;-106 [accessed 29 November 2024] unofficial translation.

In most external access control set-ups, access is granted by security personnel on-site through a centralized control room or an automated process. External access control points may be equipped with video surveillance, metal detectors, security scanners and/or communication facilities based on the CI facility's assessed needs (see graphic below).



In more critical or secure premises, it may be necessary to use more than one form of access control. For example, the Singapore Association of Banks recommends a range of two-factor authentication access control systems to be used for this purpose.²⁵³ One related good practice is to create security level zoning with role-based access privileges. An example of security level zoning from Singapore is as follows:²⁵⁴

Accessibility Control	Area	Who Can Access
None	Public areas	All employees and the public
Limited	Visitor areas	All employees and visitors with names pre-registered with the security office
Moderate	Employee common areas/offices, etc.	All employees
High	Restricted areas	Authorized employees

Another good practice is to require advanced notification of a planned visit to a CI facility, with the number of days required to process visitors clearly communicated to relevant personnel. This allows for visitors to be verified in advance, including by providing photographic identification prior to and upon arrival. This also expedites the entry process and reduces the threat of attacks on visitors waiting for entry outside a CI facility's perimeter.

²⁵³ Association of Banks in Singapore (2018), *Physical Security Guidelines for Financial Institutions*. Available at: <https://abs.org.sg/docs/library/abs-scps-guidelines.pdf> [accessed 13 May 2025].

²⁵⁴ Association of Banks in Singapore (2018), *Physical Security Guidelines for Financial Institutions*. Available at: <https://abs.org.sg/docs/library/abs-scps-guidelines.pdf> [accessed 13 May 2025].

Internal Access Control

Once a person has gained access to a CI site, internal access controls are used to ensure that only authorized individuals gain access to different areas of the site. A NATO directive on physical security expands on this:

“Access control may be exercised internally over a site, a facility within the site, and zones or rooms within a facility. The control mechanism may be electronic, electro-mechanical, or physical. It may also be controlled by a guard or a receptionist. A pass or personal recognition system governing the regular staff can control entry into secure or restricted areas. In cases where a pass recognition system is in place within the establishment, security passes should be worn visibly at all times, in order to permit recognition, identification, and challenge if a member of staff is unsure of a person’s authority to be there.”²⁵⁵



All internal access points should be designed with a level of security that corresponds to the sensitivity of the area. As with exterior entry points, internal access points should be complemented with other measures such as lighting, video surveillance and door access control hardware, including secure locking mechanisms.

Automated Electronic Access Control Systems

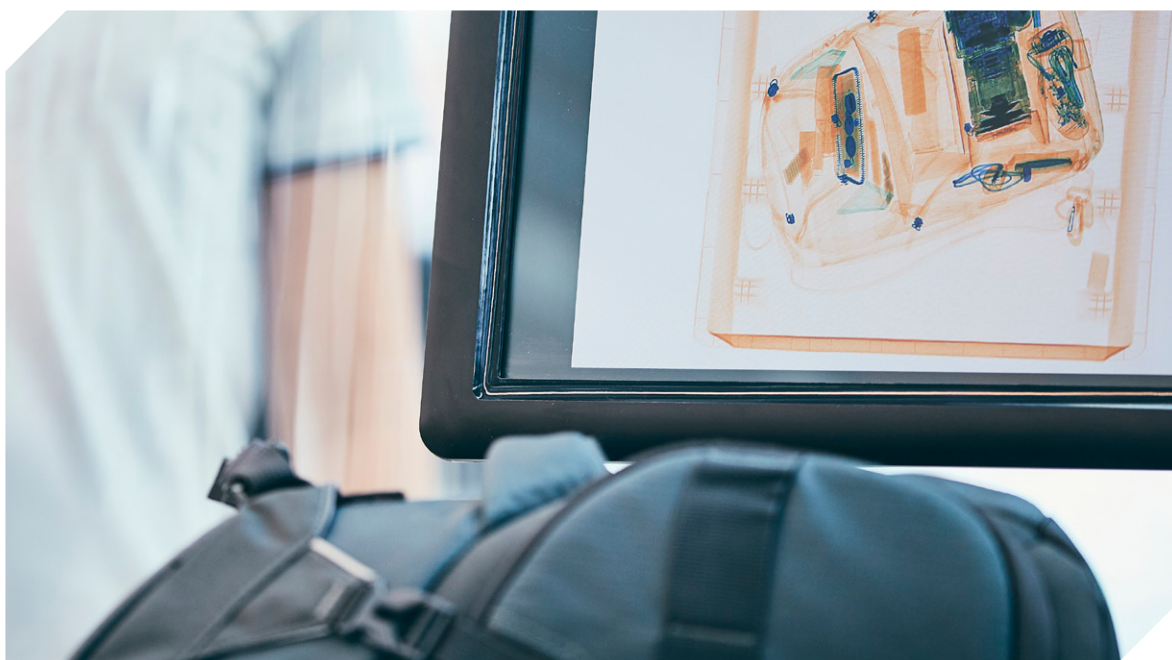
Electronic access controls systems are used to ensure that only authorized individuals enter or exit a controlled area. They function by way of an automated system. In such cases, authorized individuals are accredited and provided with a code, badge or other form of device that holds authenticating information and is recognized by the automated system. In the case of biometric access control systems, authorized individuals provide the necessary biometric information in order to obtain access. The US DHS identifies at least three categories of automated access control, shown in following table:²⁵⁶

²⁵⁵ Criscuolo, M. (2020), Directive on Physical Security. NATO document AC/35-D/2001-REV3 (Brussels: NATO).

²⁵⁶ US DHS (2011), *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings: FEMA-426/BIPS-06/* October 2011. Edition 2. Available at: <https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf> [accessed 13 May 2025].

Automated Access Control Category	Description
Coded devices	Coded devices require a person to enter a code (something they know) to be admitted by an entry control device. Individual codes are usually required for control of entry to more critical areas. Coded devices verify the authenticity of the entered code; electronically coded devices include electronic and computer-controlled keypads.
Credential devices	Credential devices identify a person using a credential (i.e., plastic card or key) (something they have) that contains a pre-recorded code authorizing entry into a controlled area. These devices only authenticate the credential assuming the user of the credential is authorized to enter. The most commonly used credential access cards include magnetic stripe cards, proximity cards, smart cards and implant chips.
Biometric devices	Biometric devices are based on the measurement of one or more physical or personal characteristics of an individual (something they are or do). Devices recognizing characteristics such as fingerprints, hand geometry, voiceprints, handwriting, and retinal blood vessel patterns have been used for entry control. The most common biometric devices are fingerprint verification devices, retinal pattern verification, hand geometry devices, and facial recognition devices.

6.9 Security Screening



Rigorous security screening measures of goods and people are critical at the point of entry to a CI facility. Unauthorized individuals may seek to access a facility overtly by misusing legitimate visitor procedures (including to covertly bring in a weapon or explosive devices), or they may wish to target a facility covertly, such as by having an explosive device delivered via the postal service.

Security Screening for Personnel and Packages

A 2020 European Commission Report on building perimeter protection emphasized the importance of screening both individuals and packages before they enter a facility, due to the risk of an individual being in possession of a firearm or an explosive device.²⁵⁷ For critical facilities, the Report recommends the use of full-body scanners to detect metallic or non-metallic objects hidden on a person, or the use of walk-through and hand-held metal detectors. X-ray machines can be used to screen packages, allowing security personnel to visually examine their contents using imaging software, while explosive detectors may be used as a supplementary tool to improve overall effectiveness.

If feasible, setting up a mailroom or package screening room off-site is considered good practice. This can reduce CI facility disruption in the event a suspicious package is identified. If this is not feasible and a mailroom/package screening room is located on the CI site, ensuring that the air circulation of this room is independent from the rest of the CI facility/site will help reduce disruption in the event an unidentified powder or substance is delivered.

Security Screening for Visitors

Visitor access for CI facilities may be controlled using badging, electronic turnstiles or other means. Visitor access points should be located near security personnel, giving them good visibility of attempts to circumvent turnstiles or other measures in place.

Although procedures for the control of visitors at a CI facility may vary depending on local security requirements – i.e., visitors can be either escorted or unescorted – an appropriate level of control over visitors must be maintained. In every case, the following minimum requirements should apply to escorted and unescorted visitors:

- ▶ *Escorted visitors* should be accompanied at all times by personnel with the appropriate level of authorized access. They should be required to wear a pass that identifies them as a visitor and should not be left alone while in the premises.
- ▶ *Unescorted visitors* may be provided with temporary, unaccompanied authorization to enter a CI facility or parts of it. However, unescorted visitors should still be required to wear a pass that identifies them as a visitor and to return their pass as soon as their business within the facility is completed.

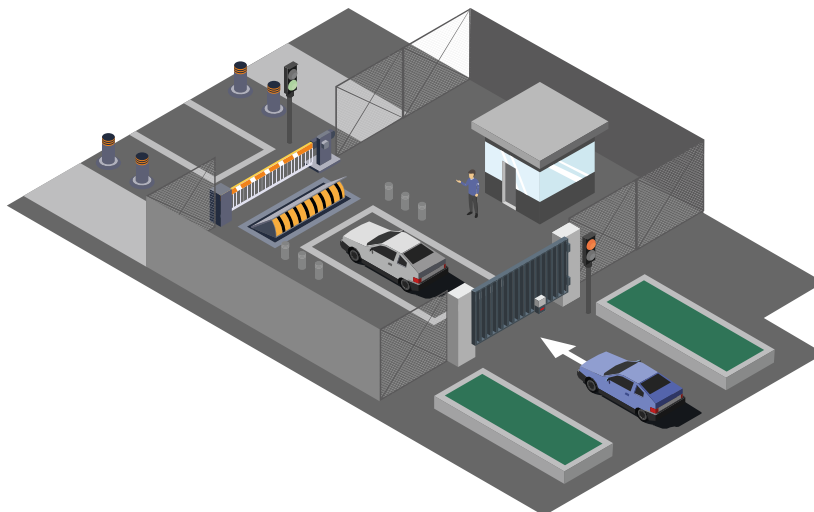
For both escorted and unescorted visitors, it is considered good practice for security personnel to record entry and exit times, photograph the visitors, and retain this information for a defined period of time in line with local data protection laws and regulations.

As part of enhancing CI facility personnel's security awareness, a challenge culture should be encouraged among personnel so that any visitor on the CI site who is not displaying their pass can be challenged as to why they do not have their pass on display.

²⁵⁷ Vasilis, K.; Larcher, M. (2020), *Guideline, building perimeter protection: Design recommendations for enhanced security against terrorist attacks*, Publications Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en> [accessed 13 May 2025].

Security Screening for Vehicles

Vehicle security screening points allow security personnel to verify and authorize vehicular access to a CI site, reducing scope for the unauthorized access of threat actors and their weapons. From the entry control point, personnel can control the approach and direction of vehicles, accommodate queuing (which should include a rejection lane), and support the duties of other security personnel.



One effective technique for securely managing vehicular access to a CI site is the use of “Sally Ports” or “Tiger Traps” (see graphic above). These are normally employed in high-risk environments and consist of an enclosure with two electrically operated barriers, only one of which is allowed to open at any one time. The first barrier only opens after authorized entry is approved and closed after the vehicle enters. The second barrier is opened after an inspection by competent security personnel is completed, and closed after the vehicle exits. This ensures that a following vehicle cannot “tailgate” the lead vehicle and obtain entry without screening.

6.10 Restricted Areas

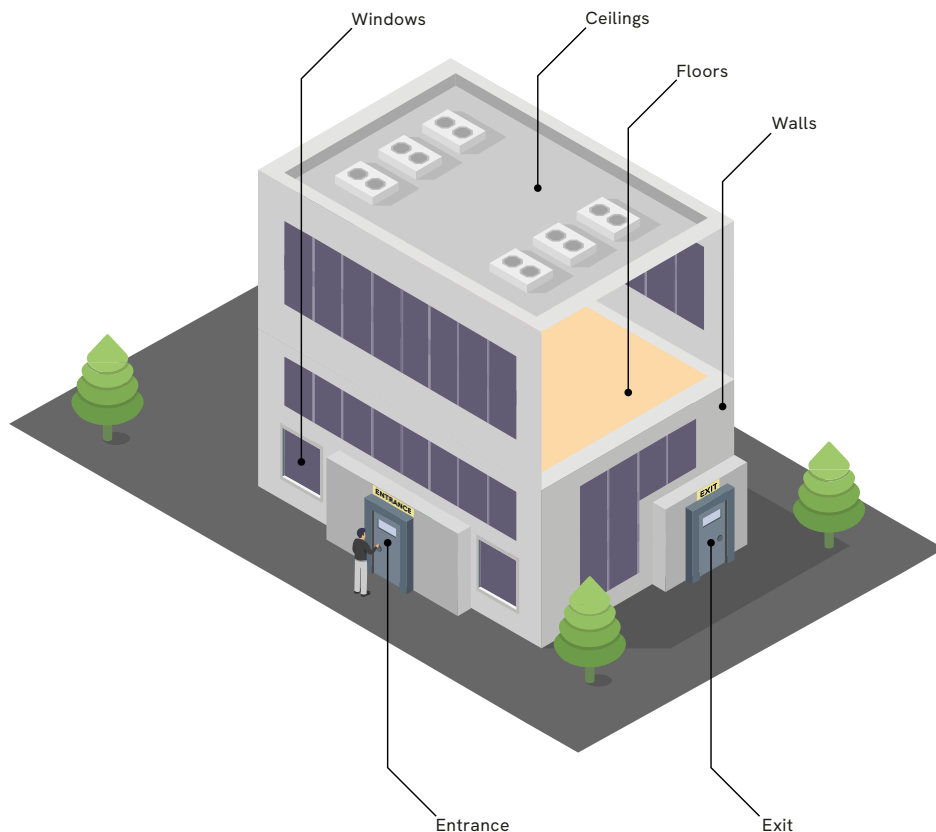
In addition to a CI site’s general perimeter security and access controls, any given CI site likely also includes areas of enhanced restriction, where access is further limited to authorized personnel only. Restricted areas are normally used to secure or safeguard high value assets or material, or house VSS controls or other security measures. However, they can be any space designated by CI owners/operators. Such areas require additional protection, since they may be targeted by terrorists should they overcome a CI site’s perimeter and other layers of defence. Additional protective measures include but are not limited to:

- ▶ limiting the number of entrances and exits to the minimum necessary;
- ▶ minimizing the number of doors, since doors are generally weaker than the building structure, thus making them less attack resistant;
- ▶ prohibiting access for all external vehicles and using a dedicated fleet of vehicles;
- ▶ installing outward opening doors, since they are more robust and secure from an external attack.

Warning signs displaying “Restricted Area” or a related message should also be posted at the boundary of each restricted area so they can be easily read by people approaching on foot or in a vehicle.

6.11 Building Structure

At a CI facility, building structure and integrity are fundamental to the facility’s physical security from a range of threats and hazards, including terrorist attacks. This is relevant in terms of both design decisions and construction materials to ensure there are no exploitable vulnerabilities.



Entrances and Exits

Doors are essential elements in the physical security of an asset. As outlined by the United Kingdom’s NPSA, doors provide a number of key functions, including:

- ▶ Controlling authorized access and preventing unauthorized access;
- ▶ Aiding the flow of people by avoiding the creation of an access choke point;
- ▶ Providing protection from blast or ballistic threats (if using enhanced protective security doors);
- ▶ Protecting from fire and/or smoke ingress;
- ▶ Creating a barrier that delays the progress of an adversary;
- ▶ Providing a means of escape in an emergency (i.e., during active shooter scenarios).²⁵⁸

258 NPSA (2021), Door Security. Available at: <https://www.npsa.gov.uk/door-security> [accessed 3 March 2024].

Doors that provide access outside the building should include secure locks, although they should easily open in the event of an evacuation. All doors and facades should be resistant to physical attacks. In special cases, bullet resistant glazing may be introduced to manage specific threats. Regardless of how the doors are secured, they should comply with relevant fire regulations.

The Singapore Ministry of Home Affairs has provided further guidance: “External doors should open outwards towards the direction of any possible threat. The frame can then support the door against forced entry or blast effects from the outside. However, in this case, the hinges require to be hardened against tampering as they will be located on the outside of the building. The frame and wall attachments should be hardened to the same level as the door.”²⁵⁹

Walls, Ceilings and Floors

Walls are physical barriers that segregate one area of a building from another (or the inside of a building from the outside). They play a major part in the overall physical security of the structure. The exterior of all buildings in a CI facility should be secured against unauthorized access, especially in cases where a surrounding perimeter/fence is absent, or in the event such a fence is breached. In the guidance of the US Department of Energy it is emphasized that perimeter walls, floors and ceilings “must be permanently constructed and attached to each other,” and that “all construction must be done in a manner that provides visual evidence of unauthorized penetration.”²⁶⁰

Substantial, reinforced walls help protect against explosions, small arms fire, forced entry and other security threats. CI owners/operators may also wish to consider installing a blast shielding wall or reinforcing glass facades and structures in certain parts of relevant buildings, depending on the threats they face.

Where it is possible to access a building by going over the top of a wall, an IDS may be installed to ensure that the area cannot be entered undetected.

Ceilings and floors should be constructed using materials that offer penetration resistance to delay unauthorized entry into the building and provide evidence of attempts at unauthorized entry (i.e., signs of force or damage to ceilings or floor construction).

²⁵⁹ Joint Operations Group – Ministry of Home Affairs (no date), *Guidelines for Enhancing Building Security in Singapore*. Available at: <https://www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security> [accessed 13 May 2025].

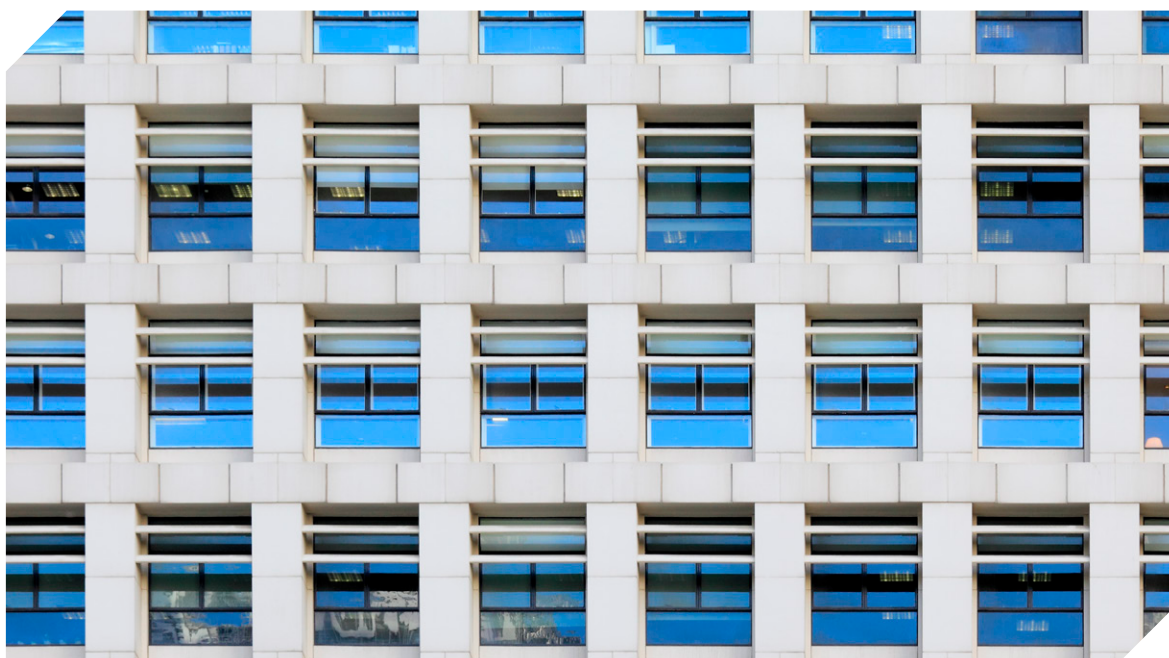
²⁶⁰ US Department of Energy (2021), Physical Protection Programme, DOE O 473.1A , Attachment 2: Physical Protection Baseline Requirements. Available at: <https://www.directives.doe.gov/directives-documents/400-series/0473.1-BOrder-a/@images/file> [accessed 13 May 2025].

Windows

Windows represent an easier opportunity for entering a facility than doors or walls, since they often do not have the same level of physical robustness. Thus windows need integrated security features:

- ▶ Windows should offer penetration resistance to, and evidence of, unauthorized entry.
- ▶ Window frames should be securely anchored in the walls, with windows locked from the inside or installed in fixed frames, meaning that window panes cannot be removed from the outside.
- ▶ Visual barriers should be used if visual access is a factor. For example, all windows that allow visual observation of classified activities should be made opaque or equipped with blinds, drapes or other coverings.

When assessing the security of a window against armed intrusion or explosive attacks, the entire window system (not only the glazing) should be assessed to ensure robustness.²⁶¹



Windows at ground level or other easily reachable windows should be constructed from materials that provide protection from forced entry. The level of protection for the windows should be in line with the strength of its adjoining walls, as well as the connection between windows and the wall, which needs to be able to resist the same force.

Windows: Glazing

In addition to facilitating entry for a malicious actor, windows also pose a safety hazard in the event of an explosive attack. According to the US Department of Defense, “[i]n past explosive events where there was no building collapse, a high number of injuries resulted from flying glass fragments and debris from walls, ceilings, and fixtures (non-structural features).”²⁶² According to the United Nations Department for Safety and

²⁶¹ UNDSS (no date), *Blast Protection for Windows*. Available at: https://www.unicef.org/jordan/media/5951/file/LRFP-2021-9166373-Annex_4-Blast_Protection_for_Windows.pdf [accessed 13 May 2025].

²⁶² US Department of Defense (2018), *Unified Facilities Criteria (UFC): DoD Minimum Antiterrorism Standards for*

Security (UNDSS), as many as 80 per cent of victims in large bombing attacks are killed or injured by glass fragmentation.²⁶³ When assessing window locations for susceptibility to explosive attacks, the UNDSS thus notes that less glazing results in a lower threat of projectiles in the event of an explosion.²⁶⁴ The testing of windows for blast resistance is addressed in the ISO 16933:2007 standard Glass in Building: Explosion-Resistant Security Glazing.²⁶⁵

There are several basic types of glazing that are commonly used in the design of protective window glazing systems: heat-strengthened glass, fully thermally tempered glass, and laminated glass. All have different levels of resistance to breakage by explosive events. They thus should be selected by CI owners/operators and competent authorities based on need and assessed risks.

LAMINATED GLASS



Effectiveness and considerations of laminated glass use against UAS-driven attack tactics. Used with permission of the European Commission's Joint Research Centre.²⁶⁶

Buildings, p. 18. Available at: https://www.wbdg.org/FFC/DOD/UFC/ARCHIVES/ufc_4_010_01_2018_c1.pdf [accessed 13 May 2025].

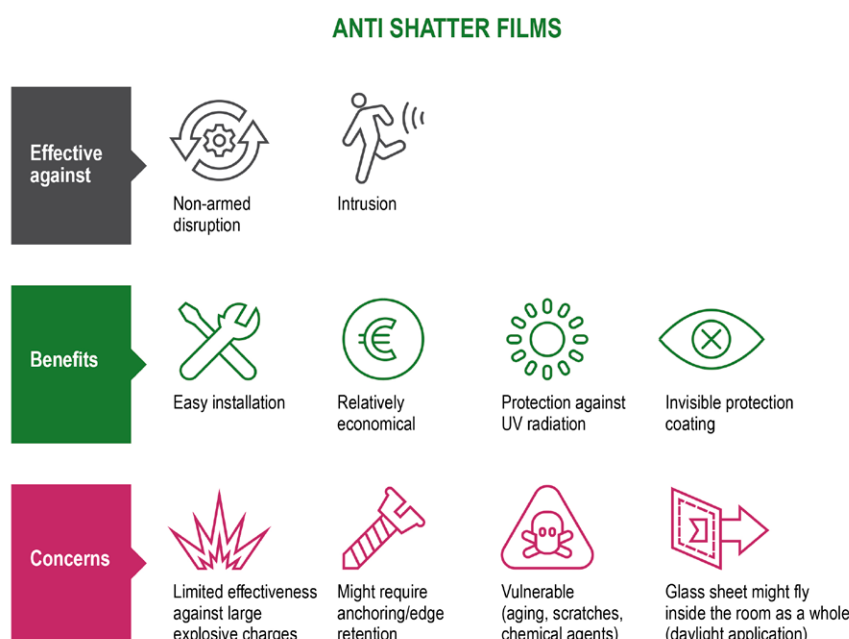
263 UNDSS (no date), *Blast Protection for Windows*. Available at: https://www.unicef.org/jordan/media/5951/file/LRFP-2021-9166373-Annex_4-Blast_Protection_for_Windows.pdf [accessed 13 May 2025].

264 UNDSS (no date), *Blast Protection for Windows*. Available at: https://www.unicef.org/jordan/media/5951/file/LRFP-2021-9166373-Annex_4-Blast_Protection_for_Windows.pdf [accessed 13 May 2025].

265 ISO (2007), *Glass in building — Explosion-resistant security glazing — Test and classification for arena air-blast loading* (ISO Standard No. 16933:2007). Available at: <https://www.iso.org/standard/38166.html> [accessed 16 May 2025]. For further reading on different types of glazing and window standards, see, e.g., European Reference Network for Critical Infrastructure Protection (2014), *A comparison of existing standards for testing blast resistant glazing and windows*. Available at: https://erncip-project.jrc.ec.europa.eu/sites/default/files/ReqNo_JRC94930_A%20comparison%20of%20existing%20standards%20for%20testing%20blast%20resistant%20glazing%20and%20windows.pdf [accessed 13 May 2025].

266 European Commission Joint Research Centre (2023), *Protection against Unmanned Aircraft Systems: Handbook on UAS Risk Assessment & Principles for Physical Hardening of Buildings and Sites*. Available at: <https://publications.jrc.ec.europa.eu/repository/handle/JRC132967> [accessed 13 May 2025].

Although annealed glass and heat-strengthened glass are the most frequently used materials for glazing, any glazing type can be covered with an anti-shatter film to reduce the risk of flying glass fragments and thus, to reduce risk of injury.



*Effectiveness and considerations of anti-shatter film use against UAS-driven attack tactics.
Used with permission of the European Commission's Joint Research Centre.²⁶⁷*

Windows: Bullet Resistant Glass

Conventional bullet resistant glass is made by laminating layers of glass with poly-vinyl butyrate. In some cases, bullets will be stopped by the glass but splinters of glass may be ejected. While not likely to cause serious injury, these can still cause eye or skin damage. Thus, thicker glass may be needed.

To identify products that achieve appropriate levels of resistance to bullets, European Standard (EN) 1522:2000 covers bullet resistant requirements and classification for windows, doors shutters and blinds.

Blast Curtains

For facilities deemed to be at a higher risk from terrorist attacks or for facility windows assessed as being more exposed to explosive events (such as windows facing a public street), additional measures to prevent shards of glass or other debris being expelled in the event of an explosion should be considered. One solution is the installation of blast curtains. According to the European Commission's Joint Research Centre, the main aim of such measures is "to catch the flying fragments that are produced from the failure of the windows as a result of a propagating blast wave and they are usually installed behind the building's façade".²⁶⁸ Although it is still possible for fragments to enter a

²⁶⁷ European Commission Joint Research Centre (2023), *Protection against Unmanned Aircraft Systems: Handbook on UAS Risk Assessment & Principles for Physical Hardening of Buildings and Sites*. Available at: <https://publications.jrc.ec.europa.eu/repository/handle/JRC132967> [accessed 13 May 2025].

²⁶⁸ Vasilis, K.; Larcher, M. (2020), *Guideline, building perimeter protection: Design recommendations for enhanced*

room's interior and cause injury, a blast curtain reduces the travel distance of airborne debris significantly.

Blast curtains can be produced using polyester materials or steel. Each material will behave differently during an explosive event and capture glass shards more or less effectively. Thus appropriate testing should be carried out and a material selected based on the assessed risk to the window in question. Blast curtains can be used as a stand-alone measure, or in conjunction with anti-shatter films or laminated protective glass solutions.²⁶⁹

Mailrooms



Mailrooms can represent a significant CI facility vulnerability if they are poorly located, poorly constructed or insufficiently designed to address potential threats from, for example, mail-borne IEDs. Considerations for the location of a mailroom should be made for newly constructed CI facilities, with preference given to mailrooms located near the perimeter of a CI facility to avoid mail-borne IEDs being transported through a CI facility on the way to processing in a mailroom.²⁷⁰ For existing CI facilities with fixed mailrooms not located near the building perimeter, arrangements should be made to ensure the room has an appropriate level of blast resistance and a separate ventilation system in the event of a chemical or biological attack. These points are reinforced and built upon in the following guidance from the Association of Banks in Singapore:

“If [mail]rooms are not properly designed and located, it can present a threat to the building and its occupants when mail is used as a means of chemical,

security against terrorist attacks, Publications Office of the European Union, p. 45. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en> [accessed 13 May 2025].

²⁶⁹ Vasilis, K.; Larcher, M. (2020), *Guideline, building perimeter protection: Design recommendations for enhanced security against terrorist attacks*, Publications Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en> [accessed 13 May 2025].

²⁷⁰ US Department of Defense (2018), *Unified Facilities Criteria (UFC): DoD Minimum Antiterrorism Standards for Buildings*, p. 27. Available at: https://www.wbdg.org/FFC/DOD/UFC/ARCHIVES/ufc_4_010_01_2018_c1.pdf [accessed 13 May 2025].

biological, radiological and explosive (CBRE) attacks. Ideally, mailrooms should be located near the entrance to the building or in a separate part of the building away from critical areas and key structural elements of the building. To prevent airborne threats, mailrooms should also have a dedicated/independent air handling unit or ventilation system, taking into consideration the design and cost elements. The area where incoming mail and parcels are being screened should be designed to mitigate blast effects.

“As mailrooms are high risk areas, the room should be built with adequate protection such as CCTV surveillance and door access control systems. In addition, access to the mailroom should be restricted to authorised personnel only. In some instances, critical infrastructure facilities may not have an in-house mailroom and may receive mail from third party service providers or couriers. These providers and couriers may be exposed to the same level of threat from incoming mail, and any relevant mailroom security training should be part of the pro-active security response to identify and detect such threats for escalation and response.”²⁷¹

Personnel processing mail at a CI facility should be trained in procedures for handling mail, including appropriate actions in the event a suspicious letter or parcel is received. This should include frequent training updates to ensure they are aware of current violent actor modus operandi. This may necessitate close co-operation and engagement with local and national law enforcement and other security services.

An organizational policy for the facility should also be in place to address various responses required both internally within the CI facility (including reporting to CI facility security teams), and externally (such as contact with law enforcement or bomb disposal units).

²⁷¹ Association of Banks in Singapore (2018), *Physical Security Guidelines for Financial Institutions*. Available at: <https://abs.org.sg/docs/library/abs-scps-guidelines.pdf> [accessed 13 May 2025].



Security Planning and Target Hardening

//

Mitigating the risk posed by different types of terrorist attack methods requires general physical security measures, such as those covered in previous chapters, as well as specific plans and steps. This chapter provides guidance on the latter.

//

7 Security Planning and Target Hardening

CI facilities face a range of threats from threat actors, including terrorists. Threat actors can be patient, flexible and, in some cases, well-resourced. Should they decide to target a CI facility, given the possibility for high impacts, they are likely to plan their attack carefully. To understand the threats posed by threat actors, a CI owner/operator should first seek to assess its threat environment and then the risk(s) to the facility in question (for more information, see Chapter 5, Terrorism Threat and Risk Assessment). This process will bring deeper insight into the vulnerabilities of CI assets, and also identify likely threat scenarios that can then be planned for. While many threat actors may share a similar intent (for example, to damage or degrade a CI facility), their capabilities will likely vary significantly. Some will be able to carry out complex and co-ordinated attacks using sophisticated weaponry, while others will only be able to undertake more simple attacks, such as using vehicles. Mitigating the risk posed by each type of attack requires general physical security measures, such as those covered in the previous chapter, as well as plans and specific steps for various types of attack in mind. This chapter provides guidance on the latter.

This chapter will first explore how terrorist organizations prepare for attacks, with a focus on hostile reconnaissance. It will then consider different types of terrorist attacks – including the use of hostile vehicles, explosives, CBRN materials, firearms and hostage-taking – and the steps that CI owners/operators can take to prepare their facilities accordingly. The chapter concludes with practices for the evacuation, invacuation and lockdown procedures needed in crisis situations. It will also emphasize the importance of implementing a business continuity management system and crisis communications framework.

7.1 Terrorist Attack Planning through Hostile Reconnaissance



While not an exact sequence, there are general stages through which a terrorist must advance in order for an attack to be successful. These stages include a range of planning and preparatory activities, particularly in instances where the target is well fortified (such as a CI facility) or a complex attack methodology will be used.²⁷² While there are multiple different conceptualizations of the terrorist attack planning cycle, they all generally address the following key tasks (not necessarily in this order):

- ▶ Sourcing the necessary materials and logistics (weaponry, funds, personnel, etc.);
- ▶ Identifying potential targets;
- ▶ Gathering information on potential targets to support attack planning and identify vulnerabilities for exploitation (both online and offline);
- ▶ Selecting the target;
- ▶ Determining the attack methodology;
- ▶ Executing the attack (including escape options, if not a suicide attack);
- ▶ Determining publicity and propaganda opportunities post-attack.

As shown, there are multiple pre-attack tasks for which a threat actor will require information specific to an intended target or targets. In such cases, they may find hostile reconnaissance desirable. Hostile reconnaissance generally encompasses the activities a threat actor undertakes to gain information as part of the preparatory phase of an attack on a defined target. Specific to an attack on a CI facility, the type of information a threat actor may wish to acquire through hostile reconnaissance can include, *inter alia*:

- ▶ Site-specific information (i.e., pedestrian and traffic patterns, entry and exit points acquired through photographs/videos, floorplans, security plans, evacuation plans);
- ▶ Security information (i.e., specific security measures in place, location of security personnel, entry procedures, patrol timings and procedures);
- ▶ Personnel or vehicle accreditation (i.e., via images on websites, social media);
- ▶ Corporate information (i.e., organizational charts, personnel contact details, office locations);
- ▶ Planning information (i.e., new building/development plans, security upgrades, etc.).

In the process of conducting hostile reconnaissance, a threat actor will seek to validate information they have already gathered on a potential target, identify and collect new information, eliminate targets from their list, and eventually settle on a final target. Hostile reconnaissance on a CI facility can be conducted in person or virtually. Virtual hostile reconnaissance may involve visiting a CI facility's website in order to identify information about its perimeter, physical security measures, or entry and accreditation process. It may also involve identifying critical services outside a CI facility's perimeter, such as electrical substations, powerlines and pipelines, which may be more vulnerable to attack than the CI facility itself.

²⁷² Smith, B. L.; Damphousse, K.R.; Paxton, R. (2006), *Pre-incident Indicators of Terrorist Incidents: The Identification of Behavioral, Geographic, and Temporal Patterns of Preparatory Conduct*, p. 7 (Washington, DC: National Institute of Justice, Department of Justice). Available at: <https://www.ncjrs.gov/pdffiles1/nij/grants/214217.pdf> [accessed 13 May 2025].

In-person hostile reconnaissance provides a threat actor a first-hand look at outward-facing security measures (i.e., guard posts and security patrols) or security counter-measures (i.e., identification card checks or bag checks), which may aid them in determining the feasibility of an attack on the target (or targets) in question.²⁷³

Hostile reconnaissance may involve a threat actor taking videos or photographs of a target facility, or jotting down notes. In some cases, a threat actor may inquire with CI facility personnel about the security measures in place at a facility, or even test security responses by leaving suspicious items unattended, attempting to bring prohibited items on site, or parking in prohibited areas. A threat actor may also carry out an attack rehearsal. This may include walking through entry and exit points, transporting items that serve as stand-ins for weapons or bombs, or rehearsing timings and event sequences. An attack rehearsal is more likely to be conducted for an attack on a soft target or public space. However, it is possible that a threat actor may wish to conduct rehearsal on a CI facility, even if only partially feasible (for example, rehearsing an attack up until the point of entry to a facility).

In the course of conducting hostile reconnaissance, threat actors may become vulnerable to detection by security services or CI owners/operators. For example, they may unintentionally disclose information about their potential intentions or target selection by searching for information online, visiting the intended target in person, or querying facility personnel. Therefore, it is vitally important that CI owners/operators raise awareness among facility personnel on hostile reconnaissance as a pre-attack phenomenon, and ensure that there are adequate frameworks in place to channel reports and information to the appropriate security focal points.

Detecting Hostile Reconnaissance and Suspicious Activities

Given that hostile reconnaissance is a key task that most threat actors, including terrorists, will undertake before conducting a terrorist attack, it is highly important to ensure that measures to detect such activities are in place at a CI facility. Hostile reconnaissance is rarely identified as such in the moment. It is more likely to be identified through multiple suspicious, unusual or out-of-place incidents taking place over a period of time. If analysed by competent security personnel, these may be determined to be part of a hostile reconnaissance campaign by a threat actor. Thus detecting suspicious activities is directly linked to the detection of hostile reconnaissance.

To detect suspicious activity which may constitute hostile reconnaissance, a CI owner/operator may consider adopting a targeted, multi-faceted programme that allows CI facility personnel to identify and report suspicious activities. In turn, competent security personnel can react as needed. In some cases, this may be part of a larger programme aimed at creating a security culture among CI facility personnel.

273 Pounder, D. (2018), "Perspective: Picking Target, Surveillance Begin the Hostile Events Attack Cycle", Homeland Security Today [webpage]. Available at : <https://www.hstoday.us/subject-matter-areas/counterterrorism/perspective-picking-target-surveillance-begins-the-hostile-events-attack-cycle> [accessed 10 December 2024].

Practice: International Civil Aviation Organization's Guidance on Developing a Security Culture (2022)²⁷⁴

"Security culture is an organizational culture that encourages optimal security performance. Security culture is commonly understood to be a set of norms, beliefs, values, attitudes and assumptions that are inherent in the daily operation of organizations and are reflected by the actions and behaviours of all entities and personnel within those organizations. Security culture cannot be considered in isolation from the organizational culture as a whole.

"In order to establish or improve security culture in organizations, measures should be developed to enhance such norms, beliefs, values, attitudes and assumptions. Those enhancements should aim at furthering the following principles:

1. continuously improve security, recognizing that a security culture in an organization is an essential component of an effective, proactive and reactive security regime, which supports and maintains a risk-resilient structure that helps to manage effectively both insider and external risks;
2. encouraging awareness of and alertness to security risks by all personnel and the role that they personally play in identifying, eliminating or reducing those risks;
3. encouraging familiarity with security issues, procedures and response mechanisms (i.e., whom to call or processes to report in case of suspicious activity);
4. recognizing the importance of security from all levels of an organization, including management, and reflecting that through the observation and participation in all security measures;
5. allowing the necessary time and making the necessary efforts to comply with security measures, even when under pressure;
6. promoting willingness to accept responsibility, to be pro-active and to make decisions autonomously in the event of security occurrences, which include incidents, deficiencies and breaches;
7. challenging other personnel in case of irregularities and accept being challenged (i.e., promote speaking up, acknowledge different perceptions);
8. immediately reporting occurrences or any suspicious activity that might be security-related – independent of who is doing it;
9. fostering critical thinking regarding aviation security and interest in identifying potential security vulnerabilities, deviation from applicable procedures, and solutions; and
10. handling sensitive aviation security information appropriately."

Source: ICAO

²⁷⁴ International Civil Aviation Organization (ICAO) (2022), ICAO Security Culture Guidance Material. Available at: <https://www.icao.int/Security/Security-Culture/Documents/ICAO%20-%20Security%20Culture%20Guidance%20Material.pdf> [accessed 13 May 2025].

Key considerations for a CI owner/operator programme focused on detecting hostile reconnaissance and suspicious activities are:

- ▶ Identifying suspicious activity;
- ▶ Reporting suspicious activity;
- ▶ Analysing information for patterns and other insights;
- ▶ Sharing information with appropriate stakeholders.

Identifying suspicious activity: CI facility personnel should be sufficiently trained to monitor their surroundings for suspicious activity and, when necessary, immediately report it to an appropriate security focal point. This may include training in behavioural detection, a method of detecting individuals with hostile intentions by observing their behaviour and activities.²⁷⁵ Raising the level of security awareness among CI facility personnel may involve providing threat briefings to the wider workforce and disseminating materials on threat actors and common modus operandi. Briefings are important in aiding personnel to recognize behaviour patterns and build a holistic view of the range of possible suspicious activities.

National Practice: Swiss Federal Office of Civil Aviation's Guidance on Developing Awareness-raising Campaigns to Enhance the Security Culture within the Civil Aviation Sector (2020)²⁷⁶

- ▶ "An awareness-raising campaign is one possible means of ensuring security culture or elements of it are known or borne in mind. For the campaign to be effective, it should be designed specifically, efficiently and in a targeted manner. The campaign must not only communicate threats and risks but also ensure that the persons addressed understand the contents and are motivated to implement the desired objectives.
- ▶ "The method of communication is also a relevant factor. Fear-inducing or intimidating communication is often counter-productive, since this is more likely to instill fear in those addressed rather than motivate them. Risks should ideally be presented using internal examples and the information should generally be simple and brief.
- ▶ "The campaign should be supported by suitable accompanying measures. Among other things these may include posters and flyers, e-mailings or special events such as themed or focus meetings.
- ▶ "It is also helpful if an emotional bond to the campaign is made. This can be supported by 'branding', for example. Integrating an impressive 'brand name' and/or a logo creates positive emotions, motivation and credibility."

Source: Switzerland's Federal Office of Civil Aviation

²⁷⁵ NPSA (27 February 2023), Behavioural Detection [webpage]. Available at: <https://www.npsa.gov.uk/behavioural-detection-0> [accessed 10 December 2024].

²⁷⁶ Swiss Federal Office of Civil Aviation (2020), *Security Culture: Guidance on the development and expansion of security culture and a possible awareness-raising campaign*. Available at: <https://www.icao.int/Security/Security-Culture/Documents/Switzerland%20FOCA%20-%20Guidance%20on%20development%20and%20expansion%20of%20SC%20and%20awareness%20raising.pdf> [accessed 13 May 2025].

In addition to raising the awareness of personnel, they should also be empowered to identify and report suspicious activity to an on-site security focal point. When reporting suspicious activities, personnel should be aware of key details that help follow-up activities, such as:

- ▶ What was abnormal/suspicious/unusual about the individual's/individuals' behaviour;
- ▶ Where the individual/individuals came from and went after the suspicious activity was identified;
- ▶ The number of people involved;
- ▶ A detailed description of the individual/individuals involved, i.e., gender, age, height, weight, hair cut/colour, scars, tattoos and ethnicity;
- ▶ A description of the clothing worn by the individual/individuals involved;
- ▶ A description of items carried by the individual/individuals (if relevant);
- ▶ A vehicle description (vehicle type, colour, distinguishing features, registration number, location) (if relevant);
- ▶ The individual's/individuals' reaction to questions (if relevant).

CI facility personnel (including security personnel) should be encouraged to approach unknown individuals on-site if their behaviour is considered unusual, politely asking them to explain their presence and ask open-ended questions such as "May I help you?" or "Who are you visiting today?" This demonstrates that facility personnel are not only adept at spotting new faces, but are also able to react to unusual activity. However, approaching unknown individuals should be done with caution, and only when there is no immediate or obvious threat. If the concerns of facility personnel are not resolved by this, they should follow procedures for reporting suspicious activity.

Importantly, all personnel should also be aware of local laws. For example, CI facility security personnel do not always have legal powers to seize a camera from a suspicious individual, prevent them from taking photographs, or to ask them to delete photographs.

Reporting suspicious activity: If CI facility personnel are unsatisfied after approaching an unknown individual on-site or near a facility, or they do not feel safe doing so, they should feel empowered by the CI owner/operator's management to report key details to a security focal point. Once reported, procedures should be in place for a security focal point to develop a report on the incident. The suspicious activity report should capture the key details listed above, and should be drafted by the security focal point as soon as possible to ensure these details are fresh and accurate.

An effective programme of this kind may also consider collating all suspicious activity reports (including any associated imagery and other information) in a single repository for later use. This allows for the creation of "institutional memory" (including lessons learned) and for further analysis. When personal data is involved, local and national laws as well as international standards should be followed. Further information on this can be found in Chapter 3, Human Rights Considerations.

Analysing information for patterns and other insights: A CI facility security focal point should have an overview of suspicious activities at the facility or involving the facility

over a defined period of time. This information should be routinely analysed to identify patterns in incidents of suspicious activity to determine the extent of suspicious activity at a given facility and to establish any links to a credible threat.

Sharing information with appropriate stakeholders: Information relating to suspicious activities should also be shared with appropriate security stakeholders. Determining who should have access to this information may be a decision for individual CI owners/operators, mandated by government regulators or defined in dedicated agreements between CI owners/operators and government stakeholders.

Measures to Respond to Hostile Reconnaissance and Suspicious Activities

In addition to developing and implementing a programme that supports the detection and reporting of hostile reconnaissance or suspicious activity, there are measures CI owners/operators can take to deter threat actors during hostile reconnaissance activities. One approach is to conduct security-minded communications. These seek to deter a threat actor during the hostile reconnaissance phase by convincing them that the facility is too well-fortified, too well-guarded or otherwise too difficult to attack.

In addition to security-minded communications, this objective can be furthered through effective and visible physical security and hardening measures (including those described in Chapter 6, Physical Security Measures, and this chapter. A CI owner/operator can deter threat actors by, for example, minimizing the amount of publicly available information about a given facility (including its security measures, organizational structure, and images of the facility and its surroundings online).

National Practice: UK NPSA's Security-Minded Communications Examples²⁷⁷

- ▶ "Ensure your website has a robust and up-to-date cookies policy and privacy statement so that a hostile will know that you record details about their use of your website, such as their IP address.
- ▶ "Ensure your website includes a dedicated safety and security page that highlights the range of security measures that are in place at your location (without giving away details that could be useful to a hostile). You should only promote the security measures that are actually in place.
- ▶ "Audit your communications and make sure you are not accidentally giving away information that might be useful to a hostile, like accurate maps/floor plans or exact visitor numbers or busy and quiet times.
- ▶ "Use social media, press releases and other communications to flag that security is in place at your site but do not reveal detail that would be beneficial to a hostile.
- ▶ "Think about imagery. Are you showing the location and type of CCTV installed at your site or inadvertently providing information about staff passes? If so, remove or edit the image."

Source: UK NPSA

²⁷⁷ NPSA (2024), *Security-Minded Communications. 5-Minute Read*. Available at: <https://www.npsa.gov.uk/resources/security-minded-communications-5-minute-read> [accessed 10 December 2024].

Another useful measure that CI owners/operators can employ to design a response to hostile reconnaissance or suspicious activity is to organize exercises during which internal teams simulate the role of threat actors seeking to test a facility's security posture. The results from these exercises can then be assessed, analysed and used to identify measures that would enhance a facility's security posture or make the response more efficient and effective.

7.2 Security Planning for Hostile Vehicle Attacks

A recurring and particularly damaging attack methodology used by terrorists targeting soft targets and public spaces is the ramming of large vehicles into targets at high speed to maximize human casualties and damage. Terrorists have also used vehicles to transport explosive devices closer to a site or facility. While this threat has historically been limited to attacks on soft targets, its potential threat to CI facilities – including, *inter alia*, as a way to overcome a facility's perimeter, or deliver an explosive device or group of armed attackers to an intended target – cannot be minimized.

National Practice: US CISA Questions for Assessing Vehicle Ramming Risks (2024)²⁷⁸

"The initial step in mitigation planning is performing a risk assessment specific to vehicle-to-pedestrian contact. This assessment helps critical infrastructure owners, operators, their personnel, and mass-gathering event planners identify vulnerabilities, prioritize mitigation efforts, and implement measures for pedestrian and structural security [...] The vehicle-borne threat assessment is unique in that the user assesses whether the land directly around, adjacent to, and adjoining their site or infrastructure can be a pathway for a vehicle incident. Questions to ask during an assessment could include:

- ▶ Is my land, the adjacent land, or the surrounding land traversable by vehicles?
- ▶ What types of vehicles could traverse the land?
- ▶ What is the maximum speed a vehicle could attain going over the land?
- ▶ Is there an entry control point for vehicles? If so, how far from infrastructure is it located?
- ▶ Are there security guards at entry control points?
- ▶ Where are vehicle parking spots, lots, or garages?
- ▶ Are there any delivery vehicle access points?
- ▶ Are there any natural vehicle barriers already in place?
- ▶ What angles of attack could a vehicle use to harm my infrastructure?
- ▶ Are there any traffic-calming areas?
- ▶ Are there security cameras that cover areas where vehicles are present or will/could be traversing?
- ▶ Is pedestrian traffic, whether from parking areas or near facility entry/exit points, properly separated from vehicular traffic?"

Source: US DHS CISA

²⁷⁸ US Cybersecurity & Infrastructure Security Agency (2024), *Vehicle Incident Prevention and Mitigation: Security Guide*. Available at: https://www.cisa.gov/sites/default/files/2024-04/Vehicle_Incident_Prevention_and_Mitigation_Security_Guide_508_20240418.pdf [accessed 13 May 2025].

Many security measures detailed in this section will reference a “crash rating”, which means they are rated by the vendor to withstand the impact of a moving vehicle up to a specific point. There are many factors that feed into the crash rating of a particular barrier option, including the weight of a potential hostile vehicle (motorcycle versus a large truck, for example) as well as the speed and angle at which it makes impact with the barrier or object in question. For this reason, CI owners/operators are encouraged to consider this range of factors when determining their preferred method or methods for protecting a CI facility against hostile vehicles. Some examples of national and international standards used to define crash ratings include:

- ▶ ISO (2023) *Security and resilience – Vehicle security barriers. Part 1: Performance requirement, vehicle impact test method and performance rating*,²⁷⁹
- ▶ American Society for Testing and Materials F 2656: *Standard Test Method for Crash Testing of Vehicle Security Barriers*,²⁸⁰
- ▶ British Standards Institution *Publicly Available Specification 68*.²⁸¹

279 ISO (2023) *Security and resilience – Vehicle security barriers. Part 1: Performance requirement, vehicle impact test method and performance rating*. Available at: <https://www.iso.org/standard/50080.html> [accessed 13 May 2025].

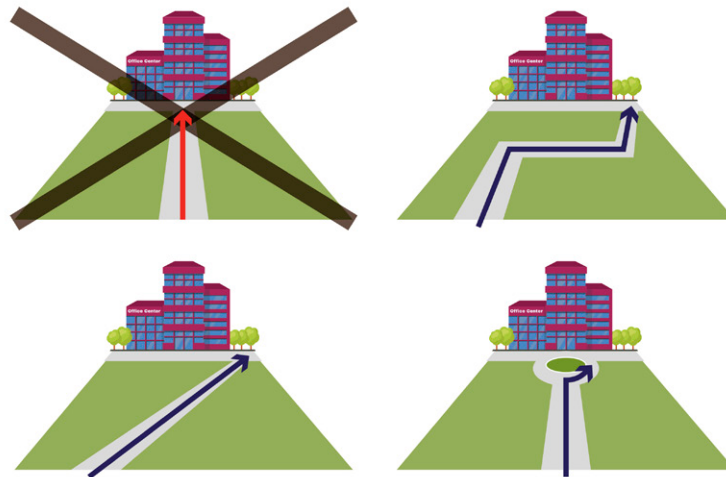
280 ASTM International (November 2023), *Standard Test Method for Crash Testing of Vehicle Security Barriers*, ASTM F2656/F2656M-23.

281 British Standards Institution (August 2013), *Impact test specifications for vehicle security barrier systems, Third Edition*.

Vehicle Speed Control

The threat of a hostile vehicle attack can be reduced significantly by controlling vehicular speed as it approaches a CI facility and removing the possibility for a hostile vehicle to directly collide with a CI building. Designing entry roads to a CI facility that do not provide direct or straight-line access makes it impossible for a vehicle to gather speed as it approaches. This type of design, together with appropriate landscaping, decreases the effectiveness of any potential hostile vehicle attack.

In instances in which a vehicle barrier is used at the entry to a CI facility, impact requirements are affected by factors such as vehicle speed upon approach and the angle of its impact on a barrier. The size of vehicle is also relevant, not only due to the force with which a larger vehicle can strike a target, but also since larger vehicles travelling at the same speed could contain more explosive material and hence cause a larger explosion that causes damage to nearby buildings. CI facilities could consider the use of different access roads for larger vehicles, with further speed reduction control measures.



*Various vehicle speed reduction measures, including indirect access to a site.
Used with permission of the European Commission's Joint Research Centre.²⁸²*

Other potential options to reduce vehicle speed through road design are the use of curved roadways, parallel approaches and chicanes:

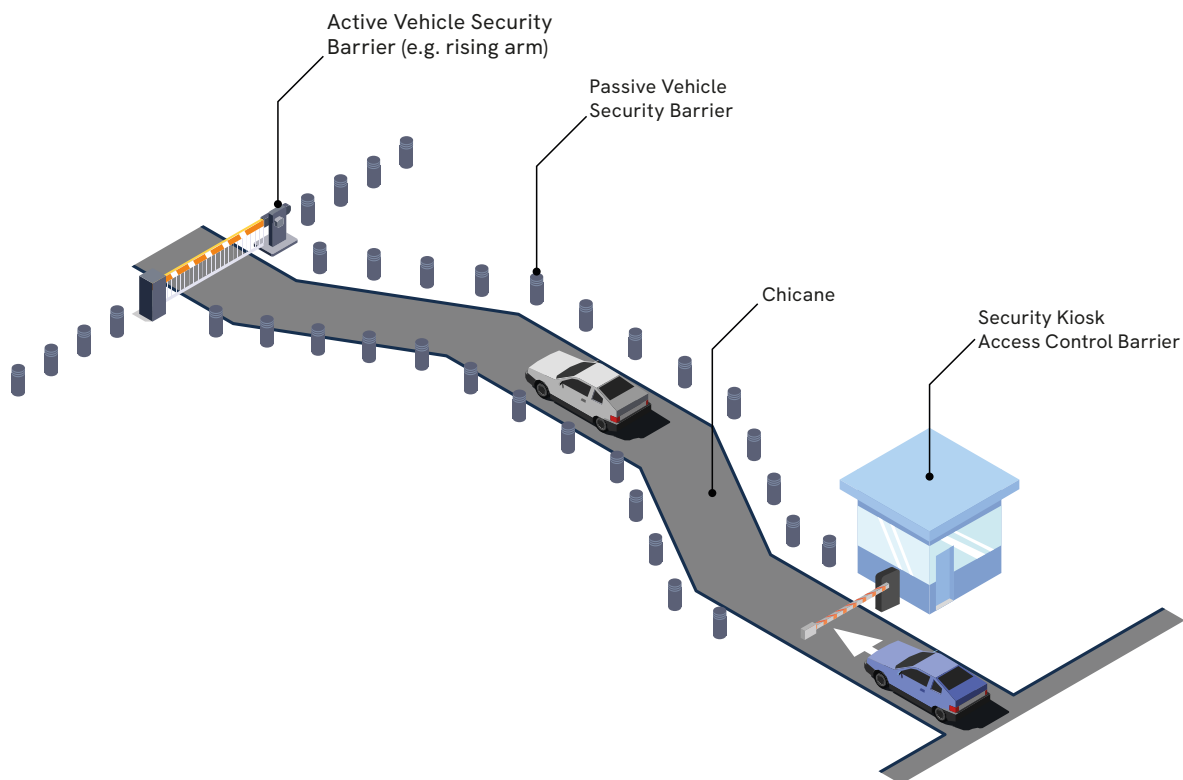
- ▶ **Curved roadways:** Straight and perpendicular approaches to the CI facility allow a vehicle to build up speed and potentially penetrate a CI facility or its perimeter. However, by curving the entry road to a CI facility, a hostile vehicle travelling at a high speed may skid or overturn. To reduce the risk of losing control, drivers will be forced to reduce speed.²⁸³
- ▶ **Parallel approaches:** Parallel roads that run alongside the perimeter of a facility can prevent a vehicle from building up enough speed for a direct attack or to overcome a facility's perimeter.²⁸⁴

²⁸² Publications Office of the European Union (2024), *Security by Design: Protection of public spaces from terrorist attacks*. Available at: <https://publications.jrc.ec.europa.eu/repository/handle/JRC131172> [accessed 13 May 2025].

²⁸³ Baker, P.; Benny, D. J. (2013), *The Complete Guide to Physical Security* (Boca Raton: CRC Press).

²⁸⁴ Baker, P.; Benny, D. J. (2013), *The Complete Guide to Physical Security* (Boca Raton: CRC Press).

- **Chicanes:** A chicane is a double bend in a road created intentionally to reduce vehicle speed and control its entry or exit (see the graphic below). Permanent chicanes can consist of vehicle barriers placed along the edges of a road, forcing a vehicle to drive through the chicane. Temporary chicanes can consist of large concrete blocks serving a similar purpose. CI facilities can implement both temporary and permanent chicanes based on its assessed threat environment.²⁸⁵



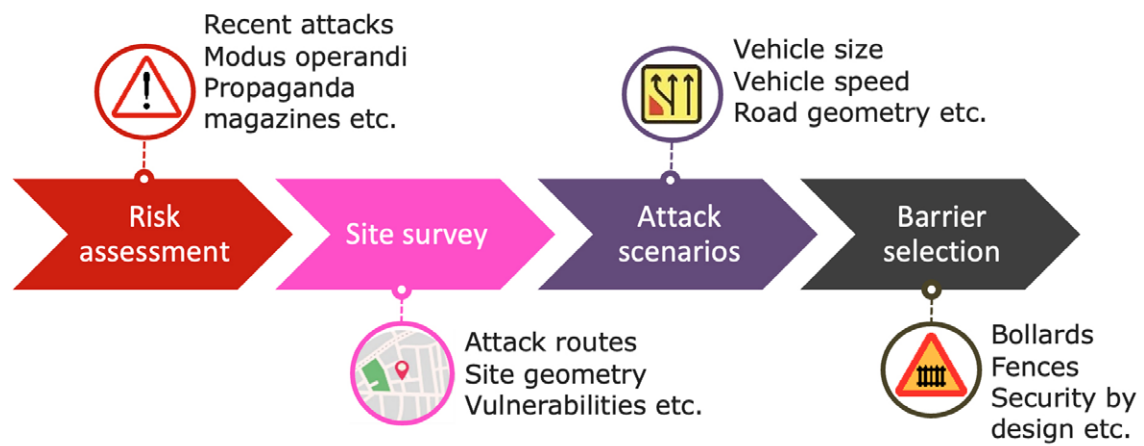
Vehicle Barriers: Passive and Active Barriers

Vehicle barriers used to mitigate hostile vehicle threats are either passive (fixed) or active (operable). The decision as to which barrier is most appropriate for a given CI facility should be based on a risk assessment that specifically examines hostile vehicle threats and potential threat scenarios. In any case, barriers must be properly designed, constructed and regularly maintained to ensure their correct operation. This is particularly relevant for active barriers with moving parts.

Performance requirements for vehicle barriers are addressed in ISO 22343:1:2023 "Security and resilience – Vehicle security barriers/Performance requirement, vehicle impact test method and performance rating".²⁸⁶

²⁸⁵ Comrie, D.; Mays, G.; Smith, P. (2009) "Vehicle-borne threats and the principles of hostile vehicle mitigation", in Comrie, D.; Mays, G.; Smith, P., *Blast Effects on Buildings (2nd Edition)* (London: ICE Publishing).

²⁸⁶ ISO (2023), *Security and resilience — Vehicle security barriers. Part 1: Performance requirement, vehicle impact test method and performance rating*. Available at: <https://www.iso.org/standard/50080.html> [accessed 13 May 2025].



*Process diagram for the selection of anti-ramming vehicle barriers.
Used with permission of the European Commission's Joint Research Centre.²⁸⁷*

Passive Vehicle Barriers

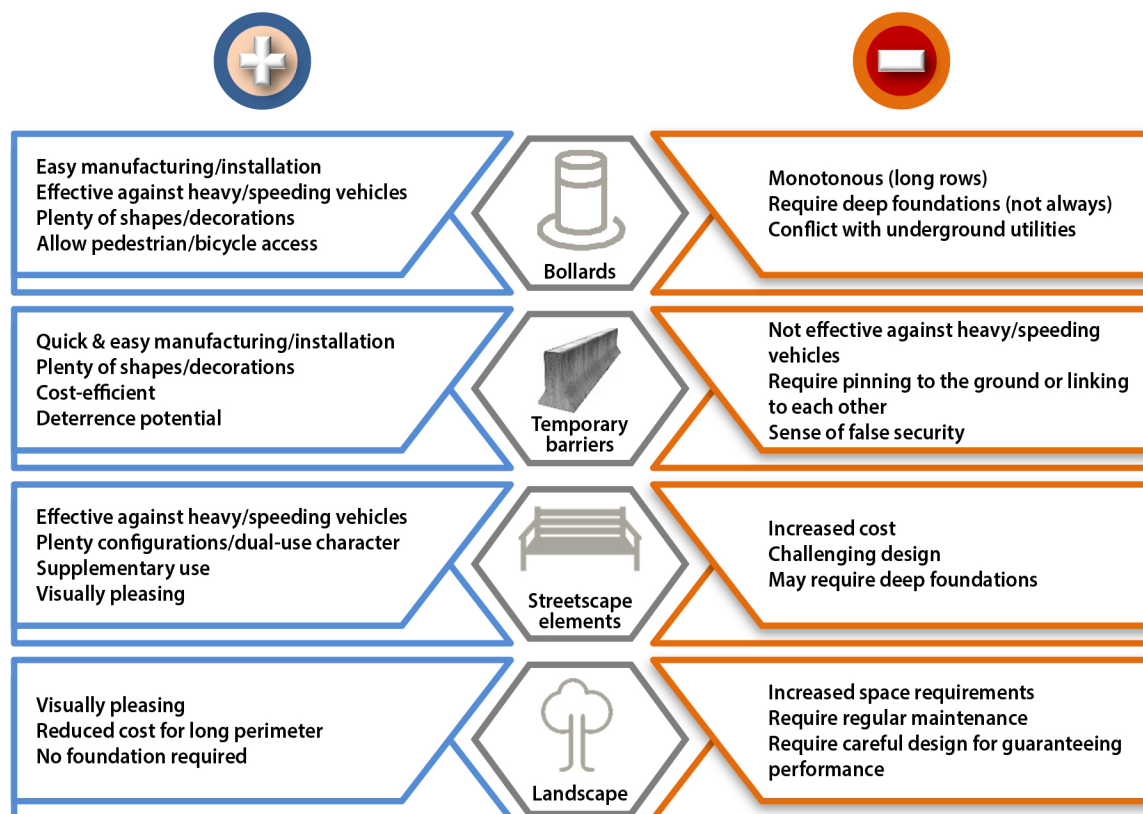
Passive barriers are solid structures that basically block vehicle entry and, in doing so, protect a facility or site's perimeter.²⁸⁸ They are designed to absorb the impact of a vehicle using a firm foundation or a combination of the structure's weight and the friction caused when it moves along the road surface.²⁸⁹

²⁸⁷ Vasilis, K.; Larcher, M. (2020), *Guideline, building perimeter protection: Design recommendations for enhanced security against terrorist attacks*, Publications Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en> [accessed 13 May 2025].

²⁸⁸ US DHS FEMA (2007), *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*. Available at: <https://www.fema.gov/sites/default/files/2020-08/fema430.pdf> [accessed 13 May 2025].

²⁸⁹ Vasilis, K.; Larcher, M. (2020), *Guideline, building perimeter protection: Design recommendations for enhanced security against terrorist attacks*, Publications Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en>

Examples of passive barriers include fixed bollards, engineered planters, heavy objects, trees, walls, water obstacles and fences.^{290, 291}



*Advantages and disadvantages of passive barrier solutions.
Used with permission of the European Commission Joint Research Centre.²⁹²*

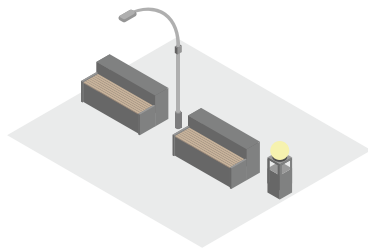
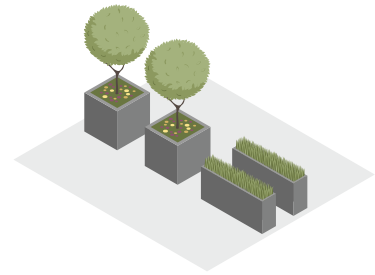
²⁹⁰ US DHS (2011), *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings: FEMA-426/BIPS-06/ October 2011. Edition 2.* Available at: <https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf> [accessed 13 May 2025].

²⁹¹ US DHS FEMA (2007), *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks.* Available at: <https://www.fema.gov/sites/default/files/2020-08/fema430.pdf> [accessed 13 May 2025].

²⁹² Vasilis, K.; Larcher, M. (2020), *Guideline, building perimeter protection: Design recommendations for enhanced security against terrorist attacks*, Publications Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en>

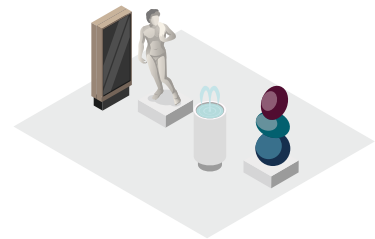
Different Passive Barrier Options (non-exhaustive)

Engineered planters: A well-designed planter can form an effective vehicle barrier and an aesthetic addition to a CI facility perimeter. Planters can either be fixed to the ground or heavy enough to rely on friction to stop or delay a hostile vehicle. In the event of the latter, planters may be pushed aside by heavy or fast-moving vehicles. Planters fixed to the ground through sufficient subterranean reinforcements may offer higher protection from a range of vehicle sizes and speeds.²⁹³



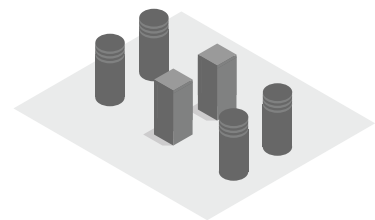
Reinforced street furniture and fixtures: Streetscape elements, such as benches and streetlights, can be hardened or reinforced to serve as passive barriers. This allows them to serve as both amenities and components of perimeter security, if properly engineered.²⁹⁴ Strategically placing them around the perimeter of a CI facility where vehicles are present may also serve aesthetic purposes.

Heavy objects: Heavy objects such as sculptures and boulders can also serve a dual purpose of aesthetics and passive barriers. To ensure that they can effectively reduce an identified threat, engineering design and/or evaluation is necessary.²⁹⁵



Landscape elements, trees: Depending on a CI facility's location, landscape elements such as rock formations, water features, elevated areas or trees may also be used as part of a facility's hostile vehicle mitigation.²⁹⁶ In some cases, such elements can also be reinforced to provide additional protection.

Specifically-designed hostile vehicle mitigation barriers: Engineered bollards are one of the most popular solutions for preventing unauthorized vehicle access. They are typically made of steel, reinforced concrete or a combination of the two (concrete core surrounded by a steel casing). Their narrow form and unobtrusive size make them more attractive for public spaces, for example, than other solutions. As a general observation, the performance of an engineered bollard depends on the depth its foundation reaches below ground and its overall size.²⁹⁷



293 US DHS FEMA (2007), *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*. Risk Management Series. Available at: <https://www.fema.gov/sites/default/files/2020-08/fema430.pdf> [accessed 13 May 2025].

294 US DHS FEMA (2007), *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*. Risk Management Series. Available at: <https://www.fema.gov/sites/default/files/2020-08/fema430.pdf> [accessed 13 May 2025].

295 US DHS FEMA (2007), *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*. Risk Management Series. Available at: <https://www.fema.gov/sites/default/files/2020-08/fema430.pdf> [accessed 13 May 2025].

296 Vasilis, K.; Larcher, M. (2020), *Guideline, building perimeter protection: Design recommendations for enhanced security against terrorist attacks*, Publications Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en> [accessed 13 May 2025].

297 US DHS FEMA (2007), *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*. Risk Management Series. Available at: <https://www.fema.gov/sites/default/files/2020-08/fema430.pdf> [accessed 13 May 2025].

Active Vehicle Barriers

Active barriers may be used at vehicle access control points around the perimeter of a CI facility, or at the entrance to a specific building within a site. For the latter, they can provide a barrier for vehicle screening or inspection. Their opening may be controlled by different actors, such as the driver of an authorized vehicle, by an automated electronic system, or by security personnel who are responsible for inspecting incoming traffic. There are both advantages and disadvantages to active barrier systems, as shown below. Due to their moving parts, maintenance of active barrier mechanical systems is required to guarantee performance.

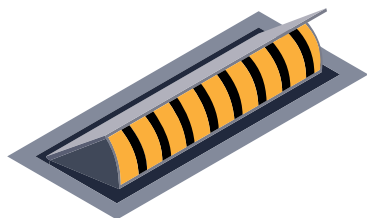
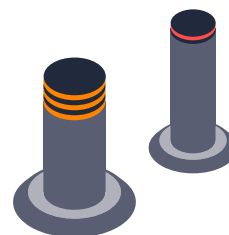
		
Immediate availability Plenty of shapes/decorations Allow pedestrian/bicycle access	 Retractable bollards	Require deep and wide foundations Expensive solutions Problematic in case of high groundwater level
Effective against heavy/speeding vehicles Shallow foundations High protection level	 Road blockers	Visually obtrusive May block pedestrian/bicycle access Expensive solutions
Effective against heavy/speeding vehicles Shallow or no foundations High protection level	 Drop-arm barriers	Visually obtrusive Block pedestrian/bicycle access Low operating speed
Part of perimeter fence Plenty of designs Deterrence effect	 Gates	Visually obtrusive Low operating speed Expensive solution

Advantages and disadvantages of active barrier solutions.
Used with permission of the European Commission’s Joint Research Centre.²⁹⁸

298 Karlos, V.; Larcher, M. (2020), Guideline, building perimeter protection: Design recommendations for enhanced security against terrorist attacks, Publications Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en> [accessed 13 May 2025].

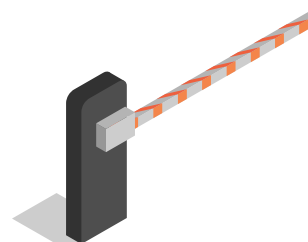
Different Active Barrier Options²⁹⁹

Retractable bollards: A retractable bollard system consists of one or multiple rising bollards operating independently or in groups of two or more.³⁰⁰ They remain in a raised position to block vehicular access and lowered only to allow approved vehicles to pass. These are generally viewed as an expensive active barrier given the high costs of installing them and ensuring they have a sufficiently deep foundation to block vehicular threats.³⁰¹



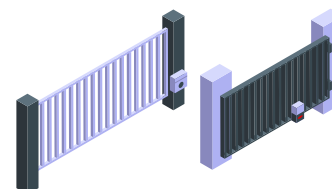
Ramp-style barriers or road blockers: Road blockers are comprised of a reinforced barrier, typically made from steel, and sit in a raised position to block vehicle access. When needed, they can be lowered with a hydraulic or electrical system to become completely flush with the ground, thereby allowing vehicles to pass.³⁰² When in a raised position, some road blockers can be fixed with spikes to deflate tires of vehicles that attempt to overcome the barrier.

Drop arm barriers: Drop arm barriers are typically deployed at checkpoints or entrance points to a protected site and are often accompanied by security personnel or an automated access control system. The barrier consists of a metal arm that sits in a horizontal position to block vehicular access,³⁰³ which is then raised to allow vehicles to pass.



Drop arm crash beams: Drop arm crash beams are generally seen as a stronger version of drop arm barriers. They are usually certified to specific vehicle crash standards and are made of adequately reinforced steel and other materials.³⁰⁴ This system operates in a similar manner to drop arm barriers, but typically has concrete or otherwise reinforced structures on both sides of its metal arm to withstand higher impacts.

Gates: Typically part of a larger perimeter fence, gates operate on wheels or hinges in order to allow vehicles to pass through. There are several types of gates that have specific crash ratings.³⁰⁵ Depending on the gate used, it is possible for a fast-moving vehicle to break through and send hazardous shrapnel flying in different directions.



299 Types of “different active barrier options” extracted from: Karlos, V.; Larcher, M. (2020), *Guideline, building perimeter protection: Design recommendations for enhanced security against terrorist attacks*, Publications Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en> [accessed 13 May 2025].

300 US DHS FEMA (2007), *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*. Available at: <https://www.fema.gov/sites/default/files/2020-08/fema430.pdf> [accessed 13 May 2025].

301 Karlos, V.; Larcher, M. (2020) *Guideline, building perimeter protection: Design recommendations for enhanced security against terrorist attacks*, Publications Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en> [accessed 13 May 2025].

302 Karlos, V.; Larcher, M. (2020) *Guideline, building perimeter protection: Design recommendations for enhanced security against terrorist attacks*, Publications Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en> [accessed 13 May 2025].

303 Karlos, V.; Larcher, M. (2020) *Guideline Building perimeter protection - Design recommendations for enhanced security against terrorist attacks*, Publications Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en> [accessed 13 May 2025].

304 US DHS FEMA (2007), *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*. Available at: <https://www.fema.gov/sites/default/files/2020-08/fema430.pdf> [accessed 13 May 2025].

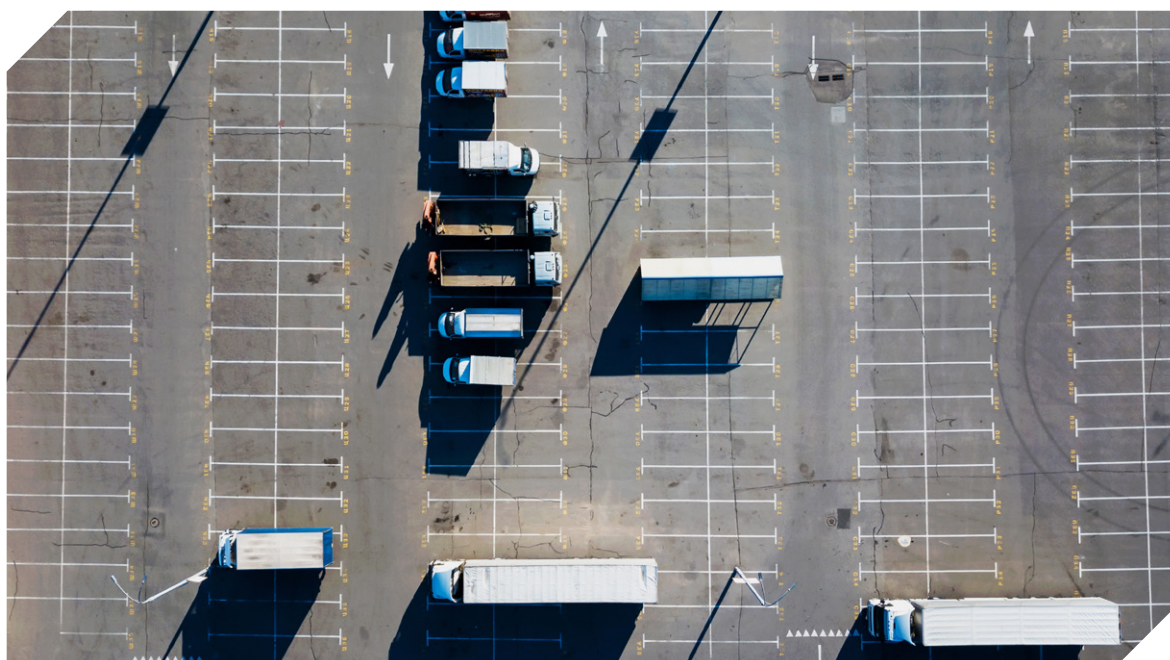
305 US DHS FEMA (2007), *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*. Available at: <https://www.fema.gov/sites/default/files/2020-08/fema430.pdf> [accessed 13 May 2025].

Temporary Barriers

During a period of elevated threat at a given CI facility, temporary barriers may provide enhanced protection against hostile vehicles. They can be deployed on short notice and reoriented to control or redirect traffic as needed. By their very nature, they are not fixed to the ground so they often rely on their mass to gradually stop a moving vehicle. This is often most effective when a vehicle is travelling at relatively low speeds. This makes temporary barriers slightly less practical for the long-term protection of sensitive sites or CI facility perimeters. They can act as a visual deterrent to influence potential aggressors, but can also provide a false sense of security. Examples of temporary barriers include concrete- or water-filled jersey barriers or large planters.³⁰⁶

Vehicle Parking

Hostile vehicles need not always be in motion to pose a threat to a CI facility. For example, they can be parked and laden with explosives. This raises the challenge of vehicle parking outside or next to a CI facility. As a general measure, parking spaces outside a CI facility should be located away from a CI facility's perimeter or critical assets. The exact stand-off distance will need to be determined by competent authorities and CI owners/operators based on the assessed explosive force of an explosive device placed inside a vehicle and parked at the site.



306 Karlos, V.; Larcher, M. (2020) *Guideline, building perimeter protection: Design recommendations for enhanced security against terrorist attacks*, Publications Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en> [accessed 13 May 2025].

7.3 Security Planning for Explosive Attacks

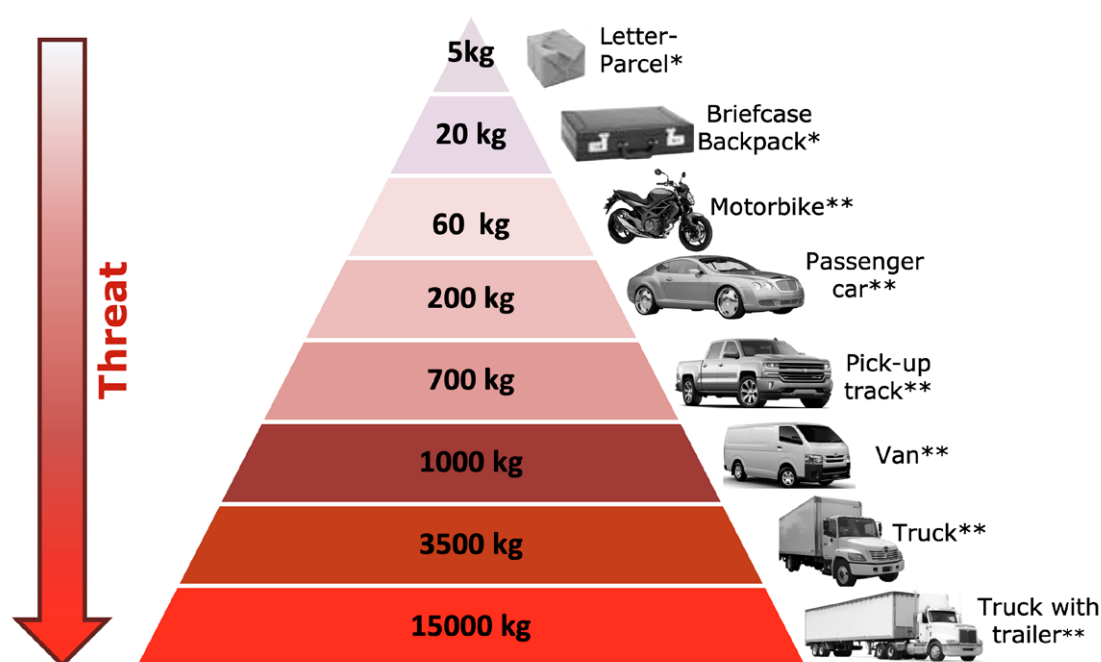
Terrorists and other violent actors may wish to target a CI facility using explosives. In order to prepare CI facilities for these threats, this section provides a range of good practices and guidance.³⁰⁷ In some cases, the guidance in this section is more closely related to responding to an explosive incident, rather than enhancing the physical security of a facility to these threats. While this may go beyond physical security considerations, it is nevertheless part of an effective security framework for any CI facility.

RISK ANALYSIS	• Asset definition (building type, open area, people, etc.) • Vulnerabilities identification (absence of security measures, etc.) • Likelihood/consequence assessment (accessibility, importance, attendance, etc.) • Risk evaluation (attack scenario prioritisation, acceptable/intolerable risk, etc.)
STAND-OFF DISTANCE (R)	• Existing perimeter protective measures (fences, detection systems, etc.) • Site geometry (inclination, natural or artificial barriers, etc.) • Deterrence measures (surveillance systems, security guards, etc.)
CHARGE WEIGHT (W)	• Possible transportation means (bags, cars, trucks, etc.) • Accessibility of explosive materials (regional safety characteristics, past events, etc.) • Charge types (TNT, ANFO, TATP, etc.)
BLAST ANALYSIS	• Calculation of scaled distance (Z) • Determination of blast parameters (peak overpressure, positive impulse, etc.)
MITIGATION SOLUTION	• Calculation of scaled distance (Z) • Determination of blast parameters (peak overpressure, positive impulse, etc.)

*Steps which can be followed to decide on appropriate hardening measures against IED attacks.
Used with permission of the European Commission's Joint Research Centre.³⁰⁸*

³⁰⁷ See also: *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* published by UNOCT, the UNSC Counter-Terrorism Executive Directorate, the UN Institute for Disarmament Research, and the UN Global Counter-Terrorism Coordination Compact.

³⁰⁸ Publications Office of the European Union (2024), *Security by Design: Protection of public spaces from terrorist attacks*. Available at: <https://publications.jrc.ec.europa.eu/repository/handle/JRC131172> [accessed 13 May 2025].



* Person borne improvised explosive device (PBIED)

**Vehicle borne improvised explosive device (VBIED)

Upper charge mass limits by means of transportation.

Used with permission of the European Commission's Joint Research Centre.³⁰⁹

Bomb Threats

Bomb threats are a common modus operandi for a range of threat actors, since they can be highly disruptive yet require minimal effort. In some cases, bomb threats have been communicated to law enforcement or CI facility personnel by terrorist organizations to warn of a real impending explosive attack. In other cases, only a threat is made with no explosives found; nonetheless, notable disruption is caused. Bomb threats can also be made by random members of the public, disgruntled current or former personnel at a CI facility, or other actors seeking to test the reaction of CI facility personnel or law enforcement. Whatever the circumstances, bomb threats at CI facilities must be taken seriously and procedures should exist to ensure rapid decision-making by competent actors on-site and elsewhere (for example, local law enforcement). Practices for ensuring facilities are sufficiently hardened against bomb threats, namely, by fortifying building and perimeter structures, are detailed in Chapter 6, Physical Security Measures. This section provides examples of good practices on responding to bomb threats at CI facilities.

CI facility personnel likely to receive bomb threats, such as receptionists or security personnel, should be trained in responding to such threats. To support personnel, CI facilities may wish to have written instructions that can be referred to in the event a threatening call is received.

³⁰⁹ Publications Office of the European Union (2024), Security by Design: Protection of public spaces from terrorist attacks. Available at: <https://publications.jrc.ec.europa.eu/repository/handle/JRC131172> [accessed 13 May 2025].

National Practice: US CISA Checklist to Response to a Bomb Threat (by Phone)³¹⁰

Date	
Time	
Time when the caller hung up	
Phone number where call was received	
Ask the caller: ▶ Where is the bomb located? (building, floor, room, etc.) ▶ What does it look like? ▶ What kind of bomb is it? ▶ What will make it explode? ▶ Did you place the bomb? ▶ Why? ▶ What is your name?	
Exact words of the threat	
Information about the caller: ▶ Where is the caller located? (background/level of noise) ▶ Estimated age ▶ Is the voice familiar? If so, who does it sound like? - Other points	

Source: US DHS CISA

³¹⁰ CISA (no date), Bomb Threat Checklist. Available at: <https://www.cisa.gov/sites/default/files/2025-03/Bomb%20Threat%20Checklist%20v3.0%20508.pdf> [accessed 18 May 2025].

Practice: Association of Banks in Singapore Guidance for Bomb Threats Received by Telephone (2018)³¹¹

When a bomb threat is received:

1. Do not panic. Stay calm.
2. Alert someone to call the Police. Keep the caller occupied by talking as long as possible while the Police traces the call.
3. The officer receiving such calls should [treat] them seriously and immediately try to determine:
 - ▶ the precise location of the bomb and exactly [what] it looks like;
 - ▶ the detonation time and what will it set off;
 - ▶ the amount and type of explosive used; and
 - ▶ the reason for such an act.
4. It is also important to take note of the following:
 - ▶ the caller's voice and vocal characteristics (e.g. pitch, male/female, adult/child);
 - ▶ the language used and accent (e.g. local or foreign);
 - ▶ manner of speaking (e.g. rapid, deliberate, emotional, angry);
 - ▶ background noises (e.g. traffic, music, public announcements, shouting);
 - ▶ the person or authority whom this message should be conveyed to;
 - ▶ do not antagonise or taunt the caller in any way; and
 - ▶ be polite and remain calm.
5. Do not spread rumours.
6. Depending on the situation, evacuation.

Source: Singapore Association of Banks

³¹¹ Association of Banks in Singapore (2018), *Physical Security Guidelines for Financial Institutions*. Available at: <https://abs.org.sg/docs/library/abs-scps-guidelines.pdf> [accessed 13 May 2025].

National Practice: US CISA Guidance on the Response to a Bomb Threat (by Social Media, Email or in Writing)³¹²

If you receive a social media or email threat:

- ▶ Do not turn off or log out of the account
- ▶ Leave the message open on the device
- ▶ Take a screenshot, or copy the message and subject line
- ▶ Note the date and time
- ▶ Notify the [relevant] Decision Maker(s)

If you receive a written threat:

- ▶ Handle the document as little as possible
- ▶ Note date, time, and location the document was found
- ▶ Secure the document and do not alter the item in any way
- ▶ Notify the [relevant] Decision Maker(s)

Source: US DHS CISA

In addition to defining the immediate steps the recipient of a bomb threat at a CI facility should take, such as what information to record and to whom it should be conveyed, an emergency response procedure should also be defined for the CI facility. It should include the early involvement of local law enforcement. The exact role of law enforcement should be defined together with law enforcement authorities to ensure that the procedure can be followed in an emergency situation.

National Practice: Canada's Centre for Occupational Health and Safety Bomb Threat Guidance (2023)³¹³

Under Canadian legislation, each jurisdiction is responsible for developing emergency response procedures in consultation with the health and safety committee (or health and safety representative) to identify and address all foreseeable emergency situations, including bomb threats. Employers should ensure that:

- ▶ A comprehensive emergency response procedure (in consultation with local police authorities) to deal with bomb threats has been developed.
- ▶ Procedures are communicated to all employees, identifying key roles in a bomb threat emergency.
- ▶ Emergency drills are conducted for bomb threats.
- ▶ Practice drills are documented.
- ▶ Evacuation procedures are in place, as may be necessary.

Source: Canada's Centre for Occupational Health and Safety

³¹² CISA (no date), Bomb Threats [webpage]. Available at: <https://www.cisa.gov/bomb-threats> [accessed 10 December 2024].

³¹³ Canadian Centre for Occupational Health and Safety (2023), Bomb Threat [webpage]. Available at: <https://www.ccohs.ca/oshanswers/hsprograms/bomb-threat.html#section-3-hdr> [accessed 10 December 2024].

If the competent actors and authorities determine that it is appropriate and proportionate to search a facility, the emergency response procedure should support the rapid execution of this task. Importantly, this procedure should be exercised on a routine basis to ensure that all facility personnel, not solely those with security roles, are aware of appropriate behaviour in the event of a bomb threat. Exercises should be based on various different scenarios, including bomb threats received in writing as a physical letter, as a phone call, or via other means.³¹⁴

National Practice: UK National Counter Terrorism Security Office Guidance on Checking a Venue for Suspicious Items³¹⁵

- ▶ Ensure plans are in place to carry out an effective search in response to a bomb threat.
- ▶ Identify who in your venue will coordinate and take responsibility for conducting searches.
- ▶ Initiate a search by messaging over a public address system (coded messages avoid unnecessary disruption and alarm), by text message, personal radio or by telephone cascade.
- ▶ Divide your venue into areas of a manageable size for 1 or 2 searchers; ideally staff should follow a search plan and search in pairs to ensure the area is covered effectively.
- ▶ Ensure those conducting searches are familiar with their areas of responsibility; those who regularly work in an area are best placed to spot unusual or suspicious items.
- ▶ Focus on areas that are open to the public; enclosed areas (e.g. cloakrooms, stairs, corridors, lifts etc.) evacuation routes and assembly points, car parks, other external areas such as goods or loading bays.
- ▶ Develop appropriate techniques for staff to be able to routinely search public areas without alarming any visitors or customers present.
- ▶ Ensure all visitors know who to report a suspicious/unattended item to, and have the confidence to report suspicious behaviour.
- ▶ Under no circumstances should any item assessed as suspicious be touched or moved in any way. Once an item is declared suspicious by a competent person, commence evacuation immediately.

Source: UK National Counter Terrorism Security Office

³¹⁴ For a complete bomb threat guide, see: CISA (no date), Bomb Threat Guide. Available at: <https://www.cisa.gov/resources-tools/resources/bomb-threat-guide> [accessed 13 May 2025].

³¹⁵ National Counter Terrorism Security Office, ProtectUK (no date), Bomb Threats [webpage]. Available at: <https://www.protectuk.police.uk/bomb-threats> [accessed 10 December 2024].

National Practice: US CISA Office for Bombing Prevention Guidance on Identifying Suspicious or Unattended Items (2023)³¹⁶

In order to distinguish between suspicious or unattended items, CISA offers a quick reference document based on the HOT Principle. Based on this principle, individuals work through three different questions:

- ▶ H: Is the item **H**idden?
- ▶ O: Is it **O**bviously suspicious?
- ▶ T: Is it not **T**ypical?

Answering these questions will help determine if the item in question is suspicious. If there is reason to believe it is suspicious, the document leads individuals to another principle, RAIN:

- ▶ **R**ecognize the indicators of a suspected explosive device.
- ▶ **A**void the area.
- ▶ **I**solate the suspected item.
- ▶ **N**otify the appropriate emergency services.

Source: US DHS CISA

Explosive Threats in the Mailroom

One way a terrorist or threat actor may wish to disrupt a CI facility is to deliver an explosive device to its mailroom. There are various advantages to this attack methodology: it limits harm to the threat actors themselves, it can bypass many of control and security measures for CI facility access that a hostile person or vehicle would be unable to bypass, and it can, if not identified by personnel in a mailroom, be delivered to specific targets within a CI facility.

Any area where incoming packages are screened should be designed to mitigate blast effects. The best practice in this regard would be to locate a mailroom entirely off the CI site to avoid disruptions in the event of a suspicious package. If this is not feasible, CI owners/operators may wish to locate mailrooms near the entrance to a building that itself is near the entrance to the CI site. This means that in the event of an explosive device detonating in the mailroom or on its way there, it has not yet travelled deep enough into a building/site to severely disrupt critical operations (depending on the location of such operations). When considering the location of a mailroom, CI owners/operators should also consider its proximity to staircases and structural elements of a building and ensure sufficient distance from them. Some CI facilities may not have an in-house mailroom, receiving mail, for example, from third party service providers or couriers at the reception area. Such reception areas may be exposed to the same explosive threats from incoming packages as a mailroom, and thus similar physical security precautions (namely measures mitigating blast effects) should be taken.

In addition to blast mitigation measures, mailrooms should also be equipped with VSS and controls to ensure that only authorized people have access to them. Mailroom

³¹⁶ CISA (no date), Suspicious or Unattended? [webpage]. Available at: <https://www.cisa.gov/sites/default/files/2023-04/Unattended%20vs%20Suspicious%20Card%20for%20Digital%20Final%20v2.1.pdf> [accessed 13 May 2025].

personnel should be trained in appropriate actions in the event a suspicious package is identified.³¹⁷ This should include the early notification of CI facility security personnel.

Suspicious Packages Found on a Critical Infrastructure Site

CI facilities should have procedures for the event a suspicious package or item is found on a CI site, since this could represent an explosive threat. Suspicious items could be a suitcase, box, bag or other object anywhere within a CI building or site. All CI personnel should be aware of this procedure and should know to whom any suspicious item found on-site should be reported.

National Practice: Russian Federation National Anti-Terrorism Committee's Recommended Procedure for Detecting a Suspicious Object that may be an Explosive Device³¹⁸

1. Immediately report the find to the administration or security of the institution.
2. Record the time and place of discovery of the unknown object.
3. Take measures to ensure that people move as far as possible from the suspicious object and danger zone.
4. Wait for the arrival of representatives of the competent authorities, indicate the location of the suspicious object, the time and circumstances of its discovery.
5. Don't panic. Inform only those who need to know about the incident about a possible explosive threat. It is also necessary to remember that the appearance of the object may hide its real purpose. The presence of an explosive device or other dangerous objects may be indicated by the following signs:
 - ▶ The presence of wires, small antennas, electrical tape, twine, rope or tape in the bag or sticking out of the bag;
 - ▶ Noise from detected suspicious objects (packages, bags, etc.). This can be the ticking of a clock, clicks, etc.;
 - ▶ The presence of batteries on the suspicious object;
 - ▶ Stretchers made of wire, ropes, twine, fishing line;
 - ▶ Unusual placement of the object;
 - ▶ The presence of an object that is not typical for the area;
 - ▶ A specific smell unusual for this area.

Source: Russian Federation's National Anti-Terrorism Committee

Since a suspicious item may be an explosive device with a remote firing system, mobile phones and radios should not be used within a defined distance. For example, the United Kingdom recommends 15 metres for mobile phones/radios and 50 metres for vehicle-mounted radio devices.³¹⁹

317 For an example of a quick reference poster, see: CISA (no date), Suspicious Mail or Packages [webpage]. Available at: <https://www.cisa.gov/sites/default/files/2023-11/Mail%20and%20Suspicious%20Package%20Guidance%20Poster.pdf> [accessed 13 May 2025].

318 National Anti-Terrorism Committee (no date), Procedure for detecting a suspicious object that may be an explosive device [webpage, in Russian]. Available at: <http://nac.gov.ru/rekomendacii-po-pravilam-lichnoy-bezopasnosti/poryadok-deystviy-pri-obnaruzhenii.html> [accessed 10 December 2024] unofficial translation.

319 Cambridgeshire Constabulary (no date), The HOT Principle [webpage]. Available at: <https://www.huntingdonshire.gov.uk/media/2750/hot-principle.pdf> [accessed 13 May 2025].

Vehicle-Borne Explosive Threats

Although terrorists continually adapt, vehicle-borne explosive threats – typically a vehicle-borne improvised explosive device (VBIED) – remain an effective and longstanding *modus operandi*. This methodology involves using a vehicle to conceal an explosive device. Various types of vehicles can be used, including cars, vans, buses, delivery trucks, etc., with larger vehicles capable of carrying larger amounts of explosives. VBIEDs can be detonated through a range of methods, including the force from ramming the vehicle into an object, a timer, a remote-activated trigger, or a human operator (suicide operation). VBIEDs are capable of causing massive structural damage to property and thus pose a major threat to the perimeters and internal structures of CI facilities.³²⁰

In addition to the primary blast effects of a VBIED's detonation, the vehicle's destruction in the blast can cause additional shrapnel and fuel explosions. Depending on the size of the explosive charge and the VBIED's location, the explosive blast can shatter windows several hundred metres away. Fragments from broken windows can be responsible for deaths and injuries, since fast-travelling glass splinters can easily penetrate the human body.³²¹

When considering VBIED threats to a CI site, it is vital to determine the distance to be maintained from a vehicular threat to ensure no damage to CI buildings, perimeter fences, gates, other vital structures, or vehicles on or near the site. Also known as stand-off distance, this is the most important factor when establishing the extent of damage that a building can suffer due to a VBIED attack.

Increasing the stand-off distance will have a significant effect on the ability to mitigate VBIED threats. Key areas to protect against VBIED threats include the site perimeter, adjacent areas, and vehicle access control points.

Person-Borne Explosive Threats

A common terrorist *modus operandi* is to deliver an explosive device to an intended target using a person – often referred to as a person-borne improvised explosive device (PBIED). A PBIED is often selected by terrorist organizations, since it allows the explosive device to be delivered to a specific, and potentially well-fortified, target. A person wearing a PBIED can adapt to a changing security environment, negotiate their entry onto a site, and make decisions/change strategy in real-time. A PBIED is typically concealed, either under or within clothing, shoes, or other types of apparel. Individuals delivering a PBIED are often referred to as suicide bombers, since they die by suicide upon detonation of the device. PBIEDs can be detonated through a range of methods, including but not limited to a switch/initiator activated by the suicide bomber him/herself, a time-delay system, or remotely by a third actor. These latter two methods ensure detonation of the PBIED, even if the person wearing it changes his/her mind.

320 For reference, see: CISA (no date), Vehicle Borne IED Identification: Parked Vehicles [webpage]. Available at: <https://www.cisa.gov/resources-tools/resources/vbied-identification-card> [accessed 13 May 2025].

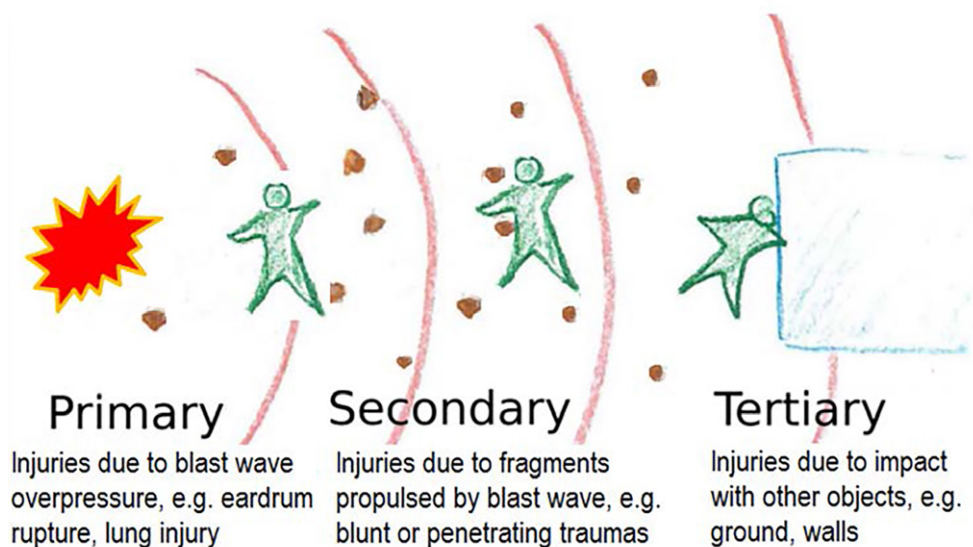
321 Karlos, V.; Larcher, M. (2020) *Guideline, building perimeter protection: Design recommendations for enhanced security against terrorist attacks*, Publications Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en> [accessed 13 May 2025].

There are specific limited measures that can mitigate a PBIED attack at a CI facility other than those covered in other sections of this *Technical Guide* such as stand-off distances, access control systems (including metal detection and security screening measures), and measures to mitigate explosive blasts. These are also covered in Chapter 6, Physical Security Measures.

Stand-off Distances

One measure to mitigate explosive threats to a CI site or building is to determine the minimum distance to be maintained between people and buildings and the explosive threat – often referred to as the stand-off distance. The stand-off distance is likely to change based on the size of an explosive charge, since its size impacts its destructive potential.

Mechanisms of Blast Injury



Used with permission of the European Commission's Joint Research Centre.³²²

³²² Publications Office of the European Union (2020), *A survey of computational models for blast induced human injuries for security and defence applications*. Available at: <https://publications.jrc.ec.europa.eu/repository/handle/JRC119310> [accessed 26 June 2025].

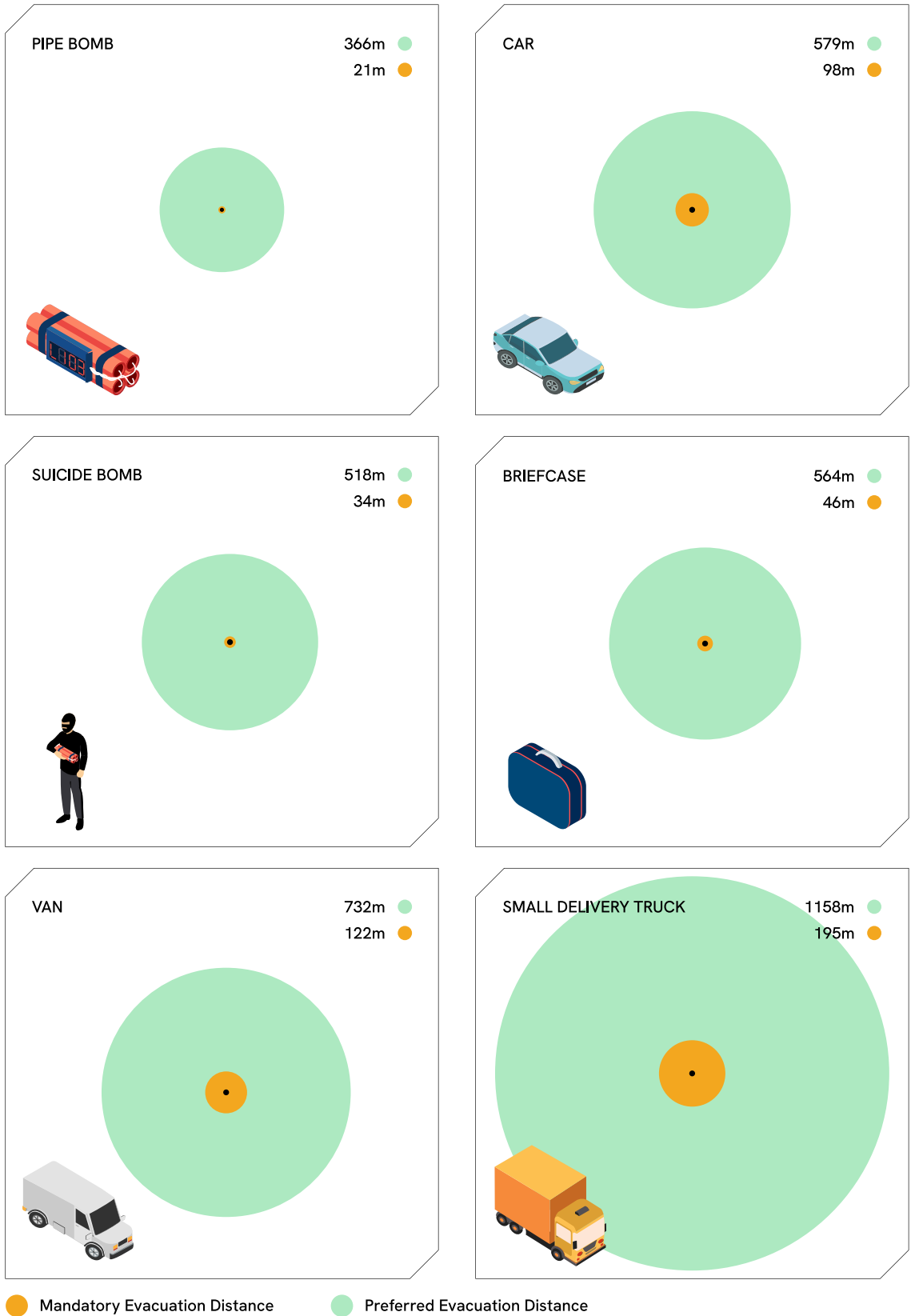
Understanding the explosive potential of vehicles based on size will help owners and operators assess the possible explosive force and determine appropriate parking standoff distances.³²³ In many national contexts, stand-off distances are recommended for a range of explosive device sizes, allowing CI owners/operators to align with this standardized approach. For example, the United Kingdom's ProtectUK Initiative recommends the following as minimum stand-off distances, however a range of up to one kilometre may have to be considered in specific circumstances:³²⁴



³²³ In this regard, a useful quick reference card can be found here: CISA (no date), DHS-DOJ Bomb Threat Stand-Off Card [webpage]. Available at: https://www.cisa.gov/sites/default/files/2025-03/Bomb%20Threat%20Stand-Off%20Card%20Digital%20Final%20v3.0_0.pdf [accessed 13 May 2025].

³²⁴ National Counter Terrorism Security Office, ProtectUK (no date), Purple Guide Chapter on Counter Terrorism - Attack Planning [webpage]. Available at: <https://www.protectuk.police.uk/purple-guide-chapter-counter-terrorism-attack-planning> [accessed 10 December 2024].

The United States' Joint Counterterrorism Assessment Team recommends the following preferred and mandatory stand-off distances, however a range of up to one kilometre may have to be considered in specific circumstances:³²⁵



325 Joint Counterterrorism Assessment Team (JCAT) (no date), JCAT Counterterrorism Guide for Public Safety Personnel. Available at: <https://www.dni.gov/nctc/jcat/references.html> [accessed 13 May 2025].

For vehicle-borne explosive threats, stand-off distance must be considered when designing roads, gates and parking spaces for vehicles within and around a CI site, since the explosive threat can move from place to place.

In cases where establishing a reasonable stand-off distance is not possible for an assessed explosive threat, it may be necessary to harden a facility's building structure to prevent collapse in the event of an explosion.

A stand-off distance must also be rapidly established by competent personnel at a CI site in the event of a suspicious item being identified. This is closely related to evacuation procedures for a CI facility, which should be well defined and exercised on a routine basis (for more information, see Chapter 9, Training and Exercising).

7.4 Security Planning for Chemical, Biological, Radiological, and Nuclear Attacks



Although a less common attack method than others explored in this chapter, the acquisition, weaponization and use of chemical, biological, radiological and nuclear (CBRN) materials by terrorist organizations has been a consistent threat to the public and CI facilities for decades. In the 2012 OSCE Consolidated Framework for the Fight Against Terrorism, the OSCE participating States identified the illicit movement of weapons and chemical, biological, radiological and nuclear materials as a focus area for the OSCE's work. This followed a 2005 OSCE Ministerial Council Decision on the threat of radioactive sources, which emphasized the "need to protect individuals, society and the environment from the harmful effects of possible accidents and malicious acts involving radioactive sources".³²⁶

³²⁶ OSCE (2005), Permanent Council Decision No. 683 (PC.DEC/683), Countering the Threat of Radioactive Sources. Available at: <https://www.osce.org/files/f/documents/0/e/15919.pdf> [accessed 13 May 2025].

The CBRN terrorist threat includes the weaponization of chemical agents, toxic industrial chemicals, biological agents, toxins, nuclear and radioactive materials. In 2021, terrorist use of chemical and biological materials was investigated by the United Nations. The United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh/Islamic State in Iraq and the Levant (UNITAD) reported:

“Evidence already secured indicates that ISIL [the Islamic State of Iraq and the Levant] tested biological and chemical agents and conducted experiments on prisoners as part of this programme, causing death. Weaponized vesicants, nerve agents and toxic industrial compounds are suspected to have been considered under the programme [...] With this material, the [UNITAD] Team has been able to identify repeated successful deployments of chemical weapons by ISIL against civilian populations between 2014 and 2016. Investigations into the successful development and use by ISIL of an indigenous chemical weapons capability may represent an unprecedented moment for accountability in modern conflict with respect to non-State actors.”³²⁷

Weaponized CBRN materials come in different shapes and sizes, and thus they present different challenges for CI owners/operators. Potential incidents include, but are not limited to:

- ▶ Detonation of an improvised radiological dispersal device;
- ▶ Detonation of an improvised nuclear device;
- ▶ Release of a biological agent as an aerosol;
- ▶ Release of a toxic chemical as a gas;
- ▶ Contamination of water or food supplies using hazardous chemical, biological or radiological materials;
- ▶ Delivery of a hazardous chemical, biological or radiological material in a letter or package.



³²⁷ UNSC (3 May 2021), Sixth report of the Special Adviser and Head of the United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh/Islamic State in Iraq and the Levant (S/2021/419). Available at: <https://documents.un.org/doc/undoc/gen/n21/104/70/pdf/n2110470.pdf> [accessed 13 May 2025].

Given the diverse delivery methods that are possible for weaponized CBRN materials, with regard to the *intentional* release of such materials, CI owners/operators may focus efforts on strengthening baseline physical security and access control measures, whilst ensuring that CBRN-specific measures are in place for high-risk parts of a facility, such as its mailroom and entrance/exit areas. Measures for the *unintentional* release of CBRN materials, such as a hazardous chemical spill, should also be considered as part of a CI facility's emergency planning; however, such measures are outside the scope of this *Technical Guide*.

In the end, the degree to which a CI owner/operator focuses on protection against CBRN attacks should be made in consultation with law enforcement and other competent authorities, which may have access to more relevant information and intelligence.

CBRN Materials and Facility Risk

Since access to CBRN materials represents a challenge for terrorist organizations, in some cases a CI facility's purpose and profile may increase its attractiveness to terrorist organizations. For example, if a CI facility stores toxic chemical substances on-site, their weaponization may be easier and thus the facility may be targeted for both the acquisition of materials and the site of an attack. The increased risk of terrorist attacks on chemical facilities led the United States to create the Chemical Facility Anti-Terrorism Standards, which took effect in 2007 and expired in 2023.³²⁸

In some cases, rather than target a CI facility for attack, terrorist organizations may cultivate insiders to help them acquire CBRN materials (for more information, see Chapter 8, Insider Threat Management). CI owners/operators may consider the attractiveness of their facility to a terrorist actor as part of the facility's risk assessment, with due consideration paid to potential access to CBRN materials.

³²⁸ CISA (no date), Chemical Facility Anti-Terrorism Standards (CFATS) Resources. Available at: <https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/cfats-resources> [accessed 12 December 2024].

National Practice: US Department of Homeland Security Chemical Facility Anti-Terrorism Standard's Risk-Based Performance Standards Guidance (2009)³²⁹

In 2007, the US DHS was granted regulatory authority over security at high-risk chemical facilities. As a result, regulations were developed that placed requirements on chemical facilities covered under Section 550 of the Homeland Security Appropriations Act of 2007. This included 18 risk-based performance standards (RBPSs) "that identify the areas for which a facility's security posture will be examined, such as perimeter security, access control, personnel surety, and cyber security. To meet the RBPSs, [owners/operators of facilities covered by the Act] are free to choose whatever security programs or processes they deem appropriate, so long as they achieve the requisite level of performance in each applicable area. The programs and processes that a high-risk facility ultimately chooses to implement to meet these standards must be described in the Site Security Plan that every high-risk chemical facility must develop pursuant to the regulations. It is through a review of the [Site Security Plan], combined with an on-site inspection, that [the DHS] will determine whether or not a high-risk facility has met the requisite levels of performance established by the RBPSs given the facility's risk profile."

Source: US DHS

Physical Measures

At least two categories of physical measures are relevant for a CI facility's protection against terrorist attacks using CBRN materials: CBRN detection equipment and air ventilation systems. This is based on the assumption that measures to address explosive attacks have been implemented at a given facility, since CBRN materials can be weaponized together with explosives.

If CI owners/operators or competent authorities assess a sufficient CBRN risk to a facility, they may deem it necessary to install detection equipment at specific locations inside and outside the facility perimeter (e.g., entrances/exits, mailrooms, loading docks, etc.). A determination of where to install this equipment should be made together with competent authorities. Since the level of risk from chemical terrorism is different from, for example, radiological terrorism, confirming a facility's need for detection equipment (including which materials it should detect) and selecting the appropriate supplier should be done in consultation with competent authorities. Equipment should be tested on a routine basis in line with guidance provided by authorities and the manufacturer's instructions.

³²⁹ CISA (May 2009), *Risk-Based Performance Standards Guidance: Chemical Facility Anti-Terrorism Standards*. Available at: https://www.cisa.gov/sites/default/files/publications/cfats-rbps-guidance_508.pdf [accessed 14 May 2025].

**National Practice: US National Institute for Occupational Safety and Health
Guidance for Protecting Building Environments from Airborne Chemical, Biological,
or Radiological Attacks³³⁰**

In 2002, guidance was released by the US National Institute for Occupational Safety and Health specifically to address terrorist attacks using chemical, biological, or radiological (CBR) materials on buildings and their occupants. The guidance, targeted at building owners and managers, provided specific recommendations in four different areas: (1) things not to do; (2) physical security; (3) ventilation and filtration; and (4) maintenance, administration and training. Examples of recommendations include:

- ▶ Preventing terrorist access to a targeted facility requires physical security of entry, storage, roof, and mechanical areas, as well as securing access to the outdoor air intakes of the building HVAC [heating, ventilation and air conditioning] system.
- ▶ Some physical security measures, such as locking doors to mechanical rooms, are low cost and will not inconvenience the users of the building. These types of measures can be implemented in most buildings. Other physical security measures, such as increased security personnel or package x-ray equipment, are more costly or may inconvenience users substantially. These measures should be implemented when merited after consideration of the threat and consequences of a terrorist attack.
- ▶ HVAC systems and their components should be evaluated with respect to how they impact vulnerability to the introduction of CBR agents. Relevant issues include the HVAC system controls, the ability of the HVAC system to purge the building, the efficiency of installed filters, the capacity of the system relative to potential filter upgrades, and the significance of uncontrolled leakage into the building.

Source: US National Institute for Occupational Safety and Health

CBRN materials weaponized by terrorists may be airborne and therefore appropriate air ventilation systems may be considered if CI owners/operators or competent authorities assess a sufficient CBRN risk. This includes both the ability of a system to filter hazardous particulates and the ability of CI owners/operators to rapidly reduce/shut down air ventilation in specific parts of a building. For example, given the risk of a CBRN material being introduced to a CI facility through its mailroom, the ability to immediately shut down air ventilation from this room to the rest of the facility may be important to reduce the spread of the CBRN material. In some cases, installing a separate air ventilation system for this room can be considered. CI owners/operators may wish to increase security measures around air intake sites, since they may be potential attack locations for a terrorist organization.

³³⁰ National Institute for Occupational Safety and Health (NIOSH) (no date), Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks [webpage]. Available at: <https://www.cdc.gov/niosh/engcontrols/ecd/detail147.html> [accessed 12 December 2024].

CBRN materials weaponized by terrorists may also be water-borne. Therefore measures aimed at controlling access to vital water supplies at a CI facility, monitoring water quality, and enabling the reliable and rapid identification of pathogens or other toxic substances in water supplies may be considered.³³¹

Preparing the Workforce

Given the diversity of CBRN materials and their varying impact on human beings, summarizing the exact indicators of exposure is challenging. However, there are some indicators that CI facility personnel should be aware of, as summarized by the UK NPSA:

“Unexplained physical symptoms such as: eye and skin irritation, twitching and convulsions, disorientation and sweating, airway irritation and breathing difficulties, nausea and vomiting.

“Other signs such as: two or more people incapacitated for no explainable reason, the presence of unusual/unattended materials, devices or equipment, unexplained vapour, mist clouds, powder, liquids or oily drops, unexplained smells or tastes, withered plant life or vegetation, distressed birds or animals.

“The onset of some symptoms can occur rapidly indicating that an attack is currently underway. In some circumstances, however, signs and symptoms may not appear for several days after an incident has occurred, and early symptoms could be mistaken for that of a common cold or flu.

“In these instances, monitoring staff sickness patterns to identify abnormalities, for example a large number of staff off sick, can help to identify these incident types.”³³²

This last sentence is worth highlighting, since it may not be immediately evident to CI facility personnel why their security focal points need to know about health matters. Without reporting the health status of personnel on a routine basis to a facility security focal point, it is challenging to identify patterns that may indicate an ongoing CBRN attack. This involves a larger discussion on the protection of the personal information of CI facility personnel and may require consultation with competent authorities.

Mailrooms of CI facilities can be the first location where chemical or biological materials such as anthrax are delivered, and thus mailroom personnel should be aware of how to respond to such threats. CI owners/operators can provide routine training to such personnel, and develop quick reference posters for mailrooms with clear and concise instructions for responding to incidents involving suspicious items.

331 Theocharidou, M.; Giannopoulos, G. (eds.) (2019), *JRC Technical Reports: Guidance on the production of a water security plan for drinking water supply* (Luxembourg: Publications Office of the European Union). Available at: https://erncip-project.jrc.ec.europa.eu/sites/default/files/2019.4805_EN_JRC116548.pdf [accessed 14 May 2025]; Coelho, M.R.; Batlle Ribas, M.; Coimbra, M.F. (2020), *JRC Technical Reports: Review of technologies for the rapid detection of chemical and biological contaminants in drinking water* (Luxembourg: Publications Office of the European Union). Available at: https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC119994_2020.1117_en_jrc119994.pdf [accessed 14 May 2025].

332 NPSA (2024), *Preparing and Responding to a Chemical, Biological or Radiological (CBR) Incident: A guide for Security Managers to reduce the impact of a CBR incident*. Available at: <https://www.npsa.gov.uk/resources/official-cbr-security-managers-guide> [accessed 14 May 2025].

National Practice: ProtectUK Mail Handling Guidance for Publicly Accessible Locations (2022)³³³

Avoid unnecessary handling and X-raying:

If you are holding the item, put it down on a cleared flat surface and:

- ▶ keep it separate so it is easily identifiable
- ▶ do not move it, even to x-ray
- ▶ if it is in an x-ray facility, leave it there

Move away immediately:

- ▶ clear the immediate area and each adjacent room, including rooms above and below
- ▶ if there is any suggestion of chemical, biological or radiological materials, move those directly affected to a safe location close to the incident, keep these individuals separate from those not involved
- ▶ prevent others approaching or accessing the cleared areas
- ▶ do not use mobile phones or two-way radios in the cleared area or within fifteen metres of the suspect package
- ▶ communicate regularly with staff, visitors and the public

Notify the police:

- ▶ if the item has been opened, or partially opened prior to being deemed suspicious, it is vital that this is communicated to the police
- ▶ and make sure informants and witnesses remain available to brief the police, and that the accuracy of their observations is preserved. Encourage witnesses to immediately record their observations in writing, and discourage them from discussing the incident or their observations with others prior to the arrival of the police

Additional CBR-specific actions:

- ▶ if a CBR incident is suspected, then undertake improvised decontamination of contaminated individuals as quickly as possible, ideally within the first 15 minutes
- ▶ in the event of a CBR incident occurring it is advised that lifts should not be used in order to move around, or evacuate the building
- ▶ if the alteration of the [heating, ventilation, and air conditioning] system features within your response plan [...], this should be undertaken as quickly as possible

Source: UK National Counter Terrorism Security Office

An additional and critical component for preparing the workforce at a CI facility is ensuring adequate and available stockpiles of suitable personal protective equipment.

CBRN-specific Crisis Management Planning

CI owners/operators may wish to integrate CBRN-specific incidents into their crisis management planning, since a terrorist attack involving CBRN materials is fundamentally different from a terrorist attack using firearms or an explosive device.

³³³ National Counter Terrorism Security Office, ProtectUK (1 March 2022), Venues and Public Spaces (VaPS) guidance. Mail handling [webpage]. Available at: <https://www.protectuk.police.uk/mail-handling> [accessed 12 December 2024].

As a result, crisis management plans (including evacuation, invacuation or shelter in place plans) that have been prepared for other forms of terrorist attack may not be applicable to an incident involving CBRN materials. As an example, if a toxic chemical gas is released on the ground floor of a CI facility, using an elevator to escape to upper floors may create an effect in which the hazardous gas is pulled into upper floors.³³⁴ This contrasts with the use of an elevator during an active shooter incident, when it may be advisable to use an elevator as a means to escape the threat on a particular floor. To support decision-making in this regard, atmospheric dispersion modelling for attacks using CBRN materials may be useful. Moreover, if specific measures for invacuation or shelter in place are deemed necessary for a CBRN attack, personal protective equipment should be readily available for personnel.

When examining facility risk to terrorist attacks using CBRN materials, one factor worth consideration is that a CBRN attack can create mass casualties (either immediately or delayed). If successfully deployed, an attack using a noxious chemical gas or biological agent could, in a short period of time, overwhelm a facility's medical capacity and local emergency services. Preparing for such a threat, if deemed necessary by CI owners/operators and competent authorities, requires close and co-ordinated involvement of emergency services and first responders as part of routine CBRN-specific crisis exercises.

334 NPSA (2024), *Preparing and Responding to a Chemical, Biological or Radiological (CBR) Incident: A guide for Security Managers to reduce the impact of a CBR incident*. Available at: <https://www.npsa.gov.uk/resources/official-cbr-security-managers-guide> [accessed 14 May 2025].

National Practice: ProtectUK Guidance on Chemical, Biological and Radiological Attacks for Publicly Accessible Locations (2022)³³⁵

Good general physical and personnel security measures will help to reduce CBR incidents. Apply appropriate personnel security standards to contractors and visitors, especially those with frequent access to your site.

Full CBR protection can be extremely expensive to implement, however, some measures that will help reduce the effects of a CBR event, can be put in place at relatively low cost.

The following first steps are recommended to increase resilience to a CBR attack:

- ▶ review the physical security measures relevant to areas of a building that due to their function, such as entrances, exits and windows may be at increased risk of attack
- ▶ review the design and physical security of air-handling systems, such as access to intakes and outlets, avoiding the use of ground level, or near ground level air intakes
- ▶ ensure CBR response is featured into the site's major incident plans
- ▶ consider evacuation routes
- ▶ consider the use of pre-prepared messaging
- ▶ improve air filters or upgrade your air-handling systems, as necessary
- ▶ restrict access to water tanks and other key utilities
- ▶ review the security of your food and drink supply chains
- ▶ consider whether you need to make special arrangements for mail or parcels such as a separate post room, possibly with dedicated air-handling, or even a specialist off-site facility aware that mail rooms can be a high-risk area

Source: UK National Counter Terrorism Security Office

7.5 Security Planning for Firearms Attacks

Terrorist attacks using firearms have occurred throughout the world and require similar responses, irrespective of country. Often referred to as marauding terrorist firearm attacks or active shooter attacks, these are fast-moving incidents in which assailants armed with firearms (and sometimes explosive devices) move through a facility or site with a range of aims, including to kill or injure as many persons as possible or to access specific locations.³³⁶ Terrorist attacks using firearms can range from a lone individual to a group. This poses a broad range of challenges to a CI site. Since firearms are often readily available, do not require complex supply chains or extensive technical expertise (as opposed to CBRN weapons or IEDs), and require limited training to operate, they remain a common modus operandi for terrorist organizations and other threat actors.

³³⁵ National Counter Terrorism Security Office, ProtectUK (1 March 2022), Venues and Public Spaces (VaPS) guidance Chemical, Biological and Radiological (CBR) attacks [webpage]. Available at: <https://www.protectuk.police.uk/chemical-biological-and-radiological-cbr-attacks> [accessed 12 December 2024].

³³⁶ Definition adapted from the NPSA (June 2023), Introduction to the Marauding Terrorist Attack Standard (MTAS). Available at: <https://www.npsa.gov.uk/resources/introduction-marauding-terrorist-attack-standard-mtas> [accessed 14 May 2025].

In some cases, the guidance in this section is more closely related to responding to a firearms attack, rather than enhancing the physical security of a facility to this threat. While this may go beyond physical security considerations, response planning is nevertheless part of an effective security framework for any CI facility.³³⁷



Pre-attack Measures

Measures can be taken by CI owners/operators to better prepare a CI site for terrorist attacks using firearms or even deter threat actors from carrying out such an attack. Measures include, but are not limited to:

- ▶ Establishing a video surveillance system for the site's premises, which is useful for identifying suspicious people, including those conducting pre-attack hostile reconnaissance;
- ▶ Building a security culture among all personnel, including through training and routine briefings involving local emergency services and law enforcement;
- ▶ Conducting routine patrols around (if allowed by national and local laws) and within the site;
- ▶ Applying access control measures and security screenings;
- ▶ Where necessary, enhancing the physical security of windows, doors, shutters and blinds to resist a forced entry and gunfire;
- ▶ Considering measures that allow competent personnel to secure or lock down critical parts of a CI site or building, measures that can either prevent access to threat actors or confine them, allowing personnel to escape;
- ▶ Identifying evacuation routes for every building on a CI site. Each facility should have at least two evacuation routes;

³³⁷ See also: *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* published by UNOCT, the UNSC Counter-Terrorism Executive Directorate, the UN Institute for Disarmament Research, and the UN Global Counter-Terrorism Coordination Compact.

- ▶ Implementing two different types of alarms and associated procedures at a CI site: one for safety matters (such as an evacuation due to fire) and one for security matters (such as an active shooter or external attack);
- ▶ Conducting routine exercises for all personnel, involving local emergency services and law enforcement, that simulate a terrorist attack using firearms so facility personnel are aware of evacuation/invacuation/lockdown procedures;
- ▶ Encouraging/inviting local emergency services and law enforcement to provide training in responses to terrorist attacks using firearms at the CI site;
- ▶ Developing a plan for the CI site and its personnel in the event of a terrorist attack using firearms.

National Practice: US CISA Active Assailant-Shooter Emergency Action Plan Product Suite (2025)³³⁸

In 2025, CISA developed an Active Assailant Emergency Action Plan Template and associated Instructional Guide “to help critical infrastructure organizations and venues develop a comprehensive and implementable EAP [emergency action plan]. This resource provides guidance to assist users with completing each section of CISA’s EAP Template, and includes examples and additional resources for developing an effective plan”. The Instructional Guide includes steps to prepare for active assailant shooter incidents such as, *inter alia*, defining the key roles and responsibilities of an emergency action planning team at a CI facility, developing and sharing facility floor plans with personnel and first responders, enacting facility emergency access preparedness measures (such as inviting local law enforcement and first responders to participate in annual facility visits), defining evacuation, lockdown and shelter-in-place procedures, designing business continuity plans, and planning for the post-incident recovery period.

Source: US DHS CISA

Preparing the Workforce

In addition to taking proactive measures to both deter and prepare for a terrorist attack using firearms, communicating appropriate behaviour to personnel in the event of an attack is necessary. In a crisis situation, many facility personnel – in particular those with limited experience dealing with emergencies – may not be able to think or act clearly, which could endanger them and/or their colleagues. In order to support effective decision-making during terrorist attacks, many OSCE participating States have developed succinct awareness-raising campaigns for the general public. CI owners/operators may wish to adapt these campaigns and use them for their facility personnel:

338 CISA (2023), *Security Planning Workbook*. Available at: <https://www.cisa.gov/resources-tools/resources/security-planning-workbook> [accessed 14 May 2025]; CISA (2025), Active Assailant-Shooter Emergency Action Plan Product Suite [webpage]. Available at: <https://www.cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite> [accessed 14 May 2025].

- ▶ US DHS campaign: Run, Hide, Fight;³³⁹
- ▶ France's Vigipirate campaign: Escape, Hide, Warn, Fight, Facilitate Access for Law Enforcement and Emergency Services;³⁴⁰
- ▶ UK National Counter Terrorism Security Office campaign: Run, Hide, Tell.³⁴¹

Post-attack Measures

Planning for a terrorist attack using firearms should focus heavily on ways to prevent and prepare for such attacks. Nonetheless, attention should also be paid to the immediate- and longer-term impacts of an attack on CI facility personnel and their families. The management of these impacts should form part of any emergency plan developed for a CI facility. Particular measures of note include:

In the immediate aftermath of an attack:	▶ An accounting of all personnel at a designated CI facility assembly point to determine who, if anyone, is missing and potentially injured. ▶ Determining a method for notifying families of personnel affected by the attack, including notification of casualties.
Days, weeks and months after an attack:	▶ Conducting assessments of the psychological state of personnel involved in the attack (including those who were not present but may be suffering from grief, loss or survivor's guilt) and referring them to appropriate medical and psychological specialists, if needed. ▶ Identifying and filling critical personnel positions or operational gaps created by the attack. ▶ Developing a communications strategy which openly identifies security failures in the attack and communicates concrete improvements being made, with senior level support.

7.6 Security Planning for Hostage Situations

Terrorist organizations and other threat actors can use hostage-taking as part of an attack on CI in order to gain leverage and draw attention to their demands. CI sites often hold high strategic and symbolic value. By taking hostages at these locations, threat actors may seek to force governments or CI owners/operators into negotiations, creating a sense of urgency due to the potential for loss of life and/or disruption of critical services. Hostage-taking can draw media attention and solicit a range of emotions from the general public. Public pressure to ensure the safety of the hostages and to prevent further damage can mount, resulting in pressure on authorities/stakeholders to meet demands or concede to some form of negotiation. As a result, considerable international attention has been given to the issue of hostage-taking.

339 CISA (2022), Active Shooter Pocket Card. Available at: <https://www.cisa.gov/resources-tools/resources/active-shooter-pocket-card> [accessed 14 May 2025].

340 Secrétariat général de la défense et de la sécurité nationale (SGDSN), *Guide des Bonnes Pratiques pour la Sécurité des Espaces Publics*. Available at: <https://www.sgdsn.gouv.fr/files/files/Publications/guide-unique-de-sensibilisation-vigipirate-pact-num-v7.pdf> [accessed 14 May 2025] unofficial translation.

341 National Counter Terrorism Security Office, ProtectUK (2 September 2021), Run Hide Tell. Available at: <https://www.protectuk.police.uk/sites/default/files/2023-12/Marauding%20Attacker%20Action%20Card.pdf> [accessed 14 May 2025].

International Convention against the Taking of Hostages

The International Convention against the Taking of Hostages was adopted by the United Nations General Assembly in 1979 through A/RES/34/146 and entered into force in 1983. At present, it has 39 signatories and 176 Parties.³⁴² The Convention defines the offences of hostage-taking, attempted hostage-taking, and complicity in hostage-taking. In line with Article 1 Paragraph 1, the offence of hostage-taking is committed by: "Any person who seizes or detains and threatens to kill, to injure or to continue to detain another person [...] in order to compel a third party, namely, a State, an international intergovernmental organization, a natural or juridical person, or a group of persons, to do or abstain from doing any act as an explicit or implicit condition for the release of the hostage."³⁴³

Hostage-taking is a unique form of attack and has been used by terrorist actors against CI facilities. While the focus of this *Technical Guide* is physical security measures, this section extends beyond such physical measures to provide general guidance on effective measures and considerations for preparing for and responding to hostage situations.

Given the sensitive nature of this topic, there are a limited number of good practices that are publicly available. The actions required in any given hostage-taking situation are also context specific. However, since hostage-taking is a viable threat to the security of CI facilities and their personnel, general guidance and considerations are presented in this section to guide decision makers as they plan for this type of attack.

Case Study: Al-Qaeda-linked Terrorist Attack and Hostage-taking at the In Amenas Gas Facility, Algeria (2013)³⁴⁴

On 16 January 2013, a terrorist attack involving hostage-taking occurred at the Tiguentourine gas plant in In Amenas, Algeria. The In Amenas gas development was operated as a joint venture between the Algerian national oil company, Sonatrach, British Petroleum and Statoil. At the time of the attack, 800 people were working at the facility, 130 of whom were non-local personnel from 30 different countries. The attack involved 32 well-armed terrorists and lasted several days, beginning with attacks on a bus and its escort convoy 300 metres from the facility's living area, followed by simultaneous attacks on the facility's living and gas production areas. The facility fell under the control of the terrorists within 15 minutes.

Throughout the course of the multi-day attack, the terrorists communicated with both Statoil and British Petroleum and communicated several demands, including the release of well-known prisoners in US and Algerian prisons. After several days, 40 innocent people had been murdered, and 29 of the 32 terrorists had died.

³⁴² United Nations, International Convention Against the Taking of Hostages. Available at: https://treaties.un.org/doc/Treaties/1979/12/19791218%2003-20%20PM/Ch_XVIII_5p.pdf [accessed 14 May 2025].

³⁴³ United Nations, International Convention Against the Taking of Hostages. Available at: https://treaties.un.org/doc/Treaties/1979/12/19791218%2003-20%20PM/Ch_XVIII_5p.pdf [accessed 14 May 2025].

³⁴⁴ Statoil (2013), *The In Amenas Attack. Report of the investigation into the terrorist attack on In Amenas. Prepared for Statoil ASA's Board of directors*. Available at: <https://www.equinor.com/news/archive/2013/09/12/downloads/In%20Amenas%20report.pdf> [accessed 14 May 2025].

By 17 January, the Algerian military had retaken control of the facility. Many of the surviving hostages suffered not only physical injuries, but also psychological consequences because of their experience.

Following the attack, official investigations and inquiries took place, each seeking to establish recommendations that would enhance understanding and influence future preparedness and subsequent response to similar attacks. The following are select observations from an investigative report prepared for Statoil's Board of Directors:

- ▶ **Layered Security:** Expert investigators reinforced the importance of applying a holistic approach to security at the In Amenas facility, ensuring each layer of protective security affords opportunities to (1) detect that an attack is underway, (2) delay the attackers, and (3) provide sufficient time to implement a response before the attackers have time to cause more harm. This included recommendations to:
 - a. include basic security training for all employees at the facility and specialized security training for managers and international personnel, and
 - b. to openly and clearly communicate potential security risks to employees at a facility, with mutual expectations defined between the operator and their personnel.
- ▶ **Testing and Exercising:** Expert investigators encouraged those responsible for the security of the facility to test and exercise security-related plans more frequently and co-ordinate/standardize emergency response planning across all business areas.
- ▶ **Risk Management and Assessment:** Expert investigators recommended the development of a dynamic and fit-for-purpose security risk management system. Moreover, they called for the maintaining of security risk management plans that include defined security-related scenarios.

Source: Statoil

Preparing for Hostage Situations at Critical Infrastructure Facilities

CI owners/operators should prepare for hostage situations at their facilities in order to protect both the safety and security of personnel and the facility's critical services. The following are several high-level considerations that may be taken as part of this process:

Ensuring Advanced Preparedness: One aspect of preparedness in this context is assessing the likelihood of such an incident taking place. Such an assessment may be conducted by CI owners/operators as part of their risk management process. For example, the United Kingdom maintains a National Risk Register that references "Strategic Hostage Taking", including by terrorists.³⁴⁵ This National Risk Register assesses both the impact and likelihood of such events, enabling CI owners/operators to plan and prepare security measures, crisis response plans, and training for personnel in order to manage such events, respond swiftly to threats, and minimize harm. Where this form of national guidance is unavailable, CI owners/operators may wish to assess the likelihood of a hostage situation taking place at their facility in co-ordination with law enforcement.

³⁴⁵ HM Government (2023), *National Risk Register: 2023 Edition*, pp. 39–40. Available at: https://assets.publishing.service.gov.uk/media/64ca1dfe19f5622669f3c1b1/2023_NATIONAL_RISK_REGISTER_NRR.pdf [accessed 14 May 2025].

Establishing Security Measures for Hostage Situations: To facilitate rapid and subtle communication among personnel in the run-up to a hostage situation, the implementation of a code word and establishment of a designated place of safety within a CI facility specific for hostage situations is considered good practice. Code words act as a discreet alert for individuals within a facility. When someone is in distress or suspects a hostage situation is in progress, the code word can be communicated subtly to warn others without escalating the situation or drawing attention to the threat. It is critical that the code word be easy to remember and distinct enough from everyday conversation to minimize confusion. All facility personnel should be informed about the code word, its significance, and the appropriate procedures to follow when it is used.

In tandem with a code word, a designated place of safety – often referred to as a “safe haven” or “citadels” in the maritime sector³⁴⁶ – should be established within the premises. This location should be secure, easily accessible and physically hardened against potential threats. The safe haven should accommodate individuals seeking refuge and provide means for communication with law enforcement or emergency services. For enhanced effectiveness, the safe haven may be equipped with basic necessities such as first aid kits, emergency supplies and communication devices. Depending on the advice of competent CI facility personnel, this “safe haven” may be the same room as an invacuation assembly point described later in this chapter. However this may not always be the case, since they serve different objectives.

Building a Security Culture Among Personnel: The ability of a CI facility’s personnel to identify and recognize potential threats, including an evolving attack that may lead to a hostage situation, is a key part of effective preparedness. Personnel at a CI facility should be encouraged to stay vigilant and report any suspicious activity to designated security focal points.

Organizing Training for Personnel: Building the skills of CI facility personnel to effectively respond to high-pressure situations such as a hostage situation increases their familiarity with the subject and reduces panic. Regular training and exercises for all CI facility personnel are crucial to ensure everyone understands, among other things, the designated code word and their route to the safe location(s). For larger facilities, identifying multiple safe zones increases options for personnel trying to avoid danger.

Responding to and Managing Hostage Situations

The response to a hostage situation should prioritize the preservation of life. Other goals include resolution of the incident with minimal force, and gathering intelligence on the captors’ motives, if they have not already been made evident. In most hostage situations at a CI facility, government authorities will be involved and will lead the response. However, there may be situations in which government authorities are unavailable or en route (as for example, in the case of remote oil and gas installations). Therefore, CI owners/operators may be closely involved in the immediate response and management of a hostage situation and thus should be adequately prepared. However, any engagement in the response to and management of hostage negotiations at a CI facility

³⁴⁶ Baltic and International Maritime Council (BIMCO) et al. (2018), Global Counter Piracy Guidance for Companies, Masters and Seafarers (Livingston: Witherbys Publishing Group). Available at: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/global-counter-piracy-guidance-bmp_low_17-07-18.pdf [accessed 14 May 2025].

by a CI owner/operator should be co-ordinated and agreed upon with local authorities. The following are several high-level considerations as part of this process:

Engaging in Crisis Negotiation: Crisis negotiation is a critical component of managing hostage situations. It involves trained negotiators engaging with captors. The process is nuanced and requires enhanced skills in communication, empathy and persuasion. Effective negotiators build rapport with captors, gather key details (including information about demands, condition of the hostages, or the hostage-takers' state of mind – aspects that can influence the response by authorities as well as the actions of the hostage-takers), and aim to de-escalate tensions. Useful techniques include:

- ▶ *Active Listening:* Demonstrating understanding and concern can help build trust;
- ▶ *Creating a Dialogue:* Open-ended questions encourage captors to express their motives;
- ▶ *Offering Options:* Instead of ultimatums, negotiators may suggest possible solutions that satisfy the captor's needs while ensuring hostages' safety.

Preparing for Tactical Engagement: While negotiation is essential, there are situations in which tactical intervention by competent authorities may be required. This typically extends beyond the authority of CI owners/operators and is more relevant for local authorities and law enforcement. Tactical teams from competent authorities will likely be trained to execute rescue operations when negotiations fail or if hostages are in imminent danger. Tactical teams may work with CI owners/operators to gather real-time information on the CI facility's layout, hostage(s) location, number of captors and conditions of the hostages, as well as determining when to act. In such cases, it is important for CI owners/operators to provide the requested information to the best of their abilities, providing tactical teams and other relevant actors with a reliable foundation for their work.

Ensuring Psychological Support: Both during and after a hostage incident, recognizing the psychological impact on hostages and their families is key. After an incident, hostages may experience trauma. For this reason, psychological support may be integrated into the response by competent authorities and a CI owner/operator, including providing medical attention and mental health evaluations to hostages immediately upon their release, and ensuring effective communication with the families of hostages throughout the event. This latter point helps maintain the emotional stability of those involved. When appropriate, these services may also be provided to other affected personnel.

Conducting Post-Incident Analysis: After the resolution of a hostage situation, conducting a thorough analysis is essential to understand the effectiveness of the response. There will be a clear division between the competencies of the CI owner/operator and the competent authorities involved. This review may include the negotiation and tactical strategies employed, the psychological support given, and areas for improvement in future responses. Additionally, a post-incident analysis can highlight unforeseen challenges and evolving threat patterns, ensuring that future training incorporates these insights, thereby enhancing preparedness and reducing the likelihood of similar incidents occurring in the future.

7.7 Planning for Invacuation, Evacuation and Lockdowns

In the event of an active threat to a CI facility, ensuring the safety and security of personnel should be the highest priority. In these situations, there are three options for personnel: evacuation, invacuation or lockdown (shelter in place).



Evacuation



Invacuation



Lockdown / Shelter in place

Evacuation is the process of moving personnel outside a building or site, away from an active threat. Invacuation is the process of moving personnel inside a building or site, away from an active threat. In certain circumstances, it may be safer to “invacuate” personnel to a secure location within a facility than to evacuate them outside. One potential scenario where this could apply is when an explosive threat is outside the CI building or site, with the possibility of secondary devices. In this scenario, evacuating personnel outside and putting them in range of the explosive threat (including broken glass and other shrapnel that could be produced in the explosion) could be more dangerous than keeping them inside. A lockdown is when all personnel are to remain inside a room or building for a temporary period of time, with the intention of keeping safe from an active threat. This may be the most effective course of action, as for example, in the event of a terrorist attack using firearms in which armed actors are moving through a CI building or site.

All terms describe the same objective: keeping personnel away from a dynamic threat. For the purposes of this *Technical Guide*, the terrorist threat is paramount and encompasses armed shooters, as well as vehicular, explosive or CBRN threats. Evacuation/invacuation measures are not strictly limited to terrorist threats; they are also routinely considered for fires, earthquakes, floods and unintentional incidents (power outages, etc.).

Planning for Evacuation

To prepare personnel at a CI facility for an evacuation situation, an evacuation plan should be developed, exercised with all personnel, and co-ordinated in advance with local law enforcement, local emergency services, local government bodies and, if relevant, nearby facilities (as for example schools or shopping malls). To ensure that rapid decisions can be made based on the situation, an evacuation plan should define who within a CI site decides to call for an evacuation. In many cases, the decision to evacuate will be made by a CI facility’s senior management, in consultation with law enforcement.

One dilemma facing those who have responsibility for an evacuation decision in the context of a terrorist threat is judging what constitutes a place of safety, a task that is difficult to define in plans since terrorist threats are often dynamic. In some cases, evacuation may be the riskier course to take if, for example, an evacuation route takes personnel past a suspicious item outside the building. For explosive threats, it is important to recall the stand-off distances covered earlier in this *Technical Guide*. The United Kingdom's ProtectUK Initiative recommends:³⁴⁷

Cordon Distance	Suspicious Item
100 metres	Bag/suitcase
200 metres	Car
400 metres	Large vehicle

The United States Joint Counterterrorism Assessment Team recommends:³⁴⁸

Mandatory Evacuation Distance	Preferred Evacuation Distance	Suspicious Item
21 metres	366 metres	Pipe bomb
34 metres	518 metres	Suicide bomb
46 metres	564 metres	Briefcase
98 metres	579 metres	Car
122 metres	732 metres	Van
195 metres	1,158 metres	Small delivery truck

The evacuation plan should determine in advance which personnel will remain on-site or at their posts in order to maintain critical services.

An evacuation plan should define evacuation routes to guide personnel to a facility's exit or area of relative safety. All evacuation routes and exits should be clearly marked. Exit routes should always remain clear of furniture, debris or other items, and emergency exit signs should be regularly checked to ensure they are working. People with disabilities should be consulted when designing exit routes, including favouring routes that have ramps over stairs where appropriate, and considering how personnel in wheelchairs, for example, will be able to travel down stairs when elevators are disabled. Wherever practicable, a list of those within the facility should be available at defined assembly points to help identify missing people.

³⁴⁷ National Counter Terrorism Security Office, ProtectUK (no date), Purple Guide Chapter on Counter Terrorism - Attack Planning [webpage]. Available at: <https://www.protectuk.police.uk/purple-guide-chapter-counter-terrorism-attack-planning> [accessed 10 December 2024].

³⁴⁸ Joint Counterterrorism Assessment Team (JCAT) (no date), Respond & Mitigate: Bomb Threat Standoff Distances [webpage]. Available at: <https://www.dni.gov/nctc/jcat/references.html> [accessed 10 December 2024].

CI facility assembly points are typically defined for various emergencies (such as fire or earthquake) and as a result are usually close to buildings or in an open/unprotected space. However, terrorist threats to a CI facility require a different set of considerations. For example,

- ▶ The assembly point for an evacuation prompted by an explosive threat should take into consideration the proximity of the explosive device and its size, and incorporate target hardening measures.
- ▶ A terrorist may use his/her knowledge of existing fire assembly points to detonate an explosive device within the crowd of evacuated personnel.

Since the nature of terrorist threats is inherently dynamic and unique, an assessment should be made at the time of evacuation and a decision taken as to whether the facility's defined assembly points should be used.³⁴⁹ Those planning evacuations should also have pre-defined alternate routes and exits. When feasible, and in the event a pre-defined evacuation route is unavailable and an alternative must be found, a sweep of the proposed alternative evacuation route and assembly point should be made to ensure that no explosive devices are present. An example of a potential explosive threat would be a vehicle parked in close proximity to a defined assembly point.

Once an evacuation is completed and the threat is no longer present, a decision will need to be taken regarding when personnel can re-occupy the building(s)/site. When the decision is taken, personnel may be instructed to check their own work areas to ensure that there is nothing suspicious still present. If anything suspicious is found, personnel should be informed of whom to notify.

Is evacuating for terrorism different?

CI facility personnel are likely to be familiar with the principles and practices of evacuations due to fire or earthquakes. However, in the event of a terrorist attack, the appropriate response may be to not evacuate, and thus the evacuation response will differ from that to a fire. For example, personnel may be directed to specific exits or to avoid a particular route or area. For this reason, it is important to avoid activating the same alarm for a terrorist threat and a fire to reduce the possibility of an incorrect response. If this is not feasible, then measures should be taken to inform personnel of the nature of the evacuation. This may be accomplished through a public address system, automated text or email messages, or the placement of competent personnel along the defined exit routes to inform evacuating personnel.

Planning for Invacuation

If a terrorist threat is outside a building or site, it may put personnel in danger if an evacuation route brings them into close proximity to the threat (be it a suspicious item, a CBRN-contaminated environment, or an active shooting attack). A safer alternative may be to invacuate personnel. Invacuation is the process of moving personnel inside a building or site, away from an active threat.

³⁴⁹ BaMaung, D.; Bergin, G.; Byrne, J.; Garrett, D.; Harrison, A.; Maples, L.; Quinn, L. (2022), *Terrorism and Countermeasures, Version 2*. (Naas, Co. Kildare: The Security Institute of Ireland).

Any evacuation plan should consider a scenario in which invacuation is necessary. The identification of invacuation assembly points should be defined in advance and selected with due consideration to the range of terrorist threats covered in this *Technical Guide*, since each may impact the selection process.

Considering that invacuation takes place within a building or structure, selected spaces will likely need ventilation and access to air, toilets, drinking water, emergency lighting, first aid equipment, and communications equipment.³⁵⁰

National Practice: United Kingdom's ProtectUK Guidance on Invacuation including to Protected Spaces (2022)³⁵¹

Protected spaces should be located:

- ▶ in areas surrounded by full-height masonry walls, e.g. internal corridors, toilet areas or conference rooms with doors opening inwards.
- ▶ away from windows and external walls.
- ▶ away from the area in between the building's perimeter and the first line of supporting columns (known as the "perimeter structural bay").
- ▶ away from stairwells or areas with access to lift shafts which open at ground level onto the street. This is because if compromised, a blast could travel up them. However, if the stair and lift cores are entirely enclosed, they could make good protected spaces.
- ▶ avoiding the ground floor or first floor if possible.
- ▶ in an area with enough space to contain the occupants.

Source: UK National Counter Terrorism Security Office

Planning for Shelter in Place/Lockdowns

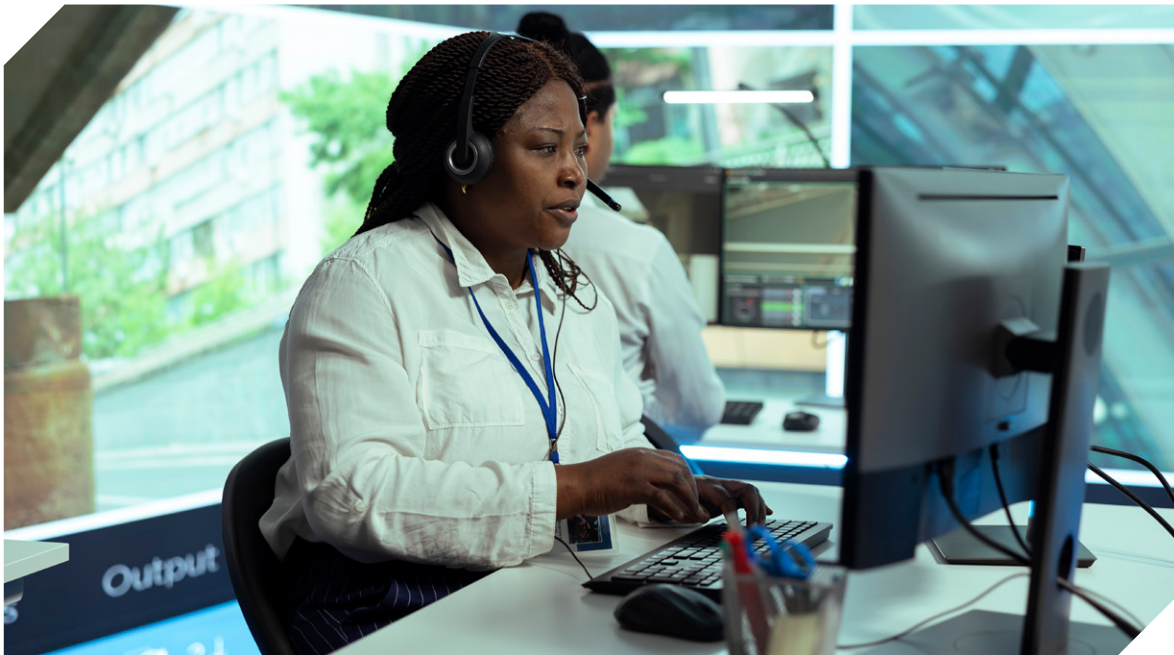
In the event of a terrorist attack using firearms where armed actors are moving through a CI building or site, the most effective course of action may be to ask all personnel to lockdown, or shelter in place. A lockdown order from competent CI facility personnel may also be given in the event an active threat is near the CI facility. This eventuality should be considered and described in a CI's emergency plans. In this type of event, personnel should be able to quickly restrict entrances and exits to all or part of a facility through physical measures such as locking doors and drawing window blinds.

350 National Counter Terrorism Security Office, ProtectUK (2022), Venues and Public spaces (VaPS) guidance: Evacuation, invacuation, lockdown, protected spaces [webpage]. Available at: <https://www.protectuk.police.uk/evacuation-invacuation-lockdown-protected-spaces> [accessed 5 March 2024].

351 National Counter Terrorism Security Office, ProtectUK (1 March 2022), Venues and Public spaces (VaPS) guidance: Evacuation, invacuation, lockdown, protected spaces [webpage]. Available at: <https://www.protectuk.police.uk/evacuation-invacuation-lockdown-protected-spaces> [accessed 5 March 2024].

7.8 Business Continuity Management

As shown throughout this chapter, CI owners/operators must plan for a range of disruptive incidents, including various types of terrorist attack scenarios. Generally, many of these plans may be part of a broader business continuity management system, which can be seen in many of the practices identified in this *Technical Guide*. The Business Continuity Institute defines business continuity as a practice which “ensures that organizations can maintain their critical business functions during – and after – an incident has occurred”.³⁵² CI owners/operators are encouraged to consider implementing and maintaining a business continuity management system as part of their efforts to continue critical services and recover from disruptive incidents such as a terrorist attack.



The relevance of business continuity management is highlighted in the EU CER Directive’s Article 13 “Resilience measures of critical entities”:

“Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

- a. prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;
- b. ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls;

³⁵² The Business Continuity Institute, *What is business continuity?* [webpage]. Available at: <https://www.thebci.org/thought-leadership/what-is-business-continuity.html> [accessed 7 August 2025].

- c. respond to, resist and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;
- d. recover from incidents, duly considering business continuity measures and the identification of alternative supply chains, in order to resume the provision of the essential service;
- e. ensure adequate employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, setting up procedures for background checks in accordance with Article 14 and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications;
- f. raise awareness about the measures referred to in points (a) to (e) among relevant personnel, duly considering training courses, information materials and exercises.”³⁵³

Business continuity management systems are addressed in ISO 22301:2019. According to the ISO, this standard “provides a framework for organizations to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of, and ensure recovery from disruptive incidents.”³⁵⁴

7.9 Crisis Communications

The incidents explored thus far in this *Technical Guide* are all forms of crises at a CI facility: terrorist attacks using vehicles, explosives, firearms, CBRN materials, or hostage situations. Various aspects of preparing for these crises have been covered in-depth in previous chapters. However the importance of communications has yet to be addressed.

In the 21st century, information – including misinformation and disinformation – moves around the world instantaneously. In a crisis situation at a CI facility this can impact the safety and security of personnel, the response to a crisis, and/or its aftermath. Unless a CI owner/operator has considered crisis communications as part of their planning, preparation for and response to a terrorist attack and exercised these communications sufficiently, they may create additional issues, including reputational damage and unwanted media attention. For terrorist-related incidents specifically, reputational damage is a major concern. Such damage may be caused if the CI owner/operator handles the incident inappropriately.

353 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> [accessed 30 October 2024].

354 ISO (2019), *Security and resilience — Business continuity management systems — Requirements* (ISO Standard No. 22301:2019). Available at: <https://www.iso.org/standard/75106.html> [accessed 14 May 2025].



Crisis Communications Frameworks

Irrespective of the size of a CI facility, developing a crisis communications framework is vital for communicating effectively with facility personnel and the public during an evolving crisis situation. According to the United Nations Office of Counter-Terrorism, the goal of a crisis communications framework is “to be positioned as a leader in responding to the impact of [a] crisis, to build community resilience, to inform and engage, to drive the right behaviours”.³⁵⁵

National Practice: Canada’s Chamber of Commerce Business Resilience Network: Principles of Effective Crisis Communications³⁵⁶

- ▶ Communicate quickly – you always have something you can say.
- ▶ Establish timelines for communicating – tell media/stakeholders when they can expect to hear from you next; uncertainty can encourage them to look elsewhere for information.
- ▶ Halt other communications – in a crisis you should be communicating only about the crisis and your response to it. All other communications should be paused.
- ▶ Use all of your channels – audiences get information from different sources, use all of your channels to communicate a consistent message.
- ▶ Short and to the point – audiences are looking for information they can use to understand the situation, and evaluate your response. Get to the point quickly, and focus only on relevant content.

Source: Canada’s Chamber of Commerce Business Resilience Network

³⁵⁵ UN Counter-Terrorism Centre (UNCCT) (no date), *Crisis Communication*. Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/final_crisis_communication_toolkit_20042023.pdf [accessed 14 May 2025].

³⁵⁶ Canadian Chamber of Commerce (no date), *Crisis Communications Planning Guide*. Available at: https://chamber.ca/wp-content/uploads/2020/07/Guide_CrisisCommunicationsPlan.pdf [accessed 14 May 2025].

The framework should include the establishment of a cross-disciplinary crisis communication team that would be activated as needed to direct pre-defined relevant communication tasks specific to an ongoing crisis. The framework may provide a structure for, among other things, development and dissemination of crisis communications messaging templates, development of a crisis communications plan, monitoring of media coverage, analysis of public perception, assessment of the crisis' public relations impact, a schedule for exercising the communications aspect of crisis situations, and the post-crisis evaluation process.³⁵⁷ Preparations should also be made in the event of a public enquiry into the CI owner/operator's handling of the crisis situation.

**Practice: United Nations Office of Counter-Terrorism Crisis Communications Toolkit:
Crisis Communication Framework³⁵⁸**

Stage	Objectives	Strategic Actions
Stage I: Activation	1. Deliver the facts and allay fear 2. Set expectation of what may lay ahead 3. Influence national perception of crisis and post-crisis narratives	▶ Activate [a] crisis management team and crisis communication team ▶ Prioritize [...] people's health and wellbeing ▶ Communicate clearly and consistently to fill the information vacuum ▶ Be consistent but agile – adapt as the context changes ▶ Equip leaders to share key messages, support [...] people and the community ▶ Prepare for escalation to a larger crisis situation
Stage II: Containment	1. Demonstrate caring and action 2. Support the individual and community, maintain operational continuity 3. Continue to influence national perception of crisis and post-crisis vision	▶ Prioritize people's safety and wellbeing ▶ Share the facts through a single 'source of truth' ▶ Monitor misinformation ▶ Be consistent but agile – adapt as the context changes ▶ Equip leaders to share key messages and support our people ▶ Prepare for escalation to the crisis situation
Stage III: Recovery	1. Demonstrate caring and action 2. Support the individual and maintain continuity 3. Address apathy, reduce anger, build future vision 4. Shape the future of the nation as it recovers from the crisis	▶ Prioritize people's health and wellbeing ▶ Share the facts through a single 'source of truth' ▶ Continue to monitor misinformation ▶ Be consistent but agile – adapt as the context changes ▶ Equip leaders to share key messages and support people ▶ Prepare for set-backs but look to the future

Source: UN Office of Counter-Terrorism

³⁵⁷ PwC (no date), Crisis communication [webpage]. Available at: <https://www.pwc.com/gx/en/issues/crisis-solutions/crisis-communication.html> [accessed 16 August 2024].

³⁵⁸ UN Counter-Terrorism Centre (UNCCT) (no date), *Crisis Communication*. Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/final_crisis_communication_toolkit_20042023.pdf [accessed 14 May 2025].

National Practice: UK Chartered Institute of Public Relations and Centre for the Protection of National Infrastructure's³⁵⁹ Suggested Areas for Inclusion in a Crisis Communication Plan³⁶⁰

The NPSA recommends that the following elements be considered for a crisis communication plan:

- ▶ Communications policy: the communications process for an incident, internal chain of command, police protocols, expectations of staff, and activities (including relevant channels).
- ▶ Holding statements: a selection of responses suitable for a range of incidents, ready for issue (with minor amendment) in the initial phase of the crisis.
- ▶ Roles and responsibilities: within the [CI owner/operator], including the designated person for emergency planning and managing crises. Identifying spokespeople and team member's specific job roles, and externally, with appropriate partners.
- ▶ Wellbeing: the crisis lifecycle can be lengthy and involve 24/7 working. Shift patterns and recovery time should be identified. Potential partners (e.g. extra resource from an external agency or another internal department, such as marketing or human resources) should be included.
- ▶ Contact list: key team members and external stakeholders, including media (as required).
- ▶ Systems: details of logins, process for corporate channels (e.g. amending website or switching to dark site), technical guides, building access details.
- ▶ Resources: templates, action plans, corporate imagery and briefing materials (e.g. fact sheets), communications log, email and WhatsApp groups, "grab bags" (e.g. phone charger, water, change of clothes, basic toiletries, information packs). If the police are taking the lead there will still be a requirement for the organisation to provide supporting resources, but your comms will not be in the front line for communication to the media.

Source: UK NPSA

Crisis Communications for Insider Events

Insider events can raise distinct challenges for crisis communications within and by organizations (for more information on insider threats, see Chapter 8, Insider Threat Management). By its very nature, an insider event is likely to be due (at least in part) to an organizational or individual failure, calling into question issues of competency, culture and trust. The impact of an insider event on both personnel and those outside a CI facility can be significant and long-lasting, potentially causing an erosion of trust (both internally and externally).

³⁵⁹ Now the National Protective Security Authority (NPSA).

³⁶⁰ Chartered Institute of Public Relations, Centre for the Protection of National Infrastructure (no date), *Crisis Management for Terrorist Related Events*. Available at: https://www.npsa.gov.uk/system/files/documents/de/eb/Crisis_Management_for_Terrorist_Related_Events.pdf [accessed 14 May 2025].

To mitigate the negative impacts of an insider event, some OSCE participating States have encouraged CI owners/operators to deploy communications techniques to successfully mitigate, manage and recover from an insider event – either through a crisis communications programme or dedicated measures focused on communications during this type of event.

National Practice: UK NPSA's Communications-related Recommendations on Insider Events for Businesses (2023)³⁶¹

1. Communication should be better integrated in the preparation and recovery of an insider event, rather than just in insider event management.
2. To ensure it is understood and elicits the desired result, insider event communication should prioritize the right message, delivered in the right tone through a compelling messenger and medium.
3. Rather than using metrics focused on how widely the message is delivered, the success of a communications strategy should be defined by how well the message is received. Unless a message is well-received, the number of people it is disseminated to is irrelevant.
4. Insider events must be embedded into existing crisis response best practices. Regular practice simulations are vital for building specific "muscle memory" and responsibly managing issues of fault, subjectivity, and truth.

Source: UK NPSA

Public Warning Systems

In UNSC Resolution 2341 (2017), the UNSC “recogniz[es] that protection efforts entail multiple streams of efforts, such as [...] public information and warning”.³⁶² Thus, as an additional communication tool, public warning systems can help inform members of the public during emergencies and may be useful as part of a broader crisis communications framework for terrorist attacks targeting CI facilities and services.

In the words of the European Emergency Number Association, a public warning system serves as “a valuable mechanism to minimise damages and manage the emergency situations during and after emergency events.”³⁶³ According to this Association, public warnings can be transmitted via mobile phones, fixed phones, television, radio, sirens and long-range acoustic devices, variable-message signs and public address systems, and the internet.³⁶⁴ The European Commission established the European Electronic Communications Code in 2018, in which Article 110 specifically requires EU Member States to have public warning systems in place that transmit warnings via mobile

³⁶¹ NPSA (2023), *Insider events: A communications guide to reduce their impact*. Available at: <https://www.npsa.gov.uk/resources/insider-event-guidance> [accessed 14 May 2025].

³⁶² UNSC (2017), Resolution 2341 (S/RES/2341). Available at: <https://documents.un.org/doc/undoc/gen/n17/038/57/pdf/n1703857.pdf> [accessed 5 May 2025].

³⁶³ European Emergency Number Association (30 September 2019), *Public Warning Systems – Update, Version 3.0*. Available at: https://eena.org/wp-content/uploads/2021_02_18_PWS_Document_FINAL_Compressed.pdf [accessed 14 May 2025].

³⁶⁴ European Emergency Number Association (30 September 2019), *Public Warning Systems – Update, Version 3.0*. Available at: https://eena.org/wp-content/uploads/2021_02_18_PWS_Document_FINAL_Compressed.pdf [accessed 14 May 2025].

number-based devices or other services, “provided that the effectiveness of the public warning system is equivalent in terms of coverage and capacity to reach end-users, including those only temporarily present in the area concerned”.³⁶⁵

National Practice: Switzerland’s Multi-channel Strategy for Information, Warning and Alarm (2024)³⁶⁶

Switzerland’s core alert system, called PolyAlert, allows for all public warning channels to be used via a single input, with all authorized civil protection authorities having access to the core systems. It allows for remote siren control and management, as well as message input by relevant authorities in case of emergency. On top of over 7,000 stationary and mobile sirens, the Swiss system also provides warnings to the population via the Alertswiss application and website, as well as radio and television, which are required by law to transmit certain messages related to public safety. Further channels for communication are a specific emergency radio, cell broadcasts, partner channels and emergency meeting points. In its *Multi-channel Strategy for Information, Warning and Alerting Outlook 2035*, Switzerland committed to further developing and updating this multi-channel system based on technological developments and security requirements.

Source: Switzerland’s Federal Office for Civil Protection

365 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321. Available at: <https://eur-lex.europa.eu/eli/dir/2018/1972/oj/eng> [accessed 31 March 2025]. A list of the emergency services available in the EU can be found under: Body of European Regulators for Electronic Communication (BEREC), Public Warning Systems [webpage]. Available at: <https://www.berec.europa.eu/en/pws> [accessed 14 May 2025].

366 Swiss Federal Office for Civil Protection (BABS) (October 2024), *Multikanalstrategie für die Information, Warnung und Alarmierung*. Ausblick 2035. Available at: <https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2024/11/27/bc33f6aa-911f-45fb-97fe-7978120b06b1.pdf> [accessed 14 May 2025] unofficial translation.



Insider Threat Management

//

The breadth of threats that insiders may pose to critical infrastructure facilities has led to a range of approaches by different owners/operators, allowing them to reflect the specific ways insiders can present risks to their organization.

//

8 Insider Threat Management

The previous chapters have explored a range of physical security solutions oriented towards external threats to CI facilities. Save for perhaps the civil aviation and energy sectors, less attention has historically been paid to the issue of insider threats.³⁶⁷ However, this is changing due to increased attention and awareness among CI owners/operators and national policymakers of the threat insiders can pose to the effective functioning of CI.

This chapter provides a range of definitions and approaches for conceptualizing insider threats, including malicious and non-malicious insiders. It then examines the ways in which individuals may engage in hostile insider activity, followed by proposals for organizational responses to this ever-present challenge.

Terrorist Insider Case Study 1 – Aviation Sector

On 2 February 2015, a Daallo Airlines plane departed from Mogadishu, Somalia. Shortly after take-off, an explosion on the plane ripped a hole in the side of the fuselage and sucked out the bomber, Abdullahi Abdisalam Borleh. Upon investigation, Somali authorities concluded that a laptop containing a bomb had prematurely detonated. According to Somali intelligence officials,³⁶⁸ video evidence shows two airport workers handing the laptop to Abdisalam Borleh before he boarded the plane.³⁶⁹

Terrorist Insider Case Study 2 – Energy Sector³⁷⁰

On 16 January 2013, 32 terrorists seized control of the Tiguentourine gas plant at In Amenas in southern Algeria, beginning a four-day siege where dozens of foreign hostages were rounded up and detained, forty of whom were eventually killed. The In Amenas plant, one of Algeria's largest gas developments located approximately 1,300 kilometres from the capital city of Algiers and 50 kilometres from the border with Libya, was operated as a joint venture between the Algerian national oil company Sonatrach, British Petroleum and Statoil.

There were a number of serious security failures in the lead up to the attack, with security measures at the site not adapted to handle an attack of the size and scale

367 UNOCT, and UNSC Counter-Terrorism Committee Executive Directorate (2022), *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices*. Available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf [accessed 13 May 2025].

368 Maruf, H. (2016), "Somali Officials: Man Killed in Plane Bombing Given Laptop Before Flight", Voice of America [webpage]. Available at: <https://www.voanews.com/a/airport-staff-airline-employees-detained-somali-plane-blast/3179920.html> [accessed 30 November 2024].

369 US Transportation Security Administration (2020), *Insider Threat Roadmap*. Available at: https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf [accessed 14 May 2025].

370 Statoil (2013), *The In Amenas Attack: Report of the investigation into the terrorist attack on In Amenas. Prepared for Statoil ASA's Board of directors*. Available at: <https://www.equinor.com/news/archive/2013/09/12/downloads/In%20Amenas%20report.pdf> [accessed 13 May 2025].

that occurred. Survivors of the attack subsequently stated that the attackers appeared well-informed about the facility, including the location of the management office, where and when senior executives would be on-site, and how to cut off the electricity, which was done within the first few minutes of the attack. Both Statoil and Algerian officials concluded that the terrorists likely benefited from some insider knowledge in the planning of the attack, however, no clear evidence of this was ever uncovered.

In a 2016 article published in the *Studies in Conflict & Terrorism journal*, the following was determined:

“While the threat from terrorism has gained widespread acknowledgement over the last decade, the infiltration of organizations by ‘terrorist’ insiders has not, and the potential dangers these individuals present has not been fully explored. There is a need to understand the wider aspects of insider threats, including motivations and attack methodologies, and to be able to demonstrate the potential devastation that could be caused.”³⁷¹

In 2023, the NPSA of the United Kingdom undertook research that reinforces the importance of mitigating insider threats to CI, indicating that:

- ▶ The number of insider events had increased by almost 50% in just two years;
- ▶ 98% of organizations feel vulnerable to insider attacks;
- ▶ Malicious or criminal insiders were behind 25% of incidents;
- ▶ Insider-related events are taking longer to resolve (three months on average), and as a result, the cost of containing the impact of insider activity was estimated at over USD 15,000,000 at the time of the NPSA research (an increase on previous years).³⁷²

In 2020, the US Transportation Security Administration similarly emphasized the insider threat within the transportation sector:

“Insider threat activity in the [transportation sector] has generally been related to industrial sabotage, theft, and/or smuggling rather than terrorism, but, as recently as 2019, terrorists have sought to leverage insiders to conduct their attacks. There are valid concerns that terrorists could exploit the tactics, techniques, and procedures used by transnational criminal organizations to identify and recruit, or develop and emplace insiders into the [transportation sector].”³⁷³

371 BaMaung, D.; McIlhatton, D.; MacDonald, M.; Beattie, R. (2016), “The Enemy Within? The Connection between Insider Threat and Terrorism”. *Studies in Conflict & Terrorism* 41(2), pp. 133–150. Available at: <https://doi.org/10.1080/1057610X.2016.1249776> [accessed 13 May 2025].

372 NPSA (2023), *Insider Events: A communications guide to reduce their impact*. Available at: <https://www.npsa.gov.uk/insider-events-communications-guidance> [accessed 13 May 2025].

373 United States Transportation Security Administration (2020), *Insider Threat Roadmap 2020*. Available at: https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf [accessed 13 May 2025].

8.1 Defining Insider Threats

Before exploring issues and practices for managing insider threats, it is important to consider how different OSCE participating States and other stakeholders define *insiders* and *insider threats*. For the term *insider*, one key recurring phrase appears across multiple definitions (including those used by the United States³⁷⁴ and the United Kingdom³⁷⁵) is *authorized access*. Each referenced definition identifies an insider as a person who has, or had, authorized access to (or knowledge of) an organization's resources, which can include personnel, facilities, information, processes and data.



This is a view shared by some CI owners/operators: the Vienna International Airport in Austria considers an insider, “a person who has or had authorised access to or knowledge of resources, tools, or processes of an organisation. This person normally works directly for or under contract with the organisation. An insider becomes an insider threat as soon as this knowledge is used intentionally against the organisation. This person has an advantage over an outsider because he or she is generally familiar with the security policies and procedures.”³⁷⁶

Definitions of *insider threats* typically focus on the intentional misuse of authorized access or understanding of an organization in order to harm it. However, unintentional insider threats are also relevant. The Help2Protect³⁷⁷ Insider Threat Program

374 CISA (no date), Defining Insider Threats [webpage]. Available at: <https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats#:~:text=Insider%20threat%20is%20the%20potential,organization%20to%20harm%20that%20organization> [accessed 12 November 2024].

375 NPSA (22 May 2023), NPSA Changes to Insider Risk Definitions [webpage]. Available at: <https://www.npsa.gov.uk/blog/npsa-changes-insider-risk-definitions> [accessed 12 November 2024].

376 Vienna Airport (no date), Types of threat – from carelessness to intention [webpage]. Available at: https://www.viennaairport.com/en/business__partner/security_culture/types_of_threat_-_from_carelessness_to_intention [accessed 12 November 2024].

377 Help2Protect (H2P) is an e-learning platform created at the end of 2018 as the main deliverable of the EU-funded project AITRAP on Insider Threats. The project was co-ordinated by the Confederation of European Security Services. More information can be found here: https://www.help2protect.info/?doing_wp_cron=1744884209.4140460491180419921875 [accessed 14 May 2025].

Development Manual states: “[i]nsider threats, to include sabotage, theft, espionage, fraud, and competitive advantage, are often carried out through abusing access rights, theft of materials, and mishandling physical devices. Insiders do not always act alone and may not be aware they are aiding a threat actor (i.e., the unintentional Insider Threat).”³⁷⁸ The US definition also includes unintentional or non-malicious acts by insiders that can have similarly negative impacts on an organization.³⁷⁹

Practice: Corporate Regulations for Physical Security and Counter-Terrorism Protection for KazMunayGas: Internal Threat Actors (2020)³⁸⁰

The KazMunayGas regulations define the “primary goals, objectives, general philosophy and areas of Physical Security and Counter-Terrorism Protection activities of the [KazMunayGas] Group”. As part of the regulations, different types of threat actors are defined in order to “establish the required level of protection for the Facility and its Critical Zones, elaborate requirements for the Physical Security and Counter-Terrorism Protection System of the Facility and evaluate its effectiveness.”

These threat actors are divided in two categories: Internal Offenders (“persons from among Facility employees and other people who have been allowed to the territory as established”) and External Offenders (“persons who are not employees/visitors of the Facility and have no right to access it”). The Regulations then provide a detailed description of both types of offenders, their main characteristics and likely tactics. The two Internal Offender types from this regulation are summarized below:

Offender type	Main characteristics	Probable tactics
1. Internal Offender Type 1 (an employee/specialist of the Facility who has authorised access to the territory) The main goal is to steal for material gain, but an Act of Terrorism possibility cannot be excluded.	1. highly aware about composition and structure of the Physical Security and Counter-Terrorism Protection System of the Facility and locations of Guard posts; 2. highly aware about locations of the targets of theft or sabotage at the Facility; 3. hardly likely to have firearms, explosives or explosive devices; 4. may be using hand tools or special tools; 5. unlikely to use vehicles; 6. prepared enough to overcome physical barriers.	Legally enters the Facility during working hours using his/her gate pass. The Offender may be a source of information about a potentially hazardous Facility for an External Offender Type 1 or 2, conspire with External and Internal Offenders to participate in joint Acts of Terrorism.

378 Help2Protect (2025), Insider Threat Programme Development Manual, Edition 5. Available at: https://www.help2protect.info/kickstarter/insider-threat-program-development/?doing_wp_cron=1744884664.1926438808441162109375 [accessed 14 May 2025].

379 CISA (no date), *Insider Threat Mitigation Guide*. Available at: <https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide> [accessed 14 May 2025].

380 Kulikov, V. (2 December 2020), Corporate Regulations for Physical Security and Counter-Terrorism Protection of Joint-Stock Company “National Company KazMunayGas”. Available at: <https://www.kmg.kz/upload/iblock/a0c/34x6gyk68gytk3y1td8tzjkq6h5irl6k/Corporate%20Regulations%20for%20Physical%20Security%20and%20Counter-Terrorism%20Protection%20of%20Joint-Stock%20Company%20National%20Company%20KazMunayGas.docx> [accessed 14 May 2025].

2. Internal Offender Type 2
([Site Security Unit] employee)

1. highly aware about composition and structure of the Physical Security and Counter-Terrorism Protection System of the Facility, locations of Guard Posts;
2. hardly aware about the production process;
3. highly aware about locations of the targets of Security Objects at the Facility;
4. has weapons and special devices (depending on the regular gear of security forces at a specific Facility);
5. may freely enter a Guarded Zone;
6. hardly prepared to overcome physical barriers.

Open access to the targets of theft during working hours using his/her official authority.

Offender: is aware about working hours of the Facility, locations of possible material and other valuables; may select the best moment for an Act of Terrorism; may conspire with External Offenders.

Source: KazMunayGas

The breadth of threats that insiders may pose to CI facilities has led to a range of approaches by different owners/operators, allowing them to reflect the specific ways insiders can present risks to their organization. For example, some organizations may base their definitions on:

- ▶ the types of threat actors considered insiders (i.e. malicious, unintentional, employee or contractor);
- ▶ the types of assets to which insiders have access (i.e. information technology [IT], facilities, networks or data); or
- ▶ the types of harm that could be done to the CI owner/operator (i.e., fraud, theft, sabotage, or violence).

These different approaches are an important reminder that the definition of *insider threat* should be specific to the context of a CI sector or stakeholder. This good practice is incorporated into US CISA guidance, which argues that an organization should “define the insider threat to address the unique nature of its operating environment, what it values, or the resources it feels are most at risk.”³⁸¹

National Practice: UK NPSA’s Five Types of Insider Events (2023)³⁸²

- ▶ Unauthorized disclosure of sensitive information;
- ▶ Process corruption (most likely fraud);
- ▶ Facilitated third-party access to an organization’s assets;
- ▶ Sabotage (physical, electronic or IT sabotage);
- ▶ Physical threat (violence).

Source: UK NPSA

381 CISA (no date), *Insider Threat Mitigation Guide*. Available at: <https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide> [accessed 14 May 2025].

382 NPSA (10 November 2023), *Introduction to Insider Risk* [webpage]. Available at: <https://www.npsa.gov.uk/introduction-insider-risk> [accessed 5 March 2024]

While there exists no consensus definition across the OSCE area for what an insider threat actually is, the following are some scenarios under which an insider may pose a threat to a CI owner/operator:



Information Theft

The theft of information such as blueprints or proprietary material that can compromise a CI owner/operator or facility, or place it at severe disadvantage or risk.



Workplace Violence

The use of violence or threats of violence to influence or threaten others at a CI facility and impact the health and safety of the facility's workforce.



Security Compromise

Acquiring knowledge of security personnel's patrol schedules and procedures in order to compromise the security capability of the facility and its personnel.



Espionage

Spying on behalf of another actor to obtain sensitive, proprietary, or important material or knowledge which could be used against the CI owner/operator.



Terrorism

Using access to a CI facility in order to commit or facilitate an act of violence in support of a terrorist or violent extremist ideology.



Physical Property Theft

Stealing material items (i.e., goods, equipment, badges).



Sabotage

The intentional destruction of equipment or IT, including direct specific harm (i.e. inserting malicious computer code into an organization's information technology infrastructure).

Understanding Insider Threats

The range of definitions of, and approaches to, insider threats outlined above is illustrative of the complexities they can pose. The term *insider* can encompass current or former employees, third-party contractors, or even business partners with access to the premises and systems within a CI facility. This is potentially a vast number of individuals. Each might be capable of observing CI processes undisturbed over a period of time and carrying out unauthorized acts.

Insiders hold distinct advantages over external threat actors, who can typically only gain access to CI by means of violent acts or subterfuge. Insiders can either be the main

conspirators in an attack on CI, or act as accomplices (i.e., informants) to outside actors. Their knowledge (or the ease with which they can acquire specific knowledge) on a targeted facility can be readily exploited for criminal purposes, including terrorist attacks.

Malicious and Non-Malicious Insiders

The activities of malicious insiders with access to critical assets and systems are a significant focus of insider risk mitigation strategies at the national, CI owner/operator, and CI facility levels. However, not all insiders are malicious and wish to cause harm. Some insiders unwittingly cause harm by doing the wrong thing due to work stress, distractions, lack of awareness, impatience, laziness, gullibility or complacency. Examples include misplacing sensitive data or leaving access areas insecure.

Other insiders might be manipulated into compromising their employer by external threat actors, such as criminals, terrorists, hackers or other external threat actors. Moreover, external threat actors may use deception to manipulate unwitting insiders in order to penetrate the security layers of target organizations. This can involve the use of social engineering techniques with the aim of securing information that can be used as blackmail.

These varied ways in which insiders pose a threat to CI owners/operators has led some to add further nuance to their definitions: the Help2Protect *Insider Threat Program Development Manual* identifies three categories of insiders:

- ▶ **The unintentional insider:** the employee does not understand that his/her actions are harmful. The employee has no intention to cause harm and may demonstrate very few indicators of risk.
- ▶ **The negligent insider:** the employee knows that his/her actions are a security violation but “takes a chance” to “cut corners.” The employee may demonstrate some indicators of risk.
- ▶ **The malicious insider:** the employee acts specifically for the purpose of damaging the organisation. The employee may take steps to hide indicators of risk.³⁸³

Malicious insiders, according to Help2Protect, fall into at least two categories:

- ▶ **Self-motivated insiders:** they are individuals whose actions are undertaken of their own volition, and not initiated as the result of any connection to, or direction by, a third party.
- ▶ **Recruited insiders:** they are individuals co-opted by a third party to specifically exploit their potential, current or former privileged access. This includes cultivated and recruited foreign intelligence, or their entities with malicious intent.³⁸⁴

383 Help2Protect (2025), *Insider Threat Programme Development Manual, Edition 5*. Available at: https://www.help2protect.info/kickstarter/insider-threat-program-development/?doing_wp_cron=1744884664.1926438808441162109375 [accessed 14 May 2025].

384 Help2Protect (2025), *Insider Threat Programme Development Manual, Edition 5*. Available at: https://www.help2protect.info/kickstarter/insider-threat-program-development/?doing_wp_cron=1744884664.1926438808441162109375 [accessed 14 May 2025].

8.2 Factors Affecting Individuals' Likelihood to Engage in Hostile Insider Behaviour

To find the most effective responses to insider threats, it is important to identify factors that can cause an employee to undertake hostile insider activity. The Help2Protect *Insider Threat Program Development Manual* identifies several potential causes as part of the insider threat pathway:

- ▶ Private or work-related crisis (financial, personal, relational, health, life events, etc.);
- ▶ Feeling of frustration, disappointment or disgruntlement;
- ▶ Over-inflated sense of abilities and achievements;
- ▶ Strong sense of entitlement and egotistical view of what the organization is, or is not, doing to/for them;
- ▶ Need to demonstrate value to others to be recognized.³⁸⁵

Hostile insider behaviour may also be carried out in retaliation against an organization or employer. A combination of these factors may result in a trigger event – such as a conflict with colleagues or an illness (including a mental health condition) – causing an individual to engage in hostile insider activity.

Even if this is not the case, an opportunity needs to be present for an insider to carry out hostile insider activity. This could involve access to valuable physical items or information, or opportunities due to lax security measures, such as the sharing of passwords or access codes by colleagues.³⁸⁶

8.3 Indicators of Hostile Insider Activity

Detecting the indicators of hostile insider activity and attack preparation is central to an effective insider threat mitigation effort by a CI owner/operator. While there is no set list of indicators – the below points do not offer an exhaustive account – there are specific activities that, when combined with other pieces of information or intelligence from competent CI security personnel or authorities, may suggest an insider threat is present or, at least, possible:³⁸⁷

- ▶ Staff visiting areas where they do not normally work or have no authority;
- ▶ Staff asking questions about the organization, the premises, management or ownership;
- ▶ Staff asking overly probing personal questions about other staff members;
- ▶ Staff taking notes or photographs of key parts of the facility;
- ▶ Staff walking around the site at unusual times without a clear, defined, or authorized purpose;

³⁸⁵ Help2Protect (2025), *Insider Threat Programme Development Manual, Edition 5*. Available at: https://www.help2protect.info/kickstarter/insider-threat-program-development/?doing_wp_cron=1744884664.1926438808441162109375 [accessed 14 May 2025].

³⁸⁶ Martin, P. (2024), *Insider Risk and Personnel Security: An Introduction* (Abingdon, New York: Routledge).

³⁸⁷ Indicators draw partially on BaMaung, D.; Bergin, G.; Byrne, J.; Garrett, D.; Harrison, A.; Maples, L.; Quinn, L. (2022), *Terrorism and Countermeasures, Version 2* (Naas, Co. Kildare: The Security Institute of Ireland).

- ▶ Staff acting nervous or anxious for no apparent reason when approached or engaged in conversation;
- ▶ Staff being present at the facility when not scheduled to work/working outside of normal working hours (if not requested by line management);
- ▶ Staff being guarded about his/her own movements, background, or family;
- ▶ Staff attempting to bypass or test security controls;
- ▶ Staff requesting clearance or access to higher-level systems without need;
- ▶ Staff displaying behaviour that demonstrates sudden affluence without an obvious cause;
- ▶ Staff maintaining access to sensitive data after termination notice;
- ▶ Staff using unauthorized external storage devices;
- ▶ Staff showing visible disgruntlement towards employer or co-workers;
- ▶ Staff engaging in chronic violation of organizational policies;
- ▶ Staff showing a notable and unexplained decline in work performance;
- ▶ Staff disclosing information not for public disclosure in public areas, to the media, or to other sources.

In addition to these potential indicators, an employee may exhibit other warning signs suggesting that a process of radicalization to violence may be underway. These include vocalizing support for violent extremist ideologies, using derogatory and violent language towards individuals, an organization or government, supporting violence as a necessary means to achieve a goal, and/or attempts to radicalize others to violence.

Although none of these red flags should necessarily be viewed as a demonstration of intent to harm by an employee, they may require the initiation of a review and clarification process. The process should involve the identification and collation of all indicators. Rather than assessing each indicator individually, they should then be analysed collectively to identify hidden or unrealized relationships between them.

8.4 Organizational Responses to Insider Threats

Although it is possible for a CI owner/operator to adopt a variety of stand-alone insider threat mitigation measures, the lack of connection between them will generally mean limited overall success. At the same time, there is no definitive *solution* for an insider threat programme, nor is there a specific approach that is *better* than others. Much will depend on the size, structure and culture of the CI organization in question, as well as the support provided by senior management and the sector involved.

Practice: International Civil Aviation Organization's Insider Threat Toolkit³⁸⁸

To support organizations operating in the aviation environment, the International Civil Aviation Organization (ICAO) developed a toolkit in collaboration with the ICAO Aviation Security Panel's Working Group on Training. The toolkit includes guidance on mitigation measures, background checks and vetting, training and awareness, access control measures, patrolling, surveillance and monitoring, reporting mechanisms, behaviour detection, security culture, leadership and strategy, human factors and advanced technologies.

Source: ICAO

Practice: International Maritime Organization Insider Threat Toolkit (2024)³⁸⁹

In 2024, the International Maritime Organization (IMO) released an Insider Threat Toolkit for organizations operating in the maritime environment, including "Maritime Administrations, Designated Authorities, shipping companies, port operators and other maritime stakeholders". The toolkit was developed together with the ICAO, so it aligns with the aforementioned ICAO Insider Threat Toolkit.

Source: IMO

There is an undeniable benefit to developing a streamlined, coherent programme focused on insider threats at CI facilities (including crisis communications for insider events, as discussed in Chapter 7, Security Planning and Target Hardening). In the United States, CISA envisages this benefit in five parts. An insider threat mitigation programme provides CI owners/operators with the ability to:

1. Establish and maintain a safe environment to prevent violence and other hostile acts from occurring.
2. Deter potential insider threats by instituting policies, security controls, procedures, and programs to protect the organization.
3. Detect threatening or concerning behaviours and identify individuals at risk of becoming an insider threat.
4. Assess information about actual or potential insider threats.
5. Manage potential insider threats before they escalate to violence, espionage, sabotage, or theft.³⁹⁰

To guide this process, several approaches for developing an insider threat programme from government bodies and the private sector are provided. In any insider threat programme, special attention should be paid to developing clear procedures and safeguards regarding the use of personal data for specific, authorized purposes in line with local data protection laws and regulations.

³⁸⁸ ICAO (2022), *ICAO Insider Threat Toolkit*. Available at: <https://www.icao.int/Security/securityculture/Documents/Insider%20threat%20toolkit.EN.pdf> [accessed 14 May 2025].

³⁸⁹ IMO (no date), *Insider Threat Tool Kit, Edition 1*. Available at: <https://www.imo.org/en/OurWork/Security/Pages/Insider-Threat%20training%20aid.aspx> [accessed 14 May 2025].

³⁹⁰ CISA (no date), *Insider Threat Mitigation Guide*. Available at: <https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide> [accessed 14 May 2025].

National Practice: Public Safety Canada's Recommended Security Action Checklist for Enhancing Critical Infrastructure Resilience to Insider Risk (2019)³⁹¹

In 2019, Public Safety Canada released a document designed to provide Canadian CI organizations guidance on what constitutes insider risk, and recommendations on how to monitor, respond to and mitigate insider risk. The guidance is presented through eight recommended security actions, each detailed below. The publicly available document also details relevant national and international standards that can be applied.

Security Action #1: Establish a Culture of Security

- ▶ Identify an organizational champion for managing insider risks with full accountability;
- ▶ Identify a senior executive accountable for the development of a company-wide security policy and program;
- ▶ Develop a governance structure, including an insider risk working group, to develop, deliver and manage an insider risk program;
- ▶ Establish an organizational "pledge" to recognize the importance of security in delivering a profitable and sustainable business;
- ▶ Design comprehensive physical and cyber network security policies and procedures encompassing all departments; and,
- ▶ Promote a culture of security at all levels by linking employee and management performance to security metrics.

Security Action #2: Develop Clear Security Policies and Procedures

- ▶ Clearly define, post, and educate employees in corporate security policies;
- ▶ Conduct employee screening based on position requirements; and
- ▶ Assign appropriate risk levels of employees commensurate with the criticality and importance of the information, systems, and area that they access.

Security Action #3: Reduce Risks from Partners and Third-Party Providers

- ▶ Conduct an organization-wide risk assessment identifying all key assets and critical systems; Identify all security concerns related to third-party access to its networks, data and systems;
- ▶ Independently verify the security posture of third party service providers, including background checks of employees with access to an organization's critical facilities or networks;
- ▶ Ensure comprehensive third-party security agreements, with assurance language included in the agreements, to reduce supply chain risk; and
- ▶ Build long-term trusted relationships with key service providers.

Security Action #4: Implement a Personnel Screening Life-Cycle

- ▶ Conduct thorough pre-employment and continuous screening of all personnel using all resources available, including social media;
- ▶ Update security access and clearances for employees based on the roles and responsibilities of their position;

³⁹¹ Public Safety Canada Critical Infrastructure Directorate (2019), *Enhancing Canada's Critical Infrastructure Resilience to Insider Risk*. Available at: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/nhncng-crtcl-nfrstrctr/nhncng-crtcl-nfrstrctr-en.pdf> [accessed 14 May 2025].

- ▶ Amend access privileges for employees that have moved to new positions within the organization; and
- ▶ Promote a transparent security program to all employees to manage physical and network security expectations.

Security Action #5: Provide Training, Raise Awareness and Conduct Exercises

- ▶ Develop a security training program for all employees;
- ▶ Raise awareness of indicators of potential security concerns;
- ▶ Provide access to employee assistance programs to help prevent employees from becoming at risk of compromise;
- ▶ Develop and promote a culture of security vigilance by encouraging employees to say something if they see something;
- ▶ Conduct periodic exercises to test the security posture within an organization.

Security Action #6: Identify Critical Assets and Protect Them

- ▶ Conduct an organization-wide assessment to identify and rank critical assets and systems and security measures to protect them;
- ▶ Monitor system usage by authorized and unauthorized users as well as physical premises access;
- ▶ Outline how/what data is being sent to 3rd parties and the sensitivity of the data, and protect data appropriately;
- ▶ Consider the principle of least privilege and separation of duties for critical systems and data; and
- ▶ Leverage visible deterrents to decrease the likelihood of unintended access to facilities, networks and systems.

Security Action #7: Monitor, Respond to and Mitigate Unusual Behaviour

- ▶ Establish a means of monitoring physical and network access from all endpoints and remote devices;
- ▶ Develop a culture that enhances employee awareness of security and reporting suspicious activity or abnormal behaviour;
- ▶ Raise awareness of the potential risks associated with social media sites;
- ▶ Limit remote access to non-critical assets and systems where possible;
- ▶ Establish protocols to report, track and respond to unusual incidents; and
- ▶ Consider engaging the security and intelligence community, including [domestic authorities].

Security Action #8: Protect Your Data

- ▶ Backup and protect all organizational data and essential systems on a regular basis;
- ▶ Develop policies for downloading large amounts of data or sensitive files;
- ▶ Consolidate access points to the internet;
- ▶ Implement segregated systems to prevent data loss; and
- ▶ Limit or restrict portable storage devices.

Source: Public Safety Canada

National Practice: US CISA Guidance on Key Elements for Establishing an Insider Threat Programme (2020)³⁹²

- ▶ Principles and standards that align the program with the culture and business of an organization and describe its purpose, goals, and objectives;
- ▶ The creation of a prioritized list of critical assets (both physical and intellectual) that are essential to the organization and whose compromise, damage, or loss can have an adverse impact on its mission;
- ▶ Definitions of the most significant and prevalent threats and how they could affect the organization's critical assets;
- ▶ Means to detect and identify indicators of potential risks;
- ▶ An Incident Response Plan in case of an insider threat incident;
- ▶ A committee of stakeholders for program governance and leadership;
- ▶ An organizational culture that encourages and provides a means of reporting. Reporting potential threats, indicators, or concerns to a responsible party is a reasonable expectation of employees and confidentiality is maintained;
- ▶ A central information hub for the collection, integration, analysis, and storage of all elements pertaining to insider threats;
- ▶ A threat management team for the assessment, response, and management of potential insider threats;
- ▶ An insider threat training and awareness program to teach the importance of identifying and reporting potential threats and how the individual is the first line of defence in protecting the organization.

Source: US DHS CISA

Vetting Personnel

As part of effective personnel security and insider threat management, many governments and CI owners/operators vet CI facility employees and perform background checks. Background checks and relevant vetting measures should be designed in line with local data protection laws and regulations, as well as broader human rights commitments. For more information, see Chapter 3, Human Rights Considerations.

³⁹² CISA (no date), *Insider Threat Mitigation Guide*. Available at: <https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide> [accessed 14 May 2025].

National Practice: Australia's AusCheck Background Check Procedure³⁹³

The Australian Department of Home Affairs manages AusCheck, which provides background checking services for a "critical worker[s] who has been identified by a responsible entity as requiring an AusCheck background check in order to have access to a critical component/s of their critical infrastructure asset/s" in "security sensitive critical infrastructure sectors in Australia." The background check consists of the following:

- ▶ identity verification
- ▶ a criminal record assessment by AusCheck using information collected by the Australian Criminal Intelligence Commission
- ▶ a national security assessment by the Australian Security Intelligence Organisation
- ▶ a "right to work in Australia" check if a person is not an Australian citizen, conducted through the Visa Entitlement Verification Online system.

Source: AusCheck

ICAO guidance calls for initial background checks³⁹⁴ for specific categories of civil aviation employees (e.g., "all employees that need unescorted access to airside and security restricted areas, and persons with access to sensitive security information"). Initial background checks for ICAO cover:

- ▶ identity (e.g. provision of a passport, identity card, records of registry of birth, etc.);
- ▶ criminal history (to the full extent permissible by local regulations and laws);
- ▶ reference check (to attest to the work ethic and overall suitability of the prospective employee); and
- ▶ employment history (e.g. previous employers, educational history, etc.).³⁹⁵

ICAO also provides guidance on recurrent background checks, continuous vetting measures, as well as enhanced background checks when necessary. The IMO provides similar guidance in its *Insider Threat Toolkit*.³⁹⁶

Article 14 of the CER Directive is specifically dedicated to background checks. In addition to providing the framework within which background checks should be conducted, the Directive specifies that it shall at least: "corroborate the identity of the person who is the subject of the background check" and "check the criminal records of that person with regards to offences which would be relevant for a specific position."³⁹⁷

393 Australian Government, Department of Home Affairs (2 December 2024), Critical Infrastructure Background Checks [webpage]. Available at: <https://www.auscheck.gov.au/critical-infrastructure/critical-infrastructure-background-checks> [accessed 7 April 2025].

394 ICAO (2022), *Annex 17 to the Convention on International Civil Aviation. Aviation Security. Safeguarding International Civil Aviation against Acts of Unlawful Interference*, 12th Edition, Principle 3.5.2.

395 ICAO (2022), *ICAO Insider Threat Toolkit*. Available at: <https://www.icao.int/Security/securityculture/Documents/Insider%20threat%20toolkit.EN.pdf> [accessed 14 May 2025].

396 IMO (no date) *Insider Threat* [webpage]. Available at: <https://www.imo.org/en/OurWork/Security/Pages/Insider-Threat%20training%20aid.aspx> [accessed 7 April 2025].

397 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, Article 14. Available at: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj> [accessed 31 March 2025].



Training and Exercising

//

*Training and exercising
are central to developing
a resilient and security-
conscious workforce at a
critical infrastructure facility.*

//

9 Training and Exercising

Training and exercising are central to developing a resilient and security-conscious workforce at a CI facility. By participating in training and exercises, CI personnel not only develop new skills but also become increasingly confident in their ability to manage an array of situations, including crises. Notably, training and exercises involving CI personnel and local authorities involved in responses to security incidents at the CI facility may help to reduce response times and facilitate smooth co-operation in crisis situations. For CI owners/operators and their security personnel, exercises in particular provide an opportunity to review existing plans and identify areas for improvement. Plans on paper are an important starting point, but they must be brought to life and routinely exercised in order to assess their effectiveness. This chapter details the importance of training and exercising as part of a CI facility's routine security planning and activities.



According to the UN Security Council, training is viewed as a core component of efforts to protect CI from terrorist attacks. In UNSC Resolution 2341 (2017), the Security Council specifically acknowledges the

“vital role that informed, alert communities play in promoting awareness and understanding of the terrorist threat environment and specifically in identifying and reporting suspicious activities to law enforcement authorities, and the importance of expanding public awareness, engagement, and public–private partnership as appropriate, especially regarding potential terrorist threats and vulnerabilities through regular national and local dialogue, training, and outreach”.³⁹⁸

³⁹⁸ UNSC (2017), Resolution 2341 (S/RES/2341). Available at: <https://documents.un.org/doc/undoc/gen/n17/038/57/pdf/n1703857.pdf> [accessed 5 May 2025].

The extent of measures within this *Technical Guide* that call for some form of workforce training shows the prominent role physical security and counter-terrorism measures play for all CI personnel and their professional development. Training can be delivered in a number of ways to ensure the broadest reach, such as instructor-led classroom training courses, on-the-job training courses, training courses provided by local emergency services or law enforcement, or remote training via webinars and web-based independent training courses.³⁹⁹ Ideally, a dedicated training programme would be developed by a CI owner/operator and would contain a combination of learning methods, with the most ideal combination tailored to the personnel receiving the training.

Case Study: 2017 Manchester Arena Bombing in the United Kingdom

The impact of inadequately trained personnel in a terrorist attack can be catastrophic. On 22 May 2017, a suicide bomber detonated a PBIED at the end of an Ariana Grande concert at the Manchester Arena. The attack killed 22 concertgoers and their waiting parents, as well as injuring hundreds of children and adults emerging from the concert hall. In response, in 2019 the then Home Secretary of the United Kingdom established a statutory public inquiry to investigate the deaths of the victims of the attack. The Manchester Arena Public Inquiry found, among other things, that the private security provider employed by the venue operator had delivered online counter-terrorism training to its personnel, however [the provider] “should have followed up this online training with practical, person-to-person training, which checked that the online training had been understood and built confidence around the reporting of concerns.”⁴⁰⁰

The United Kingdom’s private security industry regulator, the Security Industry Authority (SIA),⁴⁰¹ subsequently changed its training course content for private security personnel, adding more counter-terrorism content of improved quality.⁴⁰²

In response to the Inquiry, the Greater Manchester Police acknowledged, that “poor communications, poor planning, inadequate training, and shortcomings in strategic leadership all played a part in our failure. All of these failings could, and should, have been identified and mitigated through learning from robustly designed training exercises under the auspices of our Local Resilience Forum. Alas, these were opportunities that were not sufficiently taken.”⁴⁰³

399 CISA (November 2019), *A Guide to Critical Infrastructure Security and Resilience*. Available at: <https://cncpic.mai.gov.ro/sites/default/files/2020-03/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf> [accessed 14 May 2025].

400 Saunders, Sir J. (June 2021), *Manchester Arena Inquiry Volume 1: Security for the Arena. Report of the Public Inquiry into the Attack on Manchester Arena on 22nd May 2017*. Available at: <https://www.gov.uk/government/publications/manchester-arena-inquiry-volume-1-security-for-the-arena> [accessed 14 May 2025].

401 In the United Kingdom, the private security industry is regulated by the Security Industry Authority (SIA). The SIA decides on the content of training courses undertaken by security personnel to obtain the appropriate license for their role. Security operatives are required to obtain a license before they can carry out certain security functions. Training is seen as an essential part of the licensing requirement. For more information, see: <https://www.gov.uk/guidance/check-what-training-you-need-to-get-an-sia-licence>.

402 Saunders, Sir J. (June 2021), *Manchester Arena Inquiry Volume 1: Security for the Arena. Report of the Public Inquiry into the Attack on Manchester Arena on 22nd May 2017*. Available at: <https://www.gov.uk/government/publications/manchester-arena-inquiry-volume-1-security-for-the-arena> [accessed 14 May 2025].

403 Greater Manchester Police (3 November 2022), *Statement in response to Manchester Arena Inquiry Volume Two Report* [webpage]. Available at: <https://www.gmp.police.uk/news/greater-manchester/news/news/2022/november/statement-in-response-to-inquiry-report/> [accessed 31 August 2024].

Testing the knowledge of trainees in an exercise is one of the best ways to assess the effectiveness of training programmes, since it enables trainees to demonstrate the skills they have learned in a safe environment, rather than in a real time live emergency. Exercises can also be used to identify gaps and vulnerabilities in plans, procedures, measures and workforce composition. They are highly useful when preparing for terrorist threats, since in this form of crisis, people and personnel are likely to become highly stressed and react without fully considering their actions, which may lead them to act wrongly or irrationally.⁴⁰⁴

9.1 Training

Training plays an important role in improving the physical security of CI sites, in particular in relation to the unique threat posed by terrorist attacks. Threats to CI vary in complexity and impact. The emergence of sophisticated technological threats, such as cyber-attacks or the use of UAS, has added a new dimension of risk. In light of this, CI facility personnel who manage the security of a facility or work in the facility within any job category should have sufficient skills to understand and respond to the threats faced by CI facilities. Training can be provided by competent government authorities, CI owners/operators, private companies and others.

Since most CI across the OSCE area is owned or operated by private actors, training for facility personnel related to the prevention of and response to terrorist attacks is best developed in co-operation with national authorities, as well as, if relevant, private security providers. The OSCE has previously emphasized that incident response training for CI facility personnel involving local government officials is particularly useful for developing an effective PPP approach to the management of a crisis.⁴⁰⁵

404 Bundesamt für Sicherheit in der Informationstechnik (2008), *BSI-Standard 100-4. Notfallmanagement*. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2 [accessed 14 May 2025].

405 OSCE (2013), *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*. Available at: <https://www.osce.org/files/f/documents/7/5/103954.pdf> [accessed 14 May 2025].

National Practice: US CISA Potential Training Topics for Critical Infrastructure Personnel (2019)⁴⁰⁶

- ▶ Best practices for physical security
- ▶ Active Shooter
- ▶ Identifying and Reporting Suspicious Activity
- ▶ Insider Threat
- ▶ Credentialing
- ▶ Bag Screening
- ▶ Patron Screening
- ▶ Sector Best Practices (e.g., chemical, energy, water)
- ▶ Supply chain risk management and third-party dependency
- ▶ Incident Management and Response Bomb Threats
- ▶ Countering Improvised Explosive Devices
- ▶ Vehicle Threats
- ▶ Suicide Bombers
- ▶ Cybersecurity
- ▶ Exercises
- ▶ Terrorism Threats, Tactics, and Trends
- ▶ Industrial Control System and Operational Technology
- ▶ Risk Assessment (Threat, Vulnerability, and/or Consequence) and Mitigation

Source: US DHS CISA

9.2 Exercising



⁴⁰⁶ CISA (November 2019), *A Guide to Critical Infrastructure Security and Resilience*. Available at: <https://cncpic.mai.gov.ro/sites/default/files/2020-03/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf> [accessed 14 May 2025].

Exercising is about rehearsing (a) particular skill(s) or plan in a safe environment and interacting with others who would be affected in, at or around a CI facility by a potential incident. Exercising can be used to assess the validity of training courses, the utility of equipment, interagency/multi-stakeholder arrangements or PPPs. Exercises for CIP can take place at multiple levels:

- ▶ *At the facility level*, a facility-wide exercise can be organized for responding to a terrorist attack involving firearms, or a smaller exercise can be organized with a smaller group of personnel (including private security providers, if relevant) focused on, for example, responding to a terrorist attack using a VBIED.
- ▶ *At the CI owner/operator level*, a company-wide exercise can be organized in the event of a power outage damaging multiple facilities under the owner/operator's purview.
- ▶ *At the sector level*, a sector-wide exercise can be organized to test a sector's resilience to supply chain issues, for example.

National Practice: Malta's Emergency Exercises for Security of Gas Supplies (2020)⁴⁰⁷

As part of Malta's emergency planning efforts for major accidents involving dangerous substances, Enemalta, a major Maltese energy services provider, is required to organize multi-stakeholder emergency exercises involving all relevant stakeholders at the country's only floating storage unit for gas supplies. In addition to fire drills, chemical spills and other non-malicious incidents, drills for security breaches are expected to be exercised four times per year and for explosions, two times per year.

Source: Malta's Ministry for the Environment

The United Nations Office of Counter-Terrorism states that "in practice, different forms of exercises need to be implemented [to protect CI from terrorist attacks], depending on the objectives sought, the number of entities and participants involved, resource availability, and other factors."

"In most cases, the objectives pursued are to:

- ▶ Achieve a common understanding of applicable processes and methodologies. Clarify reciprocal roles and responsibility in CI protection cycles.
- ▶ Create personnel confidence in executing CI-related protection instructions and policies (essential during the stressful phases of a real crisis).
- ▶ Identify weaknesses and introduce any modifications necessary for the safe conclusion of an actual emergency situation.
- ▶ Ensure the operational reliability and compatibility of all communication equipment designated for use during a crisis."⁴⁰⁸

⁴⁰⁷ Malta Ministry for the Environment, Energy and Public Cleanliness (2022), *Malta's Emergency Plan: Gas Security of Supply*. Available at: <https://sostenibilita.gov.mt/wp-content/uploads/2023/11/MT-Gas-SOS-Emergency-Plan.pdf> [accessed 14 May 2025].

⁴⁰⁸ UNOCT, UNSC Counter-Terrorism Committee Executive Directorate (2022), *The protection of critical infrastructures 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 [accessed 14 May 2025].

National Practice: Public Safety Canada's Exercise Guidance for Critical Infrastructure Sectors (2022)⁴⁰⁹

Public Safety Canada encourages sectors and CI owners/operators to develop and exercise a plan to “validate and test risk mitigation actions, plans and systems”. Exercises can serve several purposes, such as to:

- ▶ Encourage the building of relationships across and between industries and disciplines;
- ▶ Clarify roles and responsibilities as well as capabilities;
- ▶ Identify and address dependencies and interdependencies of critical infrastructure;
- ▶ Raise awareness of the risks to critical infrastructure;
- ▶ Provide personnel with an opportunity to practice assigned roles;
- ▶ Determine the state of readiness for a particular incident; and
- ▶ Identify gaps in communication protocols, operating procedures and emergency response procedures.

Public Safety Canada encourages CI owners/operators and stakeholders to consider engaging in a range of different exercise types:

Tabletop exercise: A method of exercising plans in which participants perform some or all of the actions they would take in the event of plan activation to respond to a specific scenario. Specific actions are not performed.

Functional exercise: A method of exercising plans in which participants review and discuss the actions they would take in response to a specific scenario, as presented by a facilitator.

Full operational exercise: A method of exercising plans in which the participants suspend normal operation and activate the plans as if the event were real.

Source: Public Safety Canada

In some cases, governments will require CI owners/operators providing critical services to the public to prepare exercise plans in their function as an entire sector or as an individual provider. In practice, should this be pursued, the process to develop exercise plans should involve all necessary stakeholders, including CI owners/operators, law enforcement, national and local government officials, emergency response authorities, military (if relevant) and others.

⁴⁰⁹ Public Safety Canada (1 July 2010), *Risk Management Guide for Critical Infrastructure Sectors. Version 1*. Available at: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/rsk-mngmnt-gd/rsk-mngmnt-gd-eng.pdf> [accessed 14 May 2025].

National Practice: Estonia's Emergency Act (2017)⁴¹⁰

The Estonian Emergency Act (2017) provides the crisis management framework for resolving emergencies and ensuring the continuity of vital services potentially provided by the nation's CI. Chapter 5 of the Act defines these vital services, including electricity supply, natural gas supply, phone and mobile phone services, payment services, district heating, water supply and sewerage and others. Providers of vital services are required *inter alia* to "organise exercises in order to verify the continuity of the vital service provided thereby at least once every two years".

Source: Government of Estonia

Post-Exercise Evaluations

Exercises should always be followed by an evaluation process which clearly identifies and addresses successes and failures. Failures should be acknowledged and acted upon, with recommendations developed and follow-up actions defined. If CI owners/operators are not provided with genuine feedback (including on their failures) by involved government authorities, for example, they may develop an inaccurate impression of their capabilities to withstand an incident such as a terrorist attack. This could have negative consequences if an attack were to occur and the agreed and planned for processes did not work, resulting in a loss of life or critical services.⁴¹¹

⁴¹⁰ Government of Estonia, Emergency Act (3 March 2017, Estonia). Available at: <https://www.riigiteataja.ee/EN/ELI/511122019004/CONSOLIDE> [accessed 31 August 2024].

⁴¹¹ OSCE (2013), *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*. Available at: <https://www.osce.org/files/f/documents/7/5/103954.pdf> [accessed 14 May 2025].



Enhanced Threat Escalation Options



//

Enhanced threat escalation is vital for critical infrastructure sites, since they operate in environments where threats evolve rapidly, and attacks against them can have local, national, regional or international impacts.

//

10 Enhanced Threat Escalation Options

While many of the physical security measures described in this *Technical Guide* are static, the threat they are designed to mitigate is dynamic. Every CI facility has a specific threat profile. For terrorist threats, this profile may be influenced by global or regional events, the ideology of terrorist organizations, their capabilities within a particular country, their strategic objectives (which also are dynamic), and a range of other factors. It is important to consider these factors when a CI facility's threat profile is assessed by competent security personnel. This is a step that should be done on a routine basis. There may be cases in which general or specific threat information is received by a CI owner/operator meriting a renewed security posture for the facility. While the possible types of such threat information are difficult to predict, they may relate to:

- ▶ A terrorist organization releasing images of a CI facility with an expressed intention to attack it imminently;
- ▶ A government intelligence or law enforcement agency identifying a terrorist attack plot in progress that is targeting a CI facility;
- ▶ A terrorist organization calling on its sleeper cells or lone actors across the world to target a specific type of CI.

In cases such as these, a CI owner/operator may wish to take measures in response to this change in threat level, also known as enhanced threat escalation options. This chapter details such pre-planned measures deployed by CI owners/operators in response to increasing levels of threat.

10.1 National Terrorism Threat Assessments

Participating States across the OSCE area and beyond use national terrorism threat level systems to present a nationwide assessment of the terrorist threats the country faces. These systems align the threat against pre-determined tiered levels, providing a broad indication of the likelihood of a terrorist attack. National terrorism threat levels form one part of a CI owner/operator's assessment of its threat environment and overall risk (for more information, see Chapter 5, Terrorism Threat and Risk Assessment).

Participating State	System of National Terrorism Threat Assessment
United Kingdom ⁴¹²	Low: An attack is highly unlikely Moderate: An attack is possible but not likely Substantial: An attack is likely Severe: An attack is highly likely Critical: An attack is highly likely in the near future
Latvia ⁴¹³	Low: There is a general threat of terrorism Elevated: There is an increasing threat of terrorism High: There is a confirmed terrorist threat to a particular object, economic sector or state region Severe: A terrorist attack has occurred or is imminent
Russian Federation ⁴¹⁴	Elevated: There is information requiring confirmation about the real possibility of a terrorist act being committed High: There is confirmed information about the real possibility of a terrorist act being committed Critical: There is information about a terrorist act that has been committed or about the commission of actions that create an immediate threat of a terrorist act.
The Netherlands ⁴¹⁵	Level 1: Minimal: It is unlikely that a terrorist attack will occur in the Netherlands Level 2: Limited: There is a slight chance of a terrorist attack in the Netherlands Level 3: Significant: A terrorist attack in the Netherlands is conceivable Level 4: Substantial: There is a real chance of a terrorist attack in the Netherlands Level 5: Critical: A terrorist attack in the Netherlands is imminent
Canada ⁴¹⁶	Very Low: A violent act of terrorism is highly unlikely (Measures are in place to keep Canadians safe) Low: A violent act of terrorism is possible but unlikely (Measures are in place to keep Canadians safe) Medium: A violent act of terrorism could occur (Additional measures are in place to keep Canadians safe) High: A violent act of terrorism is likely (Heightened measures are in place to keep Canadians safe. Canadians are informed what action to take) Critical: A violent act of terrorism is highly likely and could occur (Exceptional measures in place to keep Canadians safe. Canadians are informed what action to take)

412 National Counter Terrorism Security Office, ProtectUK (12 March 2022), Threat Levels [webpage]. Available at: <https://www.protectuk.police.uk/threat-levels> [accessed 16 December 2024].

413 Latvian State Security Service (2024), Counterterrorism. Available at: <https://vdd.gov.lv/en/areas-of-activity/counterterrorism> [accessed 16 December 2024].

414 National Anti-Terrorism Committee (August 2023, Russian Federation). Terrorism Threat Levels (in Russian). Available at: <http://nac.gov.ru/urovni-terroristicheskoy-opasnosti.html> [accessed 16 December 2024].

415 National Coordinator for Counterterrorism and Security (2024), Terrorist Threat Assessment Netherlands [webpage]. Available at: <https://english.nctv.nl/topics/terrorist-threat-assessment-netherlands> [accessed 24 July 2024].

416 Government of Canada (2023), Canada's National Terrorism Threat Levels [webpage]. Available at: <https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html> [accessed 16 December 2024].

10.2 Enhanced Threat Escalation Options

For every CI facility, changes in the assessed threat level should trigger a review of the existing security measures in place. One factor that may contribute to a change in an assessed threat level is a change in the national terrorism threat. However, this is not always the case, since national terrorism threat levels rarely provide specific, targeted intelligence or information (i.e., suggesting a threat to the security of a specific CI site). The decision to change the assessed threat level at a CI facility should be made by CI owners/operators, in co-operation with local authorities and others as appropriate.

Enhanced threat escalation options should be designed to provide a structured and scalable approach to ensure that the response is proportionate to the potential risk and can effectively mitigate impacts. Enhanced threat escalation is vital for CI sites, since they operate in environments where threats evolve rapidly, and attacks against them can have local, national, regional or international impacts.

National Practice: Spain's Critical Infrastructure Alert Level System⁴¹⁷

Spain's CI alert system is structured by levels, each associated with a degree of risk: level 1 is low risk, level 2 is moderate risk, level 3 is medium risk, level 4 is high risk, and level 5 is very high risk. The activation of a level triggers the implementation of a set of pre-determined measures adapted to the status and nature of the threat.

Normally, the level of risk coincides with the level established under the country's general Terrorism Prevention and Protection Plan. However, the two levels do not necessarily overlap. A discrepancy may be due to a different assessment of the threat carried out by the agency in charge of CIP. Special consideration is given to the intention, capacity and probability of a deliberate attack being committed against CI owners/operators providing critical services to Spain's citizens.

Source: Spain's Ministry of Interior

At the core of enhanced threat escalation is the ability to dynamically adjust security measures based on new information/intelligence input and risk assessments. This process typically involves multiple levels or tiers of response, each corresponding to a specific threat level. For example, a CI site may start with heightened monitoring and increased communication among security teams at a lower threat level. Additional measures may be implemented as the threat escalates, as for example deploying additional security personnel, activating emergency response protocols, or increasing physical barriers.

In the highest threat scenarios, the CI site might engage law enforcement or specialized response teams and implement lockdown or evacuation procedures (for more information, see Chapter 7, Security Planning and Target Hardening). The key to enhanced threat escalation plans is that each level of response is pre-defined, ensuring that actions are swift and co-ordinated. It is equally important to recognize when to de-escalate and scale back those responses as threat levels decrease, given that they may be unsustainable in the long term.

⁴¹⁷ Plan Nacional de Protección de Infraestructuras Críticas (no date), Nivel de Alerta de Infraestructuras Críticas (NAIC) [webpage]. Available at: <https://cnpic.interior.gob.es/es/naic/> [accessed 24 July 2024].

National Practice: UK National Counter Terrorism Security Office's National Stakeholder Menu of Tactical Options (2023)⁴¹⁸

The United Kingdom provides a "set of options which can be used by the private sector and security industry to enhance the wider national security posture at times of raised threat or in response to a terrorist incident." These options are:

- ▶ Close non-essential access and egress points
- ▶ Search immediate parking areas and review access to them
- ▶ Ensure that all visitors and contractors provide at least 24 hours' notice, prior to attendance
- ▶ Ensure that visitors and contractors are accompanied at all times
- ▶ Cancel or postpone events
- ▶ Ensure all staff are challenged and their identification checked
- ▶ Check all vehicles and personnel on entry, including emergency services
- ▶ Implement a regular and unpredictable search sweep rota across site, including areas hidden from surveillance
- ▶ Restrict and only accept deliveries that are essential
- ▶ Scan all mail and ensure that postal procedures are robust
- ▶ Review and communicate incident response and business continuity plans with staff and neighbouring businesses
- ▶ Ensure full adherence to incident response and business continuity planning checklist
- ▶ Ensure that lockdown procedures are known, tried and tested
- ▶ Ensure suitability of egress routes and muster points
- ▶ Ensure that all staff are briefed on roles and responsibilities during an incident in line with response plans and procedures
- ▶ Ensure contents of crisis response and Public Access Trauma First Aid Kits are up-to-date, secure and easily accessible
- ▶ Prepare alerts, alarms and pre-scripted messages
- ▶ Ensure that staff are briefed on Threat and Response Levels
- ▶ Ensure that staff are briefed in observing, detecting and responding to suspicious activity
- ▶ Ensure that any suspicious activity is reported in a timely manner
- ▶ Implement communication links with surrounding premises to pass on information and suspicious activity
- ▶ Actively monitor [video surveillance systems] at all times and review out-of-hours footage
- ▶ Ensure that [video surveillance systems are] focused on all communal areas and vulnerable points
- ▶ Ensure a strong security posture through Security Minded Communications
- ▶ Review patrol and positioning of security staff
- ▶ Ensure that perimeter fencing and security lighting is checked
- ▶ Implement emergency change to shift patterns and agree plan with staff in advance

⁴¹⁸ National Counter Terrorism Security Office, ProtectUK (14 December 2023) National Stakeholder Menu of Tactical Options. Available at: <https://www.protectuk.police.uk/advice-and-guidance/security/national-stakeholder-menu-tactical-options-0> [accessed 16 December 2024].

- ▶ Join up resources with neighbouring businesses and contacts
- ▶ Cancel all non-essential training and meetings
- ▶ Ensure a communication strategy is agreed and document all decisions including rationale
- ▶ Ensure supporting technology, such as access control systems, are in working order
- ▶ Establish or review a Counter-Unmanned Aerial Vehicle/Unmanned Aerial System Plan.

Source: UK National Counter Terrorism Security Office

10.3 Costs of Enhanced Threat Escalation Options

Threat escalation options can be categorized based on their associated costs. By categorizing threat escalation options this way, CI owner/operators can better evaluate and choose appropriate responses based on their strategic goals and resource availability.



High-cost options

Significant expenditure of resources, such as deploying government security forces or implementing extensive security systems, which can strain a CI owner/operator's capability when used disproportionately.



Shared-cost options

The burden is distributed among multiple parties, such as through PPPs, reducing individual expenses while leveraging collective strength.



Low-cost options

Minimal resources, often relying on existing capabilities that can achieve objectives without substantial financial or logistical commitments



No-cost options

Utilize readily available or intangible assets leveraging influence and relationships without direct financial outlay.



PROTECT

PROJECT OVERVIEW

The OSCE's Project on the Protection of Vulnerable Targets from Terrorist Attacks, or Project PROTECT, enhances national approaches across the OSCE area to the protection of vulnerable targets from terrorist threats and other hazards through the provision of specialized guidance, technical assistance and opportunities for regional co-operation and dialogue on effective security practices.