UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

1

Protecting vulnerable targets from terrorist attacks

GOOD PRACTICES GUIDE

Introduction

Global Programme on Countering Terrorist Threats against Vulnerable Targets

Implemented in partnership with: UNITED NATIONS SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE (CTED) UNAOC United Nations Alliance of Civilizations unicri United Nations Interregional Crime and Justice Research Institute

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

Protecting vulnerable targets from terrorist attacks

GOOD PRACTICES GUIDE

Introduction

Global Programme on Countering Terrorist Threats against Vulnerable Targets

Implemented in partnership with: UNITED NATIONS SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE (CTED) UNAOC United Nations Alliance of Civilizations unicri United Nations Interregional Crime and Justice Research Institute

Contents

Preface

At its seventh review of the United Nations Global Counter-Terrorism Strategy, the General Assembly encouraged the Office of Counter-Terrorism (UNOCT) 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)" (General Assembly resolution 75/291, para. 74 (italics added for emphasis)).

It is in this context that UNOCT's Global Programme on Countering Terrorist Threats against Vulnerable Targets[1] has prepared this document as an introductory guide on the protection of vulnerable sites against terrorist acts. Together with its four specialized thematic modules,[2] it complements *The Protection of Critical Infrastructure against Terrorist Attacks: Compendium of Good Practices*[3] by focusing on "soft" targets (i.e., public places) as distinct types of sites worthy of a dedicated security approach by a wide range of actors.[4]

By introducing basic concepts, painting the broad threat landscape and providing a non-sector specific overview of stakeholders' roles and responsibilities, this introductory module sets the stage for a more in-depth and sector-specific examination of the challenges and opportunities relating to the protection of religious sites, tourist venues, urban centres and the threat posed by unmanned aircraft systems (UAS) to vulnerable targets.

[1] The Programme is implemented by the Office of Counter-Terrorism (UNOCT), in partnership with the Counter-Terrorism Committee Executive Directorate (CTED), the United Nations Alliance of Civilizations (UNAOC) and the United Nations Interregional Crime and Justice Research Institute (UNICRI), in close consultation with other relevant organizations, including INTERPOL. See www.un.org/counterterrorism/vulnerable-targets.

[2] The four thematic modules focus on the protection of religious sites, tourist venues, urban centers and threats posed by unmanned aircraft systems (UAS) to vulnerable sites in general.

[3] The Compendium was developed in 2018 by the Working Group on the Protection of Critical In-frastructure including Vulnerable Targets, Internet and Tourism Security of the Counter-Terrorism Implementation Task Force (CTITF). In 2019, CTITF was folded into the Global Counter-Terrorism Coordination Compact. Under this new structure, the above-mentioned Working Group and the Working Group on Preventing and Responding to Weapons of Mass Destruction Terrorist Attacks were combined to create the Working Group on Emerging Threats and Critical Infrastructure Protection.

[4] The present document and the four thematic modules adopt the terminology used in General Assembly resolution 75/291, in which public places are viewed as "soft" targets.

This introductory module and the four thematic modules feature a selection of case studies illustrating how key security-related principles – including internationally endorsed recommendations – have been operationalized by Governments, private-sector entities, operators of vulnerable sites and civil society organizations. The modules also summarize the content of several tools (e.g., manuals, handbooks, compendiums) which provide guidance on policies and operational actions to reduce the vulnerability of the sites and increase their resilience.

The analytical framework, case studies, tools and the resources featured in this introductory module and in the thematic modules are the result of intensive desk research, a formal request for inputs from all 193 Member States, discussions with individual experts, international organizations and project partners, as well as input from the Working Group on Emerging Threats and Critical Infrastructure Protection of the Global Counter-Terrorism Coordination Compact.[5] Important insight was obtained from a series of online Expert Group meetings organized by UNOCT over the course of 2021, each of which brought together national and international experts and practitioners from United Nations Member States, international and regional organizations, civil society groups, the private sector and academia. The process also benefited from the input of UNOCT's Gender Advisor and a dedicated human rights consultant in UNOCT's Special Projects and Innovation Branch.[6]

[5] See www.un.org/counterterrorism/global-ct-compact.

[6] This introductory module and the four thematic modules emphasize the need to mainstream gender in the design and implementation of action plans, training and the practice and conduct of exercises of security and emergency plans; develop gender-sensitive security planning; recognize and support the role of women in the security of vulnerable targets; tackle gender biases in law enforcement; collaboratively address security challenges specific to women in urban spaces; and address gender bias in technologies used by law enforcement and security sectors, among others. Context-specific considerations regarding gender equality should be incorporated from planning to execution and evaluation of all measures highlighted in the modules.

Index of boxes

Index of case studies

Index of tools

[1]

Understanding the basic concepts

1.1 Vulnerable, soft and hard targets, crowded and public spaces

The concepts of vulnerable, soft and hard targets, and crowded and public spaces have only recently come into common use in the counter-terrorism space.[7] Moreover, their definitions are not included in any international legal framework. To some degree, their meaning changes depending on the context and the type of discussion (policy, legal, operational, technical) in which they are employed.

In line with resolution 75/291 adopted by the General Assembly at the seventh review of the Global Counter-Terrorism Strategy, this introductory module and the four thematic modules consider that vulnerable

[7] The General Assembly mentioned “vulnerable targets” for the first time in 2006. See resolution 60/288, Annex, Plan of Action, Pillar II-Measures to prevent and combat terrorism, para. 18, in which Member States undertook to “step up all efforts to improve the security and protection of particularly vulnerable targets, such as infrastructure and public places”.

targets include critical infrastructure and public places, or "soft" targets,[8] and that their protection needs are best met though gender-responsive human rights-compliant approaches.[9]

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.[10] 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.

The "soft" character of certain places stands in contrast to the "hard" nature of some others. In policy, military and law enforcement conversation, soft targets are considered in juxtaposition to hard targets. The latter refers to sites that are generally staffed or frequented by government officials and are usually protected by strong physical security measures (e.g., embassies, military posts, international summit meetings).

To a large extent, the notion of soft targets overlaps with that of crowded places. The latter emphasizes the high density of people gathering within and around certain places (e.g., visitors to a tourist site, audience at a concert, congregants at a religious ceremony) as a specific factor of vulnerability or attractiveness for hostile actors. The notion of soft targets is also frequently used as a synonym for public spaces, although not all public spaces are necessarily (or always) crowded, and crowded spaces are not necessarily public or especially vulnerable sites (e.g., several people attending an event in a highly secured government building).

1.2 Soft targets versus critical infrastructure

The notion of soft target is usually differentiated from that of critical infrastructure, although the latter may be "soft" by virtue of not being "hard" or secured. Critical infrastructure broadly refers to assets, systems and processes that are vital for the provision of essential services (e.g., health, water, telecommunications, transport, energy), and

[8] These modules focus on public civilian places, or "soft" targets. Protection of critical infrastructure is dealt with in *The protection of critical infrastructures against terrorist attacks: Compendium of good practices* (2018), available at www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/eng_compendium-cip-final-version-120618.pdf.

[9] Section 4.1 provides an overview of Member States' obligation to ensure that any measures taken to counter terrorism comply with all their obligations under international law, in particular international human rights law and, in the context of this document, when designing and implementing measures to protect "soft" targets.

[10] As highlighted by the Security Council Counter-Terrorism Committee, "the appeal of soft targets to terrorists derives not only from their open format and limited security to facilitate access, but also from the potential to generate civilian casualties, chaos, publicity and economic impact" (S/2018/1177, para. 51).

whose disruption has the potential to cause extensive negative impacts[11] on the security, as well as the social and economic well-being of a community.[12]

Key elements of differentiation:

- A soft target is typically a physical place, while critical infrastructure may be a process, including information systems and networks;[13]
- Soft targets are usually open to and accessible by the public; in contrast, critical infrastructure is typically off-limits to the general public;[14]
- The rationale for protecting soft targets and critical infrastructure differs: critical infrastructure is protected because it forms the backbone of the life of a country and because the cascading effects that disruptions in one sector can generate on other sectors can potentially lead

[11] Although the tourist sector is typically not framed as a critical sector in a technical sense, in some Member States, it can represent a very significant proportion of national GDP. When terrorist acts affect countries whose economies are largely dependent on tourism, the overall financial and social impacts can be equivalent to – if not greater than – those caused by the collapse of a critical sector.

[12] The *Compendium of good practices* references several national definitions of “critical infrastructure”. It also examines the methodologies followed by countries to identify sectors and assets to be regarded as critical (see section 2.4.1, Determining “criticality”, p. 39).

[13] The notion of “critical information infrastructure” is key to understanding the role played by computer-controlled systems in governing the operations of energy plants, dams, bridges, food supply chains, among others.

[14] The fact that critical infrastructure is closed to the public does not imply that it is better protected than soft targets. In the absence of adequate security measures, critical infrastructure can be extremely vulnerable and thus especially enticing to terrorist actors.

to general paralysis. This explains why critical infrastructure protection efforts – unlike those for soft targets – are directed not only against the risk of terrorist attacks, but also the consequences of other human conduct (whether intentional or negligent) as well as, crucially, the disruptive impact of natural events.

These conceptual differences imply that the institutional and regulatory frameworks needed to protect critical infrastructure may not automatically apply to soft targets. This is apparent in the criteria used by Member States to distinguish between critical and non-critical infrastructure. These criteria – which are often based on prediction models about the severity, duration, geographical scope and economic consequences of disruptive events – may not be suitable for determining what constitutes soft targets.

Despite the differences, however, the task of protecting soft targets and critical infrastructure presents many shared challenges, which suggests that both should benefit from the following synergetic approach:

- Measures designed to protect critical infrastructure can offer a valuable source of inspiration for soft target protection and vice versa. At a basic level, many of the physical security tools used to deliver access control to critical infrastructure (e.g., guard posts, fences, metal detectors) are also typically employed to filter public access to soft targets;[15]
- The way in which attacks against critical infrastructure have been managed can provide useful warnings and lessons learned in efforts to prevent and mitigate risks and handle crises involving soft targets;
- The protection of both critical infrastructure and soft targets is predicated on the need for site operators and public authorities to follow risk and crisis management approaches. The procedures and institutional stakeholders involved in national threat assessments, and the response to attacks against critical infrastructure and soft targets are often the same or overlap significantly. In addition, often, critical infrastructure and soft targets are privately owned and operated, which makes the development of public–private partnerships (PPP) a central feature of preparedness and protection efforts for both;
- The interplay between critical infrastructure and soft target protection is a multidimensional one, requiring close policy, institutional and operational coordination. Critical infrastructure often enables soft targets to function; for example, uninterrupted electricity supply is needed for a sporting event to take place, and disruption in the provision of basic services, such as electricity, may not simply leave those present in a concert hall in the dark and interrupt the performance, but can potentially be part of a strategy to make evacuation efforts more difficult during a terrorist attack. Furthermore, a successful terrorist attack against a crowded tourist or religious site may cause critical infrastructure – and even an entire critical sector – to collapse; for example, hospitals may rapidly fill up beyond their capacity or communication networks may stop working as they are overwhelmed with users' requests. Attacks

[15] Other examples of security measures that can be employed to protect both critical infrastructure and soft targets can be found in the "smart city" concept and related technological solutions that seek to make modern cities more secure. For example, digital gun detection sensors may be useful for protecting assets as diverse as street markets, government buildings or transportation networks.

against soft targets may have particularly severe effects on critical infrastructure when they occur in urban areas, where the two co-exist and interact in complex and densely populated spaces. This underlies the need for an approach that considers both as part of a single multi-faceted system.

Box 1.
Aligning soft target and critical infrastructure protection efforts

"Critical infrastructure, such as power grids, dams, and government facilities, will continue to remain high on the terrorist target list. Soft targets are often part of the critical infrastructure frameworks in many nations. This ensures the infrastructure risk management system also addresses the threat against soft targets. For example, attacks on people in a train station are part of the suite of potential attack scenarios against transportation systems (air, rail, maritime). Many of the key principles that governments follow when protecting critical infrastructure against terrorist acts can also be effective for protecting soft targets. …Both soft target protection and critical infrastructure security and resilience require the same basic policy and practical framework for preparedness: prevention, protection, mitigation, response and recovery. They should be mutually reinforcing efforts …soft target assessments should be done in conjunction with the assessment of a government's capacity to develop plans and partnerships to protect critical infrastructure. In some cases, soft targets and critical infrastructure may overlap (commercial facilities) and in other cases, they may not be the same (energy sector)."

Source: Antalya Memorandum, 2017 - Good Practice 5.

[2]

The terrorist threat to vulnerable targets

Over the past few years, the presence of persistent terrorist threats against sites where large crowds of people gather has been regularly highlighted by intelligence and law enforcement agencies worldwide. In many cases, the public is generally aware of the threat because terrorist organizations have publicly called for or threatened attacks against such places.[16]

Arguably, terrorists may shift their attention to soft targets in response to strengthened security measures that make “hard” targets such as government buildings, military installations and others more difficult to attack. The situation can be likened to a balloon effect whereby better law enforcement and security in certain geographical areas may cause a criminal problem to shift to a less effectively policed territory. Following a similar logic, as the civil aviation sector responded to terrorist threats by adopting increasingly tighter pre-boarding security measures, terrorist groups have shifted their attention to surrounding, less protected areas.[17]

At the same time, as highlighted in the Antalya Memorandum of the Global Counterterrorism Forum, “the recent uptick in knife and heavy vehicle attacks, breaking from the use of armed individuals or teams of gunmen, sometimes accompanied by suicide bombers, shows flexibility and willingness to accept smaller casualty counts”.[18]

While the use of rudimentary weapons has characterized several recent attacks, the possibility of terrorist actors seeking to employ weapons of mass destruction on soft targets cannot be ruled out. The best known attempt in this regard is the 1995 sarin gas attack perpetrated by the terrorist group Aum Shinrikyo in the Tokyo subway system.[19]

[16] In November 2016, for example, Islamic State (ISIL) posted a call on its online magazine for its sympathizers to target places such as large outdoor conventions and celebrations, pedestrian-congested streets, outdoor markets, festivals, parades and political rallies.

[17] The bombing attack in Brussels in 2016 illustrates this point well. By striking at the airport’s check-in area before the security control, terrorists chose an area that was full of passengers and suitcases, which enabled them to minimize the risk of their plan being foiled, while maximizing the chances of causing extensive damage.

[18] A specific threat is posed by laden-borne vehicles parked and blown up in the proximity of soft targets. Historically, many terrorist groups have employed ambulances for this purpose, exploiting the appearance of harmlessness that is conveyed by such a vehicle.

[19] A less well-known incident occurred in 1984 with the intentional contamination of salad bars with Salmonella at 10 restaurants in Oregon, United States of America, by a group seeking to influence a local election. The incident illustrates the relative ease with which hostile actors can potentially execute a bioterrorist attack on soft targets.

Terrorist acts against soft targets continue to be committed for hostage-taking purposes[20] and may potentially come in the crosshairs of terrorists as places from which to obtain dangerous material to be used in terrorist activity elsewhere.[21]

The nature and level of threats against soft targets are influenced by local factors as well as the profile of the violent actors seeking to inflict damage on them and the people they host. Terrorists' choices to attack a certain site as opposed to another depends on a variety of considerations such as their personal grievance against specific groups (e.g., certain religious communities, tourists from certain countries, perceptions of amoral activities) and the sites' actual or perceived degrees of vulnerability. From a general standpoint, terrorist actors may decide to attack soft targets for a variety of reasons.[22] In addition to the motivations that are commonly associated with decisions to strike vulnerable sites (e.g., presence of large crowds in addition to weak or no security measures, proximity to the group's area of operation or access, possibility of achieving quick media coverage), other motivations may include the following:

- Compensating for weakness: if a terrorist group and/or a lone actor does not have the resources or the planning capabilities

[20] After taking 850 people hostage at the Moscow Dubrovka theatre, for example, terrorists placed specific political demands on the Russian Government as a condition for their liberation. In northwest Nigeria, the frequent mass kidnappings of girls and boys at boarding schools are generally committed for the purpose of requesting ransom.

[21] After observing the lack of proper security measures in several medical facilities that stored radioactive material, a 2012 report
by the United States Government warned against the risk of hostile actors exploiting security loopholes to steal such material and assemble a dirty bomb (see United States, Government Accountability Office, 2012).

[22] See Hesterman, 2019, pp. 23-26.

to conduct a successful attack against a hard target, it may fall back on a soft target;

- As a last resort: a terrorist group whose appeal and/or operational capabilities are weakening may turn its attention to easy-to-attack soft targets to regain credibility and attract new recruits;
- Testing a new strategy, tactic or weapon: soft targets may be used as testing grounds to prepare for bigger operations;
- Flexibility: soft targets may allow more room for improvisation in case a change in the original plan is needed for some reason.

[3]

Soft targets’ vulnerability to terrorist attacks

Each type of site has its own unique set of vulnerabilities deriving primarily from its characteristics and the resources available to the people who run or operate it, and those who visit and attend it. For example, religious communities and sites usually have an “open-door” policy for welcoming everyone and not asking questions about their identity, religion or provenance. Therefore, in carrying out an attack on a religious site, perpetrators may exploit the “surprise” element, especially given that worshipers may be immersed in their own spiritual practice and not pay attention to others. From a positive angle, those regularly attending a religious site may be able to take advantage of escape routes and emergency exits more readily than one-time visitors to a tourist site.

Vulnerabilities also vary significantly depending on the sites’ socioeconomic contexts, geographical locations and surroundings, as well as their physical features. An open-air market, for example, may be more difficult to attack effectively by releasing toxic agents, than a closed site, such as a theatre. In contrast, the audience in a theater will be significantly less exposed to hostile drone activity than a street market.

Despite the differences, a number of vulnerabilities can be identified that are be common across sectors and related to cultural, institutional, legal and financial factors.

- *Cultural factors:* Vulnerabilities may originate from reluctance to enhance security due to underestimation of the likelihood and/or the impact of a terrorist attack. Such an attitude on the part of some facility owners/operators may be underpinned by a “tolerant” culture that may tend to sacrifice a sound security posture for the sake of a more recreational experience for tourists and visitors to shopping malls, religious or tourist sites or cultural events, among others.

  Another potentially relevant factor is “security fatigue”: Outside of periods of heightened vigilance, usually in the aftermath of a terrorist attack, sustaining a culture of security may be a difficult long-term attitude for site operators, the public and other stakeholders to develop. Security actors themselves may attract suspicion or not be well received in certain communities (e.g., religious congregations).

  Specific vulnerabilities may also be the result of cultural barriers – such as different backgrounds, expectations and mindsets – and the associated reluctance to adopt more stringent security measures. That may make establishing effective public–private partnerships (PPPs) among the various stakeholders needed to cooperate in the protection of vulnerable sites a critical, but also challenging endeavour.[23]

- *Institutional and legal factors:* Although information-sharing is an essential ingredient of any risk/crisis management system aimed at effectively protecting vulnerable targets, this imperative may be hampered by insufficient inter-agency coordination due to regulatory gaps, unclear divisions of labour, among others. In addition, intelligence agencies may encounter legal obstacles to their disclosing classified information to operators of vulnerable sites.

  On the ground, misunderstandings may arise between landlords and tenants of vulnerable sites, and between site operators and neighbouring businesses over who is responsible for security upgrades or the management of security personnel in so-called grey areas, that is, spaces with disputed ownership structures or no clearly identified owner. This may result in failure to implement needed security interventions for preventive purposes, and potentially lead to ineffective post-incident responses.

- *Financial factors:* Many vulnerable sites have limited budgets available for security purposes. Security measures can be costly to implement where they require physical changes, addition to infrastructure, hiring of new security companies or personnel who require training. In addition, they may not be able to rely on financial incentives (e.g., funding, subsidies, tax breaks) to support the implementation of security upgrades. In the face of severe budgetary constraints, for example, operators of vulnerable sites may opt for investing scarce resources in fast-rewarding marketing operations rather than long-term security upgrades, and thus fail to address easily exploitable vulnerabilities.

[23] Public-sector authorities may approach site operators with uncompromising requests to execute financially burdensome security upgrades. In turn, operators of privately owned facilities may hesitate to engage in solid and durable PPPs due to factors such as their inability to see the business value of such a partnership, suspicion of public-sector motives, and little incentive due to lack of regulatory requirements for private-sector engagement.

[4]

Risk mitigation and response: stakeholders' roles

The foundational paradigm for protecting vulnerable targets against terrorist acts – regardless of type, size or function – lies in coordinated security planning driven by a risk/crisis management approach that is implemented by site operators and government authorities at both the national and local levels.

Risk management is defined by the United Nations Office for Disaster Risk Reduction (UNDRR) as the "systematic approach and practice of managing uncertainty to minimize potential harm and loss. ...Risk management comprises risk assessment and analysis, and the implementation of strategies and specific actions to control, reduce and transfer risks".[24]

The importance of ensuring closely coordinated risk management approaches involving all levels of government and other

[24] See United Nations International Strategy for Disaster Reduction, Terminology on Disaster Risk Reduction, 2009.

relevant actors should not be underestimated. In resolution 75/291, the General Assembly encouraged 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 the effective interaction of all stakeholders involved" (para. 71). Also, as highlighted in the GCTF Antalya Memorandum, "data to inform risk assessment can come from a variety of sources. National assessments by government security experts will incorporate sensitive and classified information accessible only to official national representatives. They should then be integrated with open-source information and the information from the industry and the private sector in a form accessible to the local security forces which need it. The public and private sectors both use risk analysis to identify and mitigate vulnerabilities in physical infrastructure and in their standard operating procedures and response plans" (p. 5, Good Practice 3).

As to crisis management, this broadly refers to the processes that need to be activated when an incident occurs. The three major steps in crisis management are developing contingency/emergency plans, identifying the crisis, and confronting and resolving the crisis.[25]

The following sections provide a snapshot of the roles that individual stakeholders can and should play in the protection of vulnerable targets within the prism of a risk and crisis management paradigm. The same stakeholder-based approach is followed in the specialized modules, which delve into how governmental and non-governmental actors can specifically contribute to the protection of religious and tourist sites, urban centers as well as vulnerable sites in general against the terrorist use of UAS.

4.1 Member States

All levels of government need to be involved in the protection of vulnerable targets according to their respective competences within the legal framework of the individual country.

General counter-terrorism measures constitute the basic tools to be employed. The full range of counter-terrorism tools and policies should be leveraged, in full compliance with human rights and gender equality standards, and applicable international law. These include measures to counter violent extremism; comprehensive and tailored prosecution, rehabilitation, and reintegration (PRR) strategies; prevention of terrorist access to weapons; international cooperation and information-sharing mechanisms stemming from international treaties; border security and management to prevent cross-border movement of terrorists; stemming the flow of foreign terrorist fighters (FTFs); and consignments involving dual-use items (e.g., the manufacture of improvised explosive devices (IEDs)).

[25] The *Compendium of good practices* provides additional information and guidance on risk and crisis management that are equally applicable to critical infrastructure and soft targets protection efforts (see sect. 2.6).

Key roles and responsibilities for protecting vulnerable targets within a country's policymaking and law enforcement capacities and for supporting counter-terrorism efforts through intelligence/information collection and analysis are outlined below.

Box 2.
Protection of public spaces: European Council conclusions

In June 2021, the European Union Justice and Home Affairs Council adopted a number of recommendations addressed to European Union member States on the protection of public spaces against terrorist acts. The following list summarizes the key points:

- Work towards the introduction or enhancement of national as well as regional and local strategies for increased resilience of local communities and public spaces;
- Support initiatives to establish secure operational and European Union interoperable communication for law enforcement agencies and other security practitioners to be able to properly protect and respond in case of cross-border cooperation in the area of public spaces and major events;
- Examine domestic legal frameworks with a view to restricting non-legitimate carrying of bladed weapons in public spaces and major events;
- Study and analyze security guidance and tools for rental vehicle operators to prevent and mitigate the risk of vehicle attacks in public spaces;
- Screen domestic legislation and local regulation with a view to ensuring that they contain clear provisions with regard to administrative requirements and responsibilities for those who plan and manage the security of public spaces;
- Continue to plan and organize practical exercises and joint training between local authorities, law enforcement, civil protection, medical emergency, private businesses, private security firms and other stakeholders in order to improve the preparedness and response of law enforcement and the first response community; and
- Incorporate crime prevention through environmental design (CPTED) techniques at local level and through public–private partnerships and projects, as a mechanism for the protection of public spaces, namely to prevent vehicle ramming, explosions, chemical, biological, radiological or nuclear (CBRN) events, improvised incendiary devices, active shooters and other modi operandi in spaces such as railway and underground railway stations, public areas of international airports, places of worship, business areas, tourist attractions (e.g. monuments and museums), universities and schools, and others which the risk assessment may advise.

Source: https://data.consilium.europa.eu/doc/document/ST-9545-2021-INIT/en/pdf

4.1.1 Member States' obligation to adopt a human rights-compliant and gender-responsive approach to countering terrorist threats to soft targets

Terrorism poses a serious threat not only to international peace and security, but also to the enjoyment of human rights, and social and economic development. Member States take steps to effectively counter and prevent terrorism as part of their obligation under international human rights law to protect the rights to life and personal security. This obligation is particularly important considering the potential impact that attacks on soft targets may have on populations, particularly in light of their openness, accessibility and nature, as places where large crowds of people gather.

States' duty to safeguard human rights implies the obligation to take necessary and adequate measures to prevent, combat and punish activities that endanger these rights, such as threats to national security or violent crime, including terrorism. In this respect, States should take guidance, inter alia, from the United Nations Global Counter-Terrorism Strategy, which emphasizes that effectively combatting terrorism and ensuring respect for human rights are not competing, but complementary and mutually reinforcing goals. Indeed, the promotion and protection of human rights constitutes an independent pillar and a cross-cutting necessity to ensure successful delivery of all four components of the Strategy. The Security Council has consistently and repeatedly affirmed that States should ensure that any measures taken to counter terrorism comply with all their obligations under international law, in particular international human rights law, international refugee law, and international humanitarian law. In resolution 2178 (2014), the Security Council noted that "failure to comply with these and other international obligations, including under the Charter of the United Nations, is one of the factors contributing to increased radicalization and fosters a sense of impunity".

Moreover, relevant provisions of Security Council resolutions require that any measures taken to prevent and combat terrorism comply with States' obligations under international law, in particular international human rights law, international refugee law, and international humanitarian law. Counter-terrorism strategies should also take into account gender and age sensitivities, the best interests of the child and the differential impact of terrorism and violent extremism conducive to terrorism on the human rights of women and girls (see S/2018/1177, annex, para. 8).

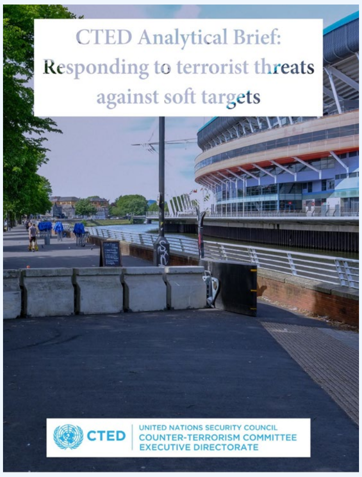
In the interest of addressing terrorist threats on soft targets, State authorities may take temporary measures that may result in the limitation of certain rights, provided these restrictions comply with the conditions set out in international human rights law. Such measures must be in genuine response to the threat at hand, be necessary by the exigencies of the situation, have a clear legal basis, and be proportionate to the pursuance of legitimate aims. States must ensure that satisfactory safeguards are set up to protect against arbitrary and disproportionate interference with human rights in this context. To meaningfully comply with these obligations, States are strongly encouraged to conduct regular human rights assessments of measures taken to tackle terrorist threats to soft targets, and ensure that such measures are evidence-based and therefore efficient, and do not reinforce exclusion, prejudice or biases, nor hinder access to or the use of the space by certain groups or populations. Likewise, integrating gender perspectives in the protection of vulnerable targets is integral to effective and efficient risk-mitigation strategies, as they consider not only the gender-specific security needs of women, men, boys and girls, but also how the underlying gendered relationships, stereotypes and dynamics influence patterns of security and insecurity, as well as vulnerabilities.

4.1.2 Policymakers

Within the parameters set by an overarching government strategy, individual ministries and departments should design their engagements based on the characteristics of the sites over which they have policy, regulatory, inspection or other responsibility. Also, partnerships should be forged with different categories of stakeholders. For example, while the protection of religious sites will entail engaging religious leaders in sustained dialogue, preventing terrorist attacks on tourist sites will require reaching out to the tourism industry. Likewise, while the security of vulnerable urban centers will rely on properly equipping municipal authorities, stemming the threat of terrorists using unmanned aircraft systems (UAS) on soft targets will hinge on creating synergies between government agencies and providers of counter UAS technologies.

The fact that different types of vulnerable sites may require tailored policy and regulatory interventions, however, does not make it less important for Governments to design an overarching approach to their protection. Such an approach should take stock of shared priorities and challenges, identify common operational needs, and optimize the use of available resources and tools for prevention, response and recovery purposes.

Tool 1.
Responding to terrorist threats against soft targets – CTED Analytical Brief (www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted-analytical-brief-soft-targets.pdf)



CTED Analytical Brief:
Responding to terrorist threats
against soft targets

CTED | UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE

The Counter-Terrorism Committee Executive Directorate (CTED) prepared this Brief in accordance with Security Council resolution 2395 (2017), which directed CTED to conduct analytical work on emerging issues, trends and developments and to make its analytical products available throughout the United Nations system. CTED also stresses the importance of involving civil society in soft target protection initiatives and emphasizes the need to enhance information-sharing and trust-building to strengthen resilience without disclosing confidential information or disrupting the population's way of life.

Tool 2.
Antalya Memorandum on the Protection of Soft Targets in a Counter-terrorism Context – Global Counter-terrorism Forum (GCTF), 2017

(www.thegctf.org/About-us/GCTF-framework-documents)

The good practices contained in the Memorandum are part of GCTF's Soft Target Protection Initiative, which is intended to inform and guide Governments and private industry as they work together to develop policies, practices, guidelines, programmes and approaches for protecting their citizens from terrorist attacks on soft targets. In recognition of the fact that no plan or strategy can protect all potential targets, the Memorandum seeks to synthesize the expertise developed on the topic in the course of various regional workshops held in 2016 and 2017.

The 13 resulting good practices are grouped within three blocks of themes:

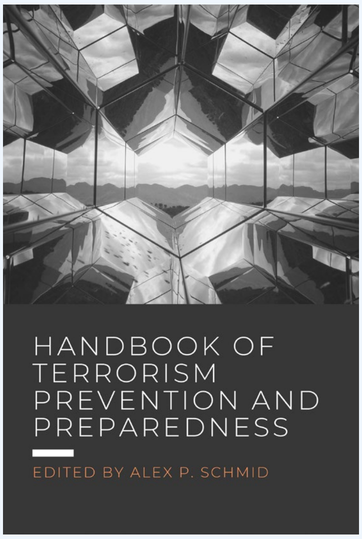
1. Understanding the threat, then identifying and prioritizing soft targets based on continuous risk assessments and established effective information sharing that promotes practical cooperation and collaboration at all levels of government (international, national, regional and local);
2. Building public–private sector partnerships to enable and improve security cooperation, and engaging the public and industry through clear and consistent messaging on the nature of the threat and proper preparedness;
3. Preparing, planning and protecting by prioritizing resources, engagement, exercises and training to improve government, industry, and public awareness and preparedness for prevention, response and recovery.

Tool 3.
Handbook of Terrorism Prevention and Preparedness – International Centre for Counter-Terrorism (ICCT)

(https://icct.nl/handbook-of-terrorism-prevention-and-preparedness)

Prepared by the International Centre for Counter-Terrorism (ICCT), the Handbook is a vast resource tool covering various aspects of anticipatory counter-terrorism, ranging from prevention of radicalization to prevention of preparatory acts, and preparedness for mitigating the consequences of attacks.

Chapter 27 in particular deals with "Layers of Preventive Measures for Soft Target Protection Against Terrorist Attacks" based on the notion that while single layers might be insufficient to stop a terrorist attack, their combination can become a powerful preventive



tool. The Handbook identifies 13 layers of preventive measures (LPMs) for mid- and downstream soft target protection:[26]

LPM1: Engage in ongoing collection of traditional open-source information (e.g., print media, radio, TV, academic studies, NGO reports) by professional monitoring agencies;

LPM2: Monitor extremist online activities with potentially violent consequences (e.g., hate speech that can be a predictor of hate crimes, including terrorism) in social media and on the dark and deep web;

LPM3: Intelligence collection from surveillance and eavesdropping on known and suspected extremist individuals and groups, and their sponsors (e.g., by bugging their phones, computers, cars, homes);

LPM4: Use of undercover agents for infiltration into violent groups and/or attracting informers from such groups (e.g., terrorists released from prison because they served their terms and returned to their groups); use of sting operations where legal;

LPM5: Exchange of finished (not raw) intelligence (signal and human), within and between government agencies, and with trusted intelligence and security agencies abroad;

LPM6: Analyse terrorist propaganda and construct counter- and alternative narratives that are backed up by credible actions to prevent and counter (further) radicalization;

LPM7: Encourage family members and friends of radicalizing young men and women to confidentially report their concerns to a trusted organization (not the police or intelligence services), while assuring them that this does not lead to the arrest of their family member or friend, but will bring them in contact with counsellors in youth mentoring or deradicalization programmes;

LPM8: Monitor young people with a history of crime and/or mental health issues who appear inclined to join extremist groups, and develop special activity programmes (e.g., sports and job training) for such youth at risk;

LPM9: Offer incentives to disillusioned members of terrorist organizations to leave the group and subsequently publicize, if they agree, their testimonies, and help them start in your career;

LPM10: Offer rewards for information tip-offs from the general public that can help to prevent a terrorist attack and/or lead to the arrest of violent extremists and terrorists;

(continued)

[26] While mid-stream prevention aims to reduce the risk of a terrorist group preparing a terrorist campaign, downstream prevention seeks to mitigate the risk of the execution of individual terrorist operations.

LPM11: Monitor and follow up specific ordinary crimes (e.g., theft of explosives), which might be perpetrated in connection with the preparation of a terrorist attack;

LPM12: Have rapid reaction protocols ready for dealing with credible attack warnings (e.g., on social media) received from the perpetrator or a spokesperson of the terrorist organization;

LPM13: Issue warnings via mass and social media to the general public when receiving credible new information about an impending terrorist attack, and advise the public to be vigilant and look out for identified suspects and suspicious objects; also open a special phone hotline to report to responders.

4.1.2.1 Designing a strategy on soft targets

The Guiding principles on foreign terrorist fighters, known as the Madrid Guiding Principles,[27] urge Member States, acting in cooperation with local authorities, to "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" (S/2018/1177, Annex, Guiding principle 50 (c)).

It is advisable that strategies adopted at the national level be the result of extensive consultation among government departments, private-sector entities/site operators and civil society organizations (see sect. 4.2.2 below) and aim at addressing a set of critical issues such as:

- What constitutes "soft" targets, and what criteria should be used to identify them?
- How is the threat landscape against soft targets going to be identified and assessed?
- What are the roles and responsibilities of individual government departments and the different levels of government (e.g., federal, state, county, municipal) in addressing threats and responding to incidents?
- Which authorities need to be involved, and which procedures should be set in motion for the purpose of risk and crisis management?
- What forms of public–private partnerships (PPPs) could be usefully established (including with site operators), how will stakeholders from the private sector be identified, and what channels will support effective public–private information-sharing? (see box 3)
- How will civil society organizations and the public-at-large be engaged in the overall protection effort?

[27] On 27 and 28 July 2015, the Counter-Terrorism Committee (CTC) held a special meeting in Madrid to discuss the follow-up to Security Council resolution 2178 (2014) on ways to stem the flow of foreign terrorist fighters. The meeting was attended by Member States, international and regional organizations, academia and civil society representatives. Participants identified 35 guiding principles (Madrid Guiding Principles) (S/2015/939, annex II). On 13 December 2018, the Committee held another special meeting, during which participants, inter alia, developed an addendum containing 17 additional guiding principles (S/2018/1177, annex).

Box 3.
Public–private partnerships (PPPs) for soft target protection – UNICRI

The Madrid Guiding Principles, in particular principles 50 and 51 (see S/2018/1177, annex), recommend that Member States, in articulating their approach to PPPs for the protection of soft targets, include the following actions:

- 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 (50 (g));
- Establish 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 (51 (c));
- Establish processes for sharing relevant information with industry and private sector partners by, for example, issuing security clearances and increasing awareness (51 (d));
- Develop cooperation mechanisms, supporting business owners and operators and infrastructure managers and by sharing plans, policies and procedures, as appropriate (51 (e)).

An overarching strategy covering soft targets across different sectors and fields of activity will thus provide the backbone for the articulation of sub-strategies and action plans for the protection of specific types of vulnerable sites. Such a strategy will have to be compatible with parallel government strategies that may have been adopted in contiguous areas such as protection of critical infrastructure, counter-terrorism, national security, and crisis management. The elaboration of a national strategy on soft targets may even constitute an opportunity to revise the entire package of connected strategies and action plans with a view to ensuring operational consistency, coordination among multiple stakeholders, streamlining procedures and optimizing resource utilization.

Case study 1. **Australia's Strategy for Protecting Crowded Places from Terrorism (ANZCTC)**

Australia's Strategy for Protecting Crowded Places from Terrorism relies on the creation of strong and trusted partnerships between all levels of government and those responsible for crowded places (i.e., owners and operators). It aims to make crowded places as resilient as possible to terrorist attacks, while preserving the use and enjoyment of those places.

The Strategy, adopted in 2017, comprises four core elements: (1) building stronger partnerships; (2) enabling better information sharing and guidance; (3) implementing effective protective security; and (4) increasing resilience.

Source: ANZCTC, 2017.

Case study 2. **Soft Targets and Crowded Places Security Plan Overview (United States Department of Homeland Security)**

The Security Plan Overview outlines the approach adopted by the United States Department of Homeland Security (DHS) to coordinate its mission to enhance the security and resilience of soft targets and crowded places (ST-CPs) across the United States.

Risk and crisis management is based on the following principles:

- A shared mission among stakeholders (including the general public, ST-CP owners and operators, security industry partners, state, local, tribal and territorial (SLTT) government partners, and the Federal government);

- DHS' role in providing security for those places for which it is responsible and supporting other stakeholders in implementing their responsibilities for ST-CP security through four lines of effort: (1) direct security operations at some facilities and locations considered ST-CPs, including transportation infrastructure, ports, waterways and Federal property; (2) awareness, intelligence, and information sharing; (3) partner capability and capacity-building; and (4) research and development.

DHS has undertaken several initiatives, including:

- Enhancing a culture of awareness through a major education and awareness campaign;
- Engaging with key international partners to share best practices and lessons learned;
- Increasing awareness of and access to DHS ST-CP resources through the development of resource guides, self-help guidance, etc.;
- Focusing and incentivizing investments in ST-CP security by leveraging grants and technical assistance to enhance ST-CP security, and incentivizing investments in the field;
- Focusing research and development on ST-CP security.

Source: United States Department of Homeland Security, 2018.

Tool 4.
Handbook to Assist the Establishment of Public–Private Partnerships to Protect Vulnerable Targets – UNICRI

(https://unicri.it/topics/public_private_security_policies)

UNICRI developed this Handbook in 2010 following a series of workshops, expert meetings, action-oriented analyses and testing events. It was designed to be used by security practitioners in public entities and private companies, and seeks to offer, in a sensible and pragmatic manner, a 10-step methodology and several tools which can be used to develop or enhance PPPs to prevent and respond to security threats at the national and/or local levels.

The Handbook complements – not replaces – existing national or regional plans and arrangements for the protection of vulnerable soft targets.

Tool 5.
Antalya Memorandum, Section B–Building Public–Private Partnerships – GCTF, 2017 (www.thegctf.org/Portals/1/Documents/Links/Meetings/2017/Twelfth GCTF Coordinating Committee Meeting/GCTF - Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context.pdf?ver=2017-09-17-010844-720)

Section B of the Memorandum focuses on building public–private partnerships to enable and improve security cooperation, and engaging industry through clear and consistent messaging on the nature of the threat and proper preparedness. The good practices outlined in that regard are:

Good practice 6: Include all stakeholders in establishing an effective national counter-terrorism framework that clarifies responsibilities for soft target preparedness—prevention, protection, mitigation, response, recovery;

Good practice 7: Enhance cooperation between and among all levels of Government, between Government and the private sector, and enhance the exchange of information and experiences between States;

Good practice 8: Establish a trusted relationship between Government and private-sector security entities, and encourage industry to play a proactive role in security efforts;

Good practice 9: Citizens and private-sector staff can contribute to security by reporting suspicious activity.

4.1.2.2 Determining what is a soft target

In its resolution 75/291, the General Assembly called upon Member States to "strengthen efforts to improve the security and protection of particularly vulnerable targets, including religious sites, educational institutions, tourist sites, urban centres, cultural and sport events, transport hubs, rallies, processions and convoys, as well as to enhance their resilience to terrorist attacks, in particular in the area of civil protection..." (para. 71). In the Addendum (S/2018/1177) to the Madrid Guiding Principles, the Security Council encouraged Member States to "determine what constitutes ... soft targets in the national context, on the basis of ongoing analysis of terrorist capabilities, intentions and past attacks..." (Guiding principle 50 (b)).

While any space can, in theory, become the object of an attack, the limited amount of resources available for security purposes imposes the need to adopt a pragmatic approach through target prioritization. The advance identification of sites exposed to the highest risk is fundamental for taking informed and intelligence-led decisions on where, how much and when to allocate resources for preventive, law enforcement and crisis management purposes. Understanding the evolving terrorist landscape, and the intent and capacities of threat actors in Member States' territories is also essential to identifying new or prioritized soft targets.

As noted in the GCTF Antalya Memorandum, "soft targets are not specific and can potentially be any place where large numbers of people congregate or gather. For this reason, the concept of protection should be dynamic, focused, and organized by geographic area instead of a more or less static concept of protection with a focus on a specific object" (Good practice 4).

In addition, while most critical infrastructure remain vulnerable on a continuous basis because operators are expected to deliver basic services uninterruptedly, sites that are typically defined as soft targets often become vulnerable only during specific periods of time (e.g., on the occasion of specific events such a concert, the opening of a street market on certain days of the week).[28] As a result, actual levels of protection need not be kept constant overtime, but rather adapted to the uses that are concretely made of the sites.[29]

Crowd density is certainly a major criterion for determining whether a place should be qualified as "soft" for the purpose of applying reinforced security measures. However, crowdedness cannot be the only criterion used to evaluate the need for and level of special protection of a particular site. Other benchmarks must be taken into account such as the particular appeal that a certain place or event has for terrorists, for example, because of its symbolic value. Another relevant factor is the outcome of the national or local threat analysis that identifies certain sites as being the object of a potential attack.

As the assessment of local circumstances and threat scenarios is key to the identification of certain areas as soft targets, local stakeholders – including site operators and local authorities – are key players for informing the prioritization effort, based on their

[28] As mentioned in section 1.2, there are different rationales for protecting soft targets and critical infrastructure, so that the criteria employed to qualify certain infrastructure as critical (e.g., the extent of damage that an attack would produce on the economy, the environment, etc.) may not be appropriate for identifying soft targets.

[29] Some sites, for example, may become vulnerable upon short notice, such as when public authorities are notified that a demonstration will take place in a certain place on a certain date.

in-depth knowledge of and direct access to information about local dynamics, crowd flows, timing of events, etc.

4.1.2.3 Setting up the institutional and operational framework for risk and crisis management

Security Council resolution 2396 (2017) stresses the need for Member States to develop, review or amend national risk and threat assessments to take into account soft targets in order to develop appropriate contingency and emergency response plans for terrorist attacks (14th preambular paragraph).

This recommendation has been further elaborated in the Addendum to the Madrid Guiding Principles, which call on Member States to develop and implement measures to protect soft targets by, inter alia, "regularly conduct(ing) risk assessments to keep pace with the evolving nature of the threat and the adversary, including by utilizing existing tools and guidance developed by international and regional organizations" (S/2018/1177, Addendum, Guiding principle 50 (b))

Guiding principle 51 recommends that, in their further efforts to protect ... soft targets from terrorist attacks, Member States, acting in cooperation with local authorities, should also consider, inter alia:

(a) Updating contingency planning, such as guidance, exercises and training for law enforcement, other relevant ministries and industry actors, in order to keep pace with actual threats, refine strategies and ensure that stakeholders adapt to evolving threats;

(b) 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 (e.g., stadiums, hotels, malls or schools);

(c) 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;

(d) Establishing processes for sharing relevant information with industry and private-sector partners by, for example, issuing security clearances and increasing awareness.

It is important for any national strategy on vulnerable soft targets to construe the risk and crisis management framework as a multi-stakeholder exercise which draws from the outcome of threat assessments conducted at the government level (both nationally and locally), and the sector level (e.g., analysis of threats impacting specific sites such as religious institutions, educational centres, tourist venues, urban centres), and is carried out at the level of individual site operators. In view of their close contact with local communities and/or their targeted expertise on security-related matters, it is critical to engage civil society organizations at an early stage as part of planning for the national strategy.

Case study 3.
Vigipirate Plan (France)

In France, the Vigipirate Plan provides the organizational and operational framework for risk and crisis management in relation to protection against terrorism. The Plan involves the State, local authorities, businesses and citizens. The terrorist attacks perpetrated in France against several soft targets in 2015 and 2016 led to a revision of the Vigipirate Plan to adapt it to a particularly high threat. The current version of the Plan is based on three pillars:

1. Development of a culture of individual and collective security throughout society;
2. Creation of three security levels depending on the assessed threat, indicated by signs in public areas, as follows:
    (a) *Vigilance:* corresponding to the permanent security posture and the implementation of 100 different measures;
    (b) *Enhanced Security – Risk of Attack:* adapts the State's response to high – very high terrorist threat. Several specific measures can be activated in addition to the permanent security measures and depending on the area at risk;
    (c) *Attack Emergency:* can be implemented immediately following an attack or if an identified and non-localized terrorist group becomes active. This level is put in place for a limited time for the purpose of crisis management operations. It enables the mobilization of exceptional resources and the diffusion of information aimed at protecting the population in a crisis situation.

(continued)

3. Implementation of new measures to strengthen government action against terrorism.

In practice, the threat analyses carried out by the competent intelligence services are used by the General Secretariat for Defense and National Security (SGDSN)[30] to establish a general Vigipirate security posture, which determines the measures to be implemented:

- at major national events (e.g., sports competitions, international summits);
- on certain key dates (e.g., start of the school year, end-of-year celebrations);
- following an attack, in France or abroad, to quickly adapt the national protection system.

The Vigipirate Plan comprises some 300 measures, including permanent measures applied to 13 major areas of activity (transport, health, etc.) and additional measures activated according to the nature and level of the assessed terrorist threat. Some of these measures are classified. The Plan is complemented in certain areas by specific intervention plans/measures (e.g., NRBC plans, Piratair-Intrusair, Pirate-mer, Piranet, Metropirate, Interception proliferation).

Source: Comprendre le plan Vigipirate, 2021 (www.gouvernement.fr/risques/comprendre-le-plan-vigipirate).

[30] Under the authority of the Prime Minister, SGDSN is an interministerial body that assists the Head of Government in designing and implementing security and defence policies.

Case study 4.
National Risk Identification Report (Swedish Civil Contingencies Agency (MSB))

Requested by the Swedish Government to outline a national risk assessment, in 2011, the Swedish Civil Contingencies Agency (MSB) produced this report based on a selection of risks identified by government authorities and county administrative boards. These risks cover a wide spectrum of incidents, including terrorism and the risk of cyberattacks.

The report also presents some typical cases that could lead to a request for international assistance. The appendices contain scenarios that were assessed through various methods.

Source: National Risk Identification Report, 2011.

4.1.2.4 Establishing a communication policy

It is important for communication strategies[31] to be implemented at all stages of risk and crisis management, with all government agencies agreeing on the facts and the approach to be followed. While informing and raising awareness among different categories of stakeholders at different phases of the security cycle and in the event of a crisis, communication plans should seek to preserve social cohesion and avoid the stigmatization of certain communities or its members.

A fundamental aspect of any communication strategy is determining the channels and modalities for engaging the public at large. In this regard, the GCTF Antalya Memorandum has identified good practices for Governments to adopt before, during and after an attack on soft targets (see Good practice 13):

> **Before an attack:** Share realistic assessments of risk to manage public expectations. The goal is to maximize the utility of warnings, and avoid allowing terrorists to drive threat perceptions. The challenge is educating the public and offering useful advice without unintentionally echoing the terrorists' message or overwhelming the public with constant information and creating threat fatigue;[32]
>
> **During an attack:** Establish how best to respond, and what information to release.

[31] The United Nations Counter-Terrorism Centre (UNCCT) of UNOCT is leading the project, "Preventing violent extremism through strategic communications", which may be of interest and assistance in this context. See www.un.org/counterterrorism/cct/strategic-communication.

[32] With regard to prevention, the GCTF Antalya Memorandum highlights steps that Governments can take, from a communication perspective, to increase the public's inclination and ability to detect threatening activity. Good practice 9 suggests that "cautionary signage, billboards, and advertisements on public transportation or in public places can enhance public awareness, and public information campaigns can work if properly focused. Use radio and TV to air public service announcements. For those countries without an existing public communication plan, regular face-to-face meetings with trade organizations or owners and operators of locations of public concern are a good starting point".

The public communications portion of a government's response plan is just as important as the operational details. Provide clear instructions to the public about areas to avoid, available shelters, and other practical information. As noted above, information should be balanced so that it does not unintentionally echo the terrorists' message;

After an attack: Get back to normal life as quickly as possible. Be prepared on social media and craft messages beforehand that you will want to convey in the aftermath of an attack. It is also critical to access communications plans in the immediate aftermath of an attack to capture lessons learned.

4.1.3 Law enforcement

The key roles and responsibilities of law enforcement agencies in soft target protection fall into three main blocks of activities:

1. *Supporting operators of vulnerable targets:* The types of support that can be offered by law enforcement agencies range from the preparation of threat/vulnerability assessments and contingency plans to assistance in organizing drills and training for site and security personnel, as well as in identifying funding opportunities to implement security upgrades. The establishment of a relationship of trust with operators of vulnerable sites will prompt the latter to adopt a proactive collaborative attitude towards security matters, and contribute to increasing law enforcement's levels of situational awareness and preparedness.

2. *Investigating terrorist attacks or preparations against vulnerable targets:* Law enforcement agencies should expand investigations into the broader networks behind an attack or its preparations. In turn, the success of these investigations hinges on the active support of relevant intelligence agencies to ascertain the likelihood of an attack and provide insight into the movement of monitored individuals. In addition, criminal justice officials must be familiar with international cooperation processes, such as mutual legal assistance, exchange of law enforcement information, extradition and the processing, preserving and exchange of evidence to be used in criminal proceedings.[33]

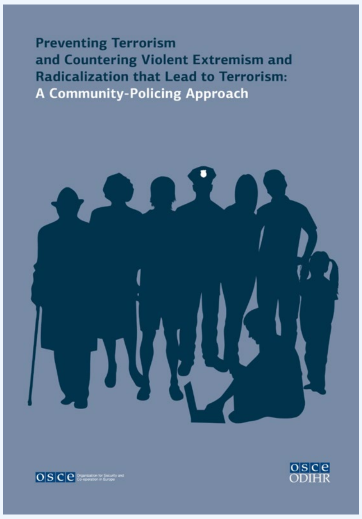
3. *Community outreach:* The GCTF Antalya Memorandum relays the experience of several stakeholders, including the effective use of police liaison officers to engage with the community, elucidate laws and help people (especially immigrants) understand their rights and duties, as a "preemptive measure aimed at detecting and resolving issues before they escalate" (see Good practice 9). Community outreach is an important aspect of community policing activities and part of the broader law enforcement strategy that emphasizes a partnership-based, collaborative effort between the police and local communities.

[33] To the extent that attacks against vulnerable targets have significant transnational dimensions – for example, because victims are nationals of several different countries – criminal justice actors from affected countries may consider applying mechanisms, such as the transfer of criminal proceedings, thereby effectively concentrating proceedings in one single jurisdiction.

Tool 6.
Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach – Organization for Security and Cooperation in Europe (OSCE), 2014

(www.osce.org/files/f/documents/1/d/111438.pdf)

This guidebook is at the intersection of three important thematic priorities for OSCE that were recently reaffirmed by participating States: (1) countering violent extremism and radicalization that lead to terrorism following a multidimensional approach; (2) promoting and protecting human rights and fundamental freedoms in the context of counter-terrorism measures are strategic focus areas for OSCE counter-terrorism activities, as outlined in the OSCE Consolidated Framework for the Fight against Terrorism (December 2012); and (3) promoting police–public partnerships/community policing, a thematic priority highlighted in the OSCE Strategic Framework for Police-Related Activities (July 2012).


Preventing Terrorism
and Countering Violent Extremism and
Radicalization that Lead to Terrorism:
A Community-Policing Approach
OSCE
OSCE ODIHR

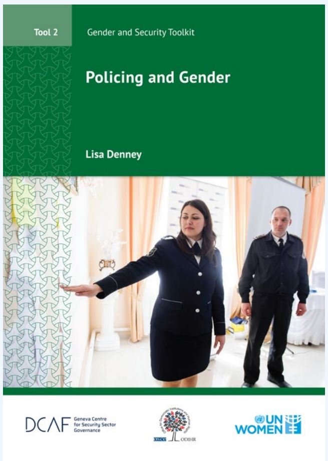
The guidebook provides policy guidance on central issues that can have an impact on the success or failure of police efforts to harness a community policing approach to preventing terrorism and countering violent extremism and radicalization. It is therefore primarily intended for policymakers and senior police professionals; however, it may also be a useful resource for members of civil society with an interest in these issues, in particular community leaders. It can serve as a common reference to promote mutual understanding and trust, and to facilitate dialogue between the police and members of the public on the threat of terrorism and the violent extremism and radicalization. It covers the following:

- Key concepts related to the prevention of terrorism and community-based approaches to countering terrorism;
- The extent to which community policing may benefit efforts to prevent terrorism encounter violent extremism and radicalization;
- Recommendations on embedding human rights and gender equality standards in community-policing;
- Practical guidance on specific implementation activities, such as coordination, tasking, trading, communication, information exchange, engagement with specific groups and evaluations.

The guidebook draws on an analysis of the accumulated experience of several OSCE participating States and partners for cooperation, and builds on previous OSCE publications.

Tool 7.
Policing and Gender – Geneva Centre for Security Sector Governance (DCAF), OSCE Office for Democratic Institutions and Human Rights (ODIHR) and UN Women, 2019
(www.osce.org/files/f/ documents/e/9/442519.pdf)

“Policing and Gender” is part of the Gender and Security Toolkit, which comprises nine tools and a series of policy briefs. “Achieving gender equality in and through policing is not simply about adding more women. It is about transforming the power relations that sustain inequality and gender-based violence (GBV). It is about protecting the human rights of all people and enabling their full contribution to public life. Integrating a gender perspective is expected of police services by virtue of international and domestic legal obligations, but it is also required to achieve more effective policing, safer societies and stronger rule of law” (see Overview, p.1).


Tool 2
Gender and Security Toolkit
Policing and Gender
Lisa Denney
DCAF Geneva Centre for Security Sector Governance
ODIHR
UN WOMEN

The toolkit sets out a range of options for integrating gender perspectives and advancing gender equality in and through policing, drawing on experience from multiple contexts. It provides guidance in the form of examples, checklists and good practices.

4.1.4 First responders

In the event of a terrorist attack, the timeliness and effectiveness of first responders’ intervention is key to mitigating the impact of the crisis and setting the recovery process on track.[34] For this to happen, it is important that all those involved in responding to soft target attacks – fire, police, emergency and health services – do the following:

1. Rely on interoperable communication systems;[35]

2. Reach out to site operators well ahead of an incident in order to familiarize themselves with site characteristics in order to deliver emergency assistance more quickly and effectively, if and when needed;

3. Engage site operators in exercises and simulations to ensure preparedness in the event that emergency procedures (e.g., site evacuations) need to be activated;

4. Consider designating a contact/focal point and ensure that site operators know who and/or which agency to contact in order to address security measures including preparedness and protection.

[34] At the same time, it is critical that first responders plan and operate their interventions in the knowledge that they may themselves become the target of terrorist violence through a secondary attack while they bring aid to victims of a terrorist incident. This calls for consistent analysis of the evolving threat of terrorist actors.

[35] The Madrid Guiding Principles encourage Member States to “promote better interoperability in security and crisis management” (Principle 50 (e)).

Box 4.
An expanded notion of interoperability

Traditionally, interoperability is understood as the technical ability of communication systems to connect/interact with each other. Recently, however, an expanded notion of interoperability is gaining traction whereby the connectivity principle should also lead to interoperable teams, synchronized procedures and information exchange practices, such as:

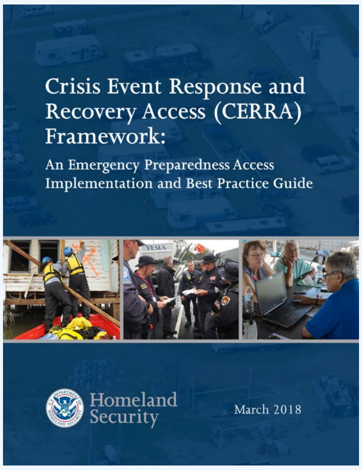
- Move beyond tech: make people and procedures interoperable; create an interoperable culture;
- Be deliberate: assign an agency or unit with the sole task of interoperability and operational integration; develop easy to deploy solutions;
- Be diligent: assure that new IT systems, training and personnel are oriented towards interoperability; assure that vendors are able to deliver on promises;
- Get ready: conduct exercises focused exclusively on integration of critical functions across agencies;
- Be your own worst critic: draft after-action reports for all exercises and incidents; make improvement plans that reflect the realities in the field; set reasonable expectations;
- Make interoperability a public safety priority: if you protect your emergency workers, they will be better prepared to protect the population they serve.

Source: Intervention by Dr. Donell Harvin, Georgetown University, delivered at the UNOCT-organized Expert Group Meeting on the Protection of Urban Centers and Tourist Venues, 15–16 June 2021 (see www.un.org/counterterrorism/events/international-expert-group-on-protection-urban-centres-touristic-venues).

Tool 8.
Crisis Event Response and Recovery Access (CERRA) Framework – United States Department of Homeland Security, 2018

(www.cisa.gov/publication/crisis-event-response-and-recovery-access)

The Framework provides guidance for competent authorities to safely, securely and effectively control and coordinate the access of key response and recovery resources to an affected area during an emergency. It features mechanisms, tools, processes and approaches for coordinating, approving and enabling access during response and recovery operations.



Crisis Event Response and Recovery Access (CERRA) Framework:

An Emergency Preparedness Access Implementation and Best Practice Guide

Homeland Security

March 2018

4.1.5 Intelligence agencies

Within their mandate of upholding national security, intelligence agencies are critical actors in the collection and analysis of information about transactions, conversations and movements of individuals and goods that may be indicative of the orchestration of terrorist acts against vulnerable targets. They also play an important role in assessing the evolving threat posed by terrorists by analysing their intent and capabilities to undertake attacks. Intelligence agencies should always exercise their mandate in accordance with the rule of law and respectful of international human rights obligations[36] and gender equality. In particular, all types of surveillance activities must be in full compliance with international obligations on the right to privacy, and subject to effective and independent oversight mechanisms. The roles and responsibilities of intelligence agencies include the following:

- Assessing, on a continuous basis, the overall nature and level of the threat, including by monitoring social platforms and processing information from non-governmental actors to detect signs of individuals' leaning towards violent behavior. The task is often a challenging one, especially in relation to individuals who become self-radicalized within short periods of time, and who do not have any formal affiliation with any terrorist organization;
- Infiltrating terrorist groups – and the social platforms used by them – with a view to learning about their structure, intent, resources and capabilities, and any ongoing plans to target vulnerable sites, among other things;[37]
- Leveraging open-source information. Information need not be sensitive or classified to be considered valuable; terrorist groups often identify targets and provide operational guidance about attack methodologies through publicly available publications;
- Working to establish or consolidate collaboration with the law enforcement community – especially at the local level and with those performing community policing tasks given their proximity and close contact with local residents, and knowledge of local contexts;
- Assembling pieces of information from different/heterogenous sources and anticipating patterns (e.g., information about theft of explosive materials connected to information about travel by certain subjects from/to certain destinations). "Weak signals" may be part of the puzzle: although they do not provide any indication of criminal behavior or intention per se, they may reveal threatening patterns once they are cross-checked with other available data;
- Considering whether to downgrade and/or redact confidential threat-related information so that it can be shared with

[36] As requested by the Human Rights Council, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, prepared a "Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight". The 35 good practices identified are the outcome of a consultation process involving Governments, experts and practitioners. See A/HRC/14/46.

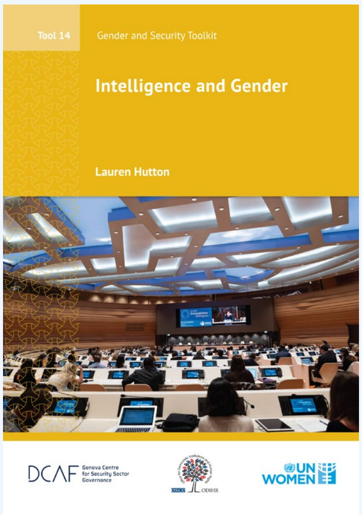
[37] Perpetrators of terrorist attacks often manifest their intention to strike in advance, on social platforms. At the same time, the more mainstream social media companies become effective in policing content published on their platforms, the more terrorist conversations tend to go to niche or custom-build social platforms, which may be harder to monitor.

other public authorities and operators of vulnerable sites for risk management purposes.[38]

- Including gender perspectives into the planning, collection, analysis and dissemination of intelligence products as a way of supporting identification of signs of instability that may have been overlooked, overcoming biases, development of a comprehensive grasp of social contexts and dynamics, and anticipation and mitigation of potential adverse consequences of intelligence collection and dissemination to the civil, political and human rights of those affected.

Tool 9.
Intelligence and Gender – DCAF, OSCE/ODIHR, UN Women, 2019

(www.osce.org/files/f/documents/f/2/447061.pdf)


Tool 14
Gender and Security Toolkit
Intelligence and Gender
Lauren Hutton
DCAF Geneva Centre for Security Sector Governance
OSCE ODIHR
UN WOMEN

“Intelligence and Gender” is part of the Gender and Security Toolkit, which comprises nine tools and a series of policy briefs. This tool, in particular, is a resource of good practices to consider when shaping policies and procedures and/or when conducting reform in the intelligence sector to advance gender equality and integrate a gender perspective.

“Given the closed and secret nature of the intelligence sector, public and security sector-wide initiatives towards integrating a gender perspective have, in general, taken a longer time to permeate the intelligence domain. Work to reform the intelligence sector seldom includes gender considerations. Efforts to address gender imbalances in intelligence services are relatively new, and dependent upon wider societal perceptions of gender roles, advances towards gender equality and the level of democratization” (p. 2).

[38] In its resolution 2396 (2017), the Security Council urged Member States to consider, where appropriate, “downgrading for official use intelligence threat and related travel data related to foreign terrorist fighters and individual terrorists, to appropriately provide such information domestically to front-line screeners, such as immigration, customs and border security agencies, and to appropriately share such information with other concerned States and relevant international organizations in compliance with international and domestic national law and policy; and to share good practices in this regard” (para. 8).

4.2 Non-government actors

Addressing the protection of vulnerable targets, the General Assembly, in resolution 75/291, called 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..." (para. 73). Member States thus recognized the importance of building multidimensional partnerships to prevent and counter the threat against vulnerable targets. This section addresses how relevant stakeholders could support government efforts in this regard.

4.2.1 Site operators

Depending on the nature of the site and applicable regulatory frameworks, operators of vulnerable targets may be private-sector entities, public authorities or mixed public–private consortiums. Although different categories of stakeholders are subject to different normative frameworks, they all have a critical role to play in ensuring that all those present on their premises – whether visitors, staff, performers or others – can benefit from a safe and secure environment.

Key blocks of responsibilities and related recommendations for site operators include the following:

- Carrying out site-specific threat and vulnerability assessments:
  - Consider how a site's specific nature, location, size, etc. exposes it to certain types of threats, as well its unique vulnerabilities;
  - Reach out to the competent local law enforcement agencies for advice in understanding current threats, and assist in designing appropriate and proportionate security plans;
  - Consider that while certain measures may be effective in mitigating some security risks, they may be useless or even counterproductive against other risks. A challenging task for site operators is to provide adequate levels of security for a multi-threat landscape;[39]
  - Test assumptions and institute a lessons-learned programme that incorporates analysis of previous attacks".[40] At the same time, an analysis that only relies on past events may be counterproductive. Arguably, "we expect groups to engage in a similar manner as they have in the past, and we harden facilities and screen people accordingly. Unfortunately, we spend an inordinate amount of resources to prevent history from repeating itself, while the groups and individuals with violent ideology work to hit United States from an unexpected or asymmetric angle".[41]

[39] For example, adding greenery to pedestrian areas may limit the speed at which a vehicle-borne attack is perpetrated, but also limit the ability of CCTV to record petty crime occurrences.

[40] Antalya Memorandum, Good practice 11: "...those lessons should be applied on the ground, and then continuing to regularly identify and share lessons learned should be part of the overall effort. The utilization of 'Red Teams' – thinking like terrorists and planning operations and tactics to expose vulnerabilities in their adversaries – can assist security officials in examining vulnerabilities or improvements in mitigation and response activities. In controlled exercises, such teams could also test security responses."

[41] Hesterman, 2019, p. 21–22.

Box 5.
Promoting gender-sensitive security planning for vulnerable targets

The development of risk mitigation policies at the institutional level should integrate gender analysis, and create, among other things, the conditions for site operators to better consider the particular security challenges and concerns of women when they plan for risk mitigation. Ensuring that gender analysis is undertaken systematically can have a significant impact on the identification of risk mitigation factors, the effectiveness of resulting strategies and their application, while minimizing disproportionate gendered impacts of risk mitigation measures.

- Taking appropriate risk mitigation measures:
  - Apply the principle of "layered security" around the site to be protected. While the mitigation measures eventually employed may vary in number, width and sophistication, the principle of "layered security" should be applied irrespective of the size and complexity of the site in question;[42]
  - Consider the full range of available security measures and select the most appropriate mix based on the outcome of security assessments, binding/recommended standards and budgetary availability. Security measures need to be commensurate with the actual threat, and implemented by well-trained and motivated personnel. They include the following:
    - "Hard" security (e.g., guards, barriers, CCTV cameras);
    - Security-by-design (i.e., integrating security concerns identified since the early stages of the sites' conceptualization);
    - Measures to address the potential threat posed by individuals who seek to be recruited (e.g., as employees, volunteers, temporary workers, etc.) or otherwise gain access to the site (e.g., as third-party contractors) so as to obtain data and/or knowledge of internal dynamics and processes that would facilitate the commission of a terrorist attack ("insider threat");
    - Cybersecurity: the increasing reliance of systems on the Internet (e.g., badge readers, cameras) means that terrorists may seek to hack those systems to gain undetected access to the site;
    - Communication tools aimed at deterring potential terrorists from attacking the site, including the use of deception tools (e.g., fake security cameras at entrance, using language on the website to give the impression that the site is highly secured).
- Preparing for emergencies:
  - Ensure that emergency plans (e.g., for evacuations) are in place and tested;
  - Involve the competent law enforcement officials, security personnel and first-responders to familiarize themselves with site features;
  - Proactively organize drill exercises, training, briefing, etc. on emergency procedures (e.g., evacuations) for people attending the site (staff, visitors, etc.) with the support of the law enforcement and first-responder community.

[42] Layered security, or "defense in depth", entails layers of security measures so that an attack that causes one measure to fail can still be avoided or mitigated by the strength of the other layers.

Box 6.
Security at vulnerable sites: an operator's perspective

- Security should facilitate business, not hinder it unnecessarily. Therefore proportionate risk-based security measures need to be designed. Consideration must also be given to how security features may affect visitors, and how the visitor may react to them;
- An appropriate screening process, reducing the chances of prohibited items entering the premises and/or performance areas, while maintaining a high level of visitor satisfaction, should be designed;
- A variety of personnel should be involved, to the extent possible, in upholding security, from guest relations teams to stewards and security staff. Search dogs may also be employed;
- Implement a comprehensive CCTV system as well as a vehicle-management system, if possible, to ensure validated persons can freely move around the site areas designated to their profile and needs;
- Work collaboratively with law enforcement, security services, authorities and industry professionals, and continually assess and enhance security operations.
- Ensure that site personnel are adequately prepared to respond to major incidents, and that they have the knowledge and training required to help themselves and others in the event of a serious incident. Educate staff about the threat of terrorism, and how they can help to prevent or deter an attack by reporting suspicious circumstances and following security protocols.

Sources: Counter Terror Business, 2020; Williams, 2021.

Tool 10.
Selected resources for operators of vulnerable targets – United States Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA)

- *Tools and resources to help businesses plan, prepare, and protect from an attack* provides expert advice and recommendations to private-sector and community partners about protective measures that can be implemented to protect facilities and venues. Businesses are encouraged to connect, plan, train and report an incident or attack, in advance, so as to better prepare organizations and employees to proactively think about the role they play in the safety and security of their businesses and communities (www.cisa.gov/publication/connect-plan-train-report).

- *Business Continuity Planning Suite* helps companies create, improve or update their business continuity plan to reduce the potential impact of disruptions. The suite includes business continuity planning training, business continuity and disaster recovery plan generators, and a business continuity plan validation (www.ready.gov/business-continuity-planning-suite).

- *Check It! – Bag Check Video* provides information to help facility/site employees properly search bags to protect venues and patrons (www.cisa.gov/video/check-it-bag-check-video).

- *Patron Screening Best Practices Guide* provides options for businesses to develop and implement patron screening procedures for major sporting events, concerts, horse races, award ceremonies, and similar gatherings (www.cisa.gov/publication/patron-screening-guide).

- *Active Shooter Emergency Action Planning* describes the fundamental concepts of developing an Emergency Action Planning (EAP) for an active shooter scenario, including important consideration of EAP development, such as:

  - A video that guides viewers through important considerations of EAP development through the first-hand perspectives of active-shooter survivors, first-responder personnel, and other subject matter experts (www.cisa.gov/active-shooter-emergency-action-plan-video);

  - A guide provides information needed to develop an Emergency Action Plan;

  - A template provides a framework for businesses to create their own Emergency Action Plan (www.cisa.gov/publication/active-shooter-emergency-action-plan-guide).

- *Active Shooter Recovery Guide* assists in the proactive implementation of policies and procedures that position organizations to effectively recover from an active-shooter incident, while providing the best support structure for their employees, contractors, visitors, patrons, family members and the community at large (www.cisa.gov/publication/active-shooter-recovery-guide).

- *Action Guide – Mass Gatherings: Security Awareness for Soft Targets and Crowded Places* identifies ways that businesses can prepare for and mitigate future attacks. It includes protective measures that provide some basic actions for consideration (www.cisa.gov/sites/default/files/publications/Mass%20Gatherings%20-%20Security%20Awareness%20for%20ST-CP.PDF).

- *What to Do – Bomb Threat Website* provides guidance and resources, including in-depth procedures for responding to bomb threats or encounters with suspicious items or behaviours, and information to help prepare and react appropriately during these incidents (www.cisa.gov/what-to-do-bomb-threat).

(continued)

- *Interagency Security Committee (ISC), Best Practices for Mail Screening and Handling Processes* provides mail centre managers, supervisors and agency security personnel with a framework for understanding and mitigating risks posed to an organization by the mail and packages it receives and delivers on a daily basis (www.cisa.gov/sites/default/files/publications/isc-mail-handling-screening-nonfouo-sept-2012-508.pdf).
- *Insider Threat Video* shows security and behaviour experts discussing how insider threats manifest in a variety of ways, including terrorism, workplace violence and breaches of cybersecurity (www.cisa.gov/insider-threat-trailer-and-video).

4.2.2 Civil society organizations

Within their various fields of activity (research, policy, community engagement), substantive focus/expertise and presence at different levels (local, national, international), civil society organizations (CSOs) can bring a wealth of perspectives and contributions to the overall effort aimed at protecting vulnerable sites. Their added value may be especially prominent in one or more of the following areas:

- Grassroots organizations operating in the proximity of vulnerable targets or implementing projects benefiting specific communities or neighbourhoods may provide critical insight into the local threat landscape. CSOs may also contribute to security plans developed by site operators or government agencies, whether locally or at the national level;
- From a perspective of up-stream prevention of terrorist attacks, CSOs conduct work and sponsor projects on de-radicalization and reducing the appeal of violent extremism (see case study 5);
- CSOs may act in various capacities as bridges between the local communities they serve and public authorities (e.g., bringing local concerns to the attention of decision-makers, ensuring that security-related messages and instructions issued by institutional actors and broadcast by the media are properly understood);
- During or in the aftermath of crises, CSOs can provide pivotal support to victims[43] and contribute to social and economic recovery efforts (see case study 6);
- CSOs are critical to the prevention and resolution of tensions within and between communities by creating safe spaces for discussing issues and concerns, channeling expressions of dissent and grievances, and facilitating the sharing of experiences and views among members of the public;
- CSOs also play a critical role in advocating that legal, policy-level and operational responses are compliant with human rights and gender equality standards.[44]

[43] Victims of human rights violations have the rights to: (a) equal and effective access to justice; (b) adequate, effective and prompt reparation for harm suffered (restitution, compensation, rehabilitation, satisfaction and guarantees of non-repetition); (c) access to relevant information concerning violations and reparation mechanisms under international law (see General Assembly resolution 60/147, annex, 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, para. 11).

[44] At the International Expert Group Meeting on Vulnerable Targets and Unmanned Aircraft Systems, held on 6-7 October 2021, a number of CSOs emphasized this point. See www.un.org/counterterrorism/events/international-expert-group-meeting-vulnerable-targets-and-unmanned-aircraft-systems. The remarks of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism were of particular importance in this context. See www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/remarks_of_the_un_sr_ct_hr_at_the_egm_vulnerable_targets_and_uas.pdf.

Case study 5.
Global Community Engagement and Resilience Fund (GCERF)

Established in 2014, GCERF is a global funding mechanism supported by 19 Governments, international organizations, foundations, corporations and individuals. Its objective is to strengthen community resilience by providing grants and support for local initiatives to address the drivers of violent extremism. Grants are disbursed to locally registered legal entities or primary recipients who coordinate a consortium of community-based organizations or to sub-recipients who run activities aimed at preventing violent extremism. An accelerated and complementary funding stream provides urgent support in response to emerging situations.

Funding is based on a number of guiding principles, including:

- *Country ownership:* activities are led by local communities and support the strategic objectives of national governments;
- *Context relevance:* funding decisions are based on thorough assessments of local factors that act as drivers of violent extremism;
- *Accountability and learning:* Methodologies and tools are continuously monitored to improve performance.

Source: GCERF (www.gcerf.org).

Case study 6.

Handling terrorism-related trauma (Trauma and Resiliency Center (NATAL), Israel)

Founded in 1998, NATAL is an apolitical organization in Israel that provides services to direct and indirect victims of trauma, including victims of terrorist acts. Its activities benefit all citizens regardless of religion, ethnic background, colour, age, gender or socioeconomic status.

The specific objectives of NATAL are to:

- Serve as a multidisciplinary treatment centre via a Clinical Unit staffed with 150 therapists located throughout the country and dealing with different facets of emotional support and psychological care;
- Reach out to the community at large by equipping it with skills to remain resilient in the face of ongoing threats, and to help in the intervention of and recovery from national emergency situations. The community outreach programme features a Mobile Unit that provides in-home treatment to people and families who – due to the severity of their trauma symptoms – feel unable to leave their homes;
- Offer veterans – through its Testimonial Center – the opportunity to document their traumatic experiences on film, under the supervision of a mental health professional;
- Raise awareness of terrorism-related trauma and de-stigmatize those seeking psychological assistance. By organizing multiple campaigns and events each year, the Trauma Advocacy and Public Relations Unit reaches out to thousands of people of all ages.

Source: NATAL (www.natal.org.il/en/).

4.2.3 Private sector (other than site operators)

"In order to maximize the potential to protect soft targets, public–private partnerships should be developed or strengthened at all levels of Government, including State, local and provincial. Member States should encourage and support such partnerships with companies that can contribute to all aspects of preparedness, namely protection from, mitigation of, response to and recovery from terrorist attacks, as well as the investigation of such incidents" (S/2018/1177, annex, para. 53).

A wide range of private sector entities are instrumental in mitigating the risk of attacks against vulnerable targets, whether they act on their own initiative, within the scope of voluntary public–private partnerships or through binding regulatory frameworks. Without claiming to be exhaustive, the following examples illustrate the diversity of the businesses potentially involved in protecting vulnerable sites:

- Private security companies (PSCS) are often called upon by operators of vulnerable targets to perform various functions broadly related to the protection of people and assets (e.g., site access control, watchmen, patrolling services, IT security, consultation on security upgrades). Whether they act in an operational or advisory capacity, PSCs can contribute to the delivery of heightened site security levels by working in tandem/coordination with law enforcement authorities, especially in countries that face significant terrorist threats and where the capacity of public security agencies is stretched. However, in order to provide genuine added value to the overall protection effort for vulnerable targets, PSC personnel need to be adequately trained. In addition, their roles and responsibilities need to be clearly covered by applicable legal frameworks and supplementary codes of conduct (see box 7). Not only does an effective regulation of private security companies guarantee basic professional standards for their employees, but also clarity in their relationship with the police, first responders and other public authorities with responsibilities for protecting vulnerable targets.

Box 7.
The International Code of Conduct for Private Security Service Providers (ICoC)

Some organizations have developed guidelines and offer certification programmes to ensure the quality and professionalism of PSC-delivered services. The Code was adopted in 2010 following a multi-stakeholder initiative launched by the Government of Switzerland.[45] While it enshrines a voluntary mechanism – and is therefore not intended as a substitute for domestic legal oversight of private security providers – the Code supports efforts to ensure PSCs exercise their duties in a human rights-compliant manner.

(continued)

[45] See https://icoca.ch/wp-content/uploads/2020/07/icoc_english3.pdf.

Its signatory companies "affirm that they have a responsibility to respect the human rights of, and fulfil humanitarian responsibilities towards, all those affected by their business activities, including personnel, clients, suppliers, shareholders, and the population of the area in which services are provided". They also recognize "the importance of respecting the various cultures encountered in their work, as well as the individuals they come into contact with as a result of those activities" (para. 4).

Today, several hundred private security providers have signed the Code. In addition, the United Nations has set membership in the Code as a mandatory requirement for the hiring of private security providers by its agencies.

In 2013, an agreement was reached on the Charter for the Oversight Mechanism of the Code. The Oversight Mechanism aims to "ensure the effective implementation of the ICoC through the certification and monitoring of private security providers, as well as through the adoption of a third-party complaint process".[46]

[46] See www.admin.ch/gov/en/start/dokumentation/medienmitteilungen.msg-id-47889.html.

- Businesses located near vulnerable sites or supplying goods/services to them can contribute to the detection and reporting of suspicious activity. They can also contribute to crisis management efforts, for example by providing shelter to people evacuated under the direction of the competent law enforcement and rescue services;
- When properly trained to recognize and report suspicious activity, drivers and other employees of transport companies are often in a privileged position to contribute to prevention efforts, due to their contact with street life and passengers on board their vehicles;
- In view of recent attacks against vulnerable sites that have been conducted with the assistance of rented vehicles, car rental agencies may stem preparatory conduct by carrying out accrued background checks on their customers.[47] Similar preventive action may be taken by other businesses dealing with dual-use items and materials, as well as vendors and retailers of unmanned aircraft systems (UAS) which may fall into the hands of hostile actors;
- In coordination with public authorities, technology companies can leverage the communication, geo-localization and algorithmic features of their online platforms to provide services to affected communities during unfolding crises or in the recovery phase (see box 7);
- Catering services can take measures to mitigate the risk of exploitation by terrorists as channels for contaminating food distributed to sites such as schools, religious sites, recreational and rehabilitation centres, etc.

Box 8.
Facebook tools that can assist in crisis response

Crisis Response on Facebook is a hub where crisis-response tools are centralized in one place:

- **Safety Check** allows users to let family and friends know that they are safe, in case of an incident affecting the area in which they are located. This feature may be activated automatically by an influx of user posts and confirmation from a third-party news or government source;[48]
- **Community Help** connects users with other people nearby the affected area to give or find help with resources such as food, supplies or shelter;
- **Raise Money** is a tool that can be used to support those affected by crises through fundraising or donating;
- **Get Information** provides links to articles, photographs and videos to help users learn more about an ongoing crisis from a variety of sources.

Source: www.facebook.com/crisisresponse/.

[47] In its Conclusions on the protection of public spaces of June 2021, the Council of the European Union encouraged Member States to "continue studying and analysing security guidance and tools for rental vehicles operators to prevent and mitigate the risk of vehicle attacks in public spaces" (annex, para. 29).

[48] Facebook's Safety Check feature was activated on the occasion of the suicide bombing attack that took place at Kabul International Airport on 26 August 2021 (see www.cnet.com/news/facebooks-safety-check-activated-after-deadly-attack-outside-kabul-airport/).

4.2.4 Users of vulnerable sites

Tourists, congregants gathered in places of worship, visitors to iconic places in urban centres, among others, are not just potential targets of terrorist attacks. They are also key actors in the overall effort to ensure that the sites they visit remain secure, and to limit the impact of crises, whenever they occur. In particular:

- Users of vulnerable sites – and the public in general – can be trained to recognize, potentially engage with, and report to authorities any unusual dynamics, including individuals who may be carrying out “pre-operational surveillance” of a site. The importance of training aimed at spotting suspicious activity cannot be overestimated, especially at a time when technological advances make it increasingly easy for would-be terrorists to go unnoticed while conducting targeted pre-attack surveillance.[49]
- During a crisis, those finding themselves on the affected site may be in a position to provide first aid before the arrival of law enforcement and medical personnel. The acquisition of general knowledge about first aid principles and the emergency treatment of injuries by people who regularly attend certain vulnerable sites may thus be critical for impact mitigation purposes.

Box 9.
The human rights impact of policies and practices aimed at detecting signs of radicalization

The Special Rapporteur on the protection of human rights and fundamental freedoms while countering terrorism was particularly concerned about approaches in which “responsibilities to detect ‘signs of radicalization’ fall upon various actors in society, including teachers, social workers, medical staff and other health-care professionals, prison staff, neighbours and family members, community leaders and members of faith-based groups.” She pointed out that “not only do those measures break the fragile trust that individuals and communities place in those professionals, whose primary duty is to protect and empower, but, without any reliable scientific understanding of the process that makes individuals turn to violent extremism, accurate identification is largely unattainable. Such policies lead to overselection and overreporting, largely on prohibited discriminatory grounds, having an impact on the rights to freedom of religion and expression and privacy”.

Source: A/HRC/43/46, para. 32.

[49] For example, UAS are increasingly equipped with silent engines and have the capability to take granular pictures from high distances. Also, ordinary consumers can buy glasses that have a built-in camera.

Tool 11.
Selected resources for users of vulnerable targets – United States Department of Homeland Security (DHS)

- **If you see something, say something** is a national campaign that raises public awareness of the indicators of terrorism and terrorism-related crime, as well as the importance of reporting suspicious activity to state and local law enforcement (www.dhs.gov/see-something-say-something/about-campaign);
- **Action Guide: Active Shooter Attacks: Security Awareness for Soft Targets and Crowded Places** lists potential warning signs, and steps to take if an incident occurs; it also contains helpful tips to assist in developing protective measures to mitigate future attacks (www.fema.gov/sites/default/files/2020-03/fema_faith-communities_active-shooter.pdf);
- **Active Shooter Preparedness website** provides access to a number of DHS products, tools and resources to help everyone prepare for and respond to an active shooter incident (www.cisa.gov/active-shooter-preparedness);
- **Action Guide: Chemical Attacks: Security Awareness for Soft Targets and Crowded Places** identifies potential scenarios and symptoms of possible chemical exposure. It also explains how individuals can respond to and mitigate future attacks (www.cisa.gov/sites/default/files/publications/Chemical Attacks - Security Awareness for ST-CP.PDF);

(continued)

- **Action Guide: Vehicle Ramming: Security Awareness for Soft Targets and Crowded Places** identifies warning signs that individuals planning a vehicle ramming attack may exhibit. It also suggests mitigation strategies and protective measures to consider (www.cisa.gov/sites/default/files/publications/Vehicle Ramming - Security Awareness for ST-CP.PDF);
- **Action Guide: Mass Gatherings: Take Charge of Your Personal Safety** provides potential indicators that may signal an attack on a mass gathering and identifies steps that individuals can take in response (www.cisa.gov/sites/default/files/publications/Mass Gatherings - Take Charge of Your Personal Safety.pdf).

References

Australia-New Zealand Counter-Terrorism Committee (ANZCTC), 2017. Australia's Strategy for Protecting Crowded Places from Terrorism (www.nationalsecurity.gov.au/crowded-places-sub-site/Files/australias-strategy-protecting-crowded-places-terrorism.pdf).

Counter Terror Business (CTB), 2020. The O2 and event security, interview (February) (https://counterterrorbusiness.com/features/ctb-interview-o2-and-event-security).

Geneva Centre for Security Sector Governance (DCAF), OSCE Office for Democratic Institutions and Human Rights (ODIHR) and UN Women, 2019. *Policing and Gender*, Tool 2, Gender and Security Toolkit.

___________, 2019. *Intelligence and Gender*, Tool 14, Gender and Security Toolkit.

Global Counterterrorism Forum, 2017. Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context (www.thegctf.org/Portals/1/Documents/Links/Meetings/2017/Twelfth GCTF Coordinating Committee Meeting/GCTF - Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context.pdf?ver=2017-09-17-010844-720).

Hesterman, Jennifer, 2019. *Soft Target Hardening: Protecting People from Attack*. Routledge.

Organization for Security and Cooperation in Europe (OSCE), 2014. Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach.

Swedish Civil Contingency Agency (MSB), 2011. A first step towards a national risk assessment: National risk identification (www.msb.se/siteassets/dokument/publikationer/english-publications/a-first-step-towards-a-national-risk-assessment---final.pdf).

United States of America, Department of Homeland Security (DHS), 2018. *Soft Targets and Crowded Places Security Plan Overview* (www.cisa.gov/sites/default/files/publications/DHS-Soft-Target-Crowded-Place-Security-Plan-Overview-052018-508_0.pdf).

United States of America, Government Accountability Office (GAO), 2012. Nuclear Nonproliferation: Additional Actions Needed to Improve Security of Radiological Sources at U.S. Medical Facilities (www.gao.gov/assets/gao-12-925.pdf).

Williams, Paul, 2021. Intervention by Head of Security at AEG Europe, at the UNOCT-organized Nations Expert Group Meeting (EGM) on the Protection of Urban Centers and Tourist Venues (15 and 16 June) (see www.un.org/counterterrorism/events/international-expert-group-on-protection-urban-centres-touristic-venues).

For more information, please visit:

www.un.org/counterterrorism/vulnerable-targets

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM