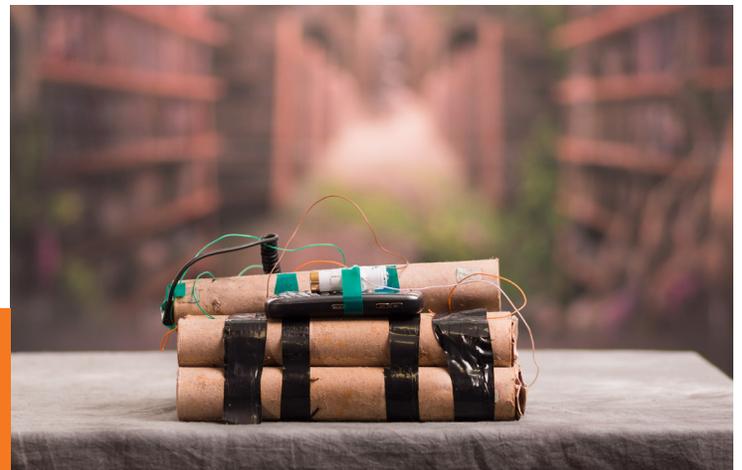


# Preventing Terrorists from Acquiring Weapons

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





# Preventing Terrorists from Acquiring Weapons

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



UNITED NATIONS  
OFFICE OF COUNTER-TERRORISM  
UN Counter-Terrorism Centre (UNCCT)



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



UNIDIR  
UNITED NATIONS INSTITUTE  
FOR DISARMAMENT RESEARCH



United Nations Global  
COUNTER-TERRORISM  
Coordination Compact

**This technical guidance document is the result of a joint project working towards Guidelines for Member States to facilitate the implementation of Security Council resolution 2370 (2017) and the relevant international standards and good practices on preventing terrorists from acquiring weapons, implemented by the United Nations Global Counter-Terrorism Coordination Compact Working Group on Border Management and Law Enforcement relating to Counter-Terrorism.**

---

**Disclaimer**

This technical guidance document is non-binding, considered a living, working reference document that will be subject to further modifications, revisions, and updates based on feedback received from Member States and the technical community of practice following the initial roll-out, application, and use.

# Table of Contents

<b>Foreword</b> .....	<b>2</b>
-----------------------	----------

<b>Introduction</b> .....	<b>4</b>
---------------------------	----------

About the joint project .....	5
-------------------------------	---

Methodological approach.....	5
------------------------------	---

Disclaimer .....	6
------------------	---

Rights of victims .....	7
-------------------------	---

<b>Executive summary</b> .....	<b>8</b>
--------------------------------	----------

## **Submodule I. Technical guidance to facilitate the implementation of Security Council resolution 2370 (2017) in preventing terrorists from acquiring improvised explosive devices and their components**

Introduction .....	10
--------------------	----

Terminology .....	11
-------------------	----

1. Functional types of an IED .....	11
-------------------------------------	----

2. Components of an IED.....	12
------------------------------	----

Objective of this submodule .....	13
-----------------------------------	----

Methodological approach.....	13
------------------------------	----

Structure of this submodule .....	14
-----------------------------------	----

Respecting human rights, fundamental freedoms, international humanitarian law, and gender- and age-related implications .....	15
---	----

### Countering terrorist acquisition and use of IEDs and components:

Upstream measures .....	16
-------------------------	----

National policy, legislation, regulation, and administrative procedures .....	16
---	----

1. National policy or strategy .....	16
--------------------------------------	----

2. National coordinating entity and coordination mechanisms.....	16
--	----

3. National legislation and regulations.....	16
--	----

4. National technical standards .....	17
---------------------------------------	----

Security and control of explosives .....	18
1. Security and control of State ammunition and explosive stockpiles .....	18
2. Security and control of explosives held by authorized civilian entities.....	19
3. Guarding or removal of unexploded ordnance, other explosive remnants of war and legacy minefields .....	19
IED risk awareness and education.....	20
Counter-IED capability development.....	21
Customs and border control.....	24
Control of IED precursors, raw materials, and components .....	25
International and regional cooperation, including information-sharing .....	27
Law enforcement intelligence led operations .....	28

**Countering terrorist acquisition and use of IEDs and components:**

<b>Downstream measures .....</b>	<b>30</b>
IED response: render safe .....	30
IED response: scene exploitation.....	31
Recovered evidence analysis .....	33
Information management .....	34
Technical exploitation of recovered IEDs .....	35
Identification of perpetrators .....	35
Criminal justice process.....	37
Development of IED countermeasures.....	38

**Submodule II. Technical guidance to facilitate the implementation of Security Council resolution 2370 (2017) in preventing terrorists from acquiring unmanned aircraft systems and components**

Introduction .....	40
Terminology .....	41
Components of UAS .....	41
Types of UAVs used in terrorist attacks.....	42
Types of terrorist use of UAS.....	43
Objective of this submodule .....	43
Methodological approach.....	44
Structure of this submodule .....	44
Respecting human rights, fundamental freedoms, and international humanitarian law, and gender and age-related implications .....	45

Countering terrorist acquisition and use of UAS: upstream measures .....	46
National policy, legislation, regulation, and administrative procedures .....	46
1. National policy or strategy .....	46
2. National coordinating entity and coordination mechanisms.....	47
3. National legislation and regulations.....	48
4. National technical standards.....	50
Capability, normative, and operational development for countering UAS.....	51
Considerations pertaining to specific areas and activities.....	53
1. Customs and border control .....	53
2. Control of UAS and key subsystems .....	55
Law enforcement intelligence led operations .....	56
International and regional cooperation, including information-sharing .....	58
Countering the terrorist acquisition and use of UAS: downstream measures.....	59
Counter-UAS, systems and techniques .....	59
UAS incident scene: safety and security .....	62
Recovery and preservation of evidence .....	63
Technical exploitation of recovered UAS and components.....	64
Information management .....	66
Identification of perpetrators .....	67
Criminal justice process.....	69
Development of UAS countermeasures .....	70

**Submodule III. Technical guidance to facilitate the implementation of Security Council resolution 2370 (2017) in preventing terrorists from acquiring small arms and light weapons, and associated ammunition**

Introduction .....	72
Terminology .....	74
Objective of this submodule .....	74
Methodological approach.....	75
Structure of this submodule .....	76
Respecting human rights, fundamental freedoms, international humanitarian law, and gender- and age-related implications .....	76

Countering terrorist acquisition of SALW and ammunition: Upstream measures .....	77
National policy, legislation, regulation, and administrative procedures .....	77
1. National policy or strategy .....	77
2. National coordinating entity and coordination mechanisms.....	79
3. National legislation and regulations.....	80
4. National administrative procedures and technical standards.....	81
Cooperation, including information-sharing .....	82
Regulation and control of manufacture.....	83
Transfer controls, including export, import, brokering, transit, or retransfer .....	83
Customs and border controls .....	87
Security and management of national stockpiles.....	89
1. Security considerations for national stockpiles .....	89
2. National accounting system .....	91
Information collection, including investigations, and analysis system .....	94
 Countering terrorist acquisition of SALW and ammunition: downstream measures.....	 95
Incident scene exploitation, including registration and documentation.....	95
Technical exploitation .....	97
Information management .....	98
Domestic tracing operations.....	99
International tracing operations .....	100
Identifying acquisition modes, involved actors, entities, individuals, and perpetrators .....	101
Criminal justice process.....	102
Development of countermeasures .....	104

## List of boxes, figures, and tables

<b>Figure 1</b>	Upstream counter-IED measures and downstream counter-IED measures .....	14
<b>Box 1</b>	Key issues for consideration on national policy, legislation, regulation, and administrative procedures .....	17
<b>Box 2</b>	Key issues for consideration on security and control of explosives.....	19
<b>Box 3</b>	Key issues for consideration on IED risk awareness and education .....	21
<b>Box 4</b>	Key issues for consideration on counter-IED capability development .....	22
<b>Box 5</b>	Key issues for consideration on customs and border control .....	24
<b>Box 6</b>	Key issues for consideration on control of IED precursors, raw materials, and components .....	26
<b>Box 7</b>	Key issues for consideration on international and regional cooperation including information-sharing.....	28
<b>Box 8</b>	Key issues for consideration on law enforcement intelligence led operations.....	29
<b>Box 9</b>	Key issues for consideration on IED response – render safe.....	31
<b>Box 10</b>	Key issues for consideration on IED response – scene exploitation.....	32
<b>Box 11</b>	Key issues for consideration on recovered evidence analysis .....	33
<b>Box 12</b>	Key issues for consideration on information management .....	34
<b>Box 13</b>	Key issues for consideration on technical exploitation of recovered IEDs.....	35
<b>Box 14</b>	Key issues for consideration on identification of perpetrators .....	36
<b>Box 15</b>	Key issues for consideration on criminal justice process .....	37
<b>Box 16</b>	Key issues for consideration on development of IED countermeasures .....	38
<b>Box 17</b>	Key issues for consideration on national policy or strategy .....	47
<b>Box 18</b>	Key issues for consideration on national coordinating entity and coordination mechanisms.....	48
<b>Box 19</b>	Key issues for consideration on national legislation and regulations.....	50
<b>Box 20</b>	Key issues for consideration on national administrative procedures and technical standards .....	51
<b>Box 21</b>	Key issues for consideration on capability, normative and operational development for countering UAS.....	53
<b>Box 22</b>	Key issues for consideration on customs and border control .....	55
<b>Box 23</b>	Key issues for consideration on control of UAS and key subsystems.....	56
<b>Box 24</b>	Key issues for consideration on law enforcement intelligence led operations .....	57
<b>Box 25</b>	Key issues for consideration on international and regional cooperation, including information-sharing .....	59
<b>Table 1</b>	C- UAS techniques .....	61
<b>Box 26</b>	Key issues for consideration on counter-UAS systems and techniques .....	63

<b>Box 27</b>	Key issues for consideration on UAS incident scene – safety and security.....	64
<b>Box 28</b>	Key issues for consideration on recovery and preservation of evidence .....	65
<b>Box 29</b>	Key issues for consideration on technical exploitation of recovered UAS and components .....	66
<b>Box 30</b>	Key issues for consideration on information management .....	67
<b>Box 31</b>	Key issues for consideration on identification of perpetrators .....	69
<b>Box 32</b>	Key issues for consideration on criminal justice process.....	70
<b>Box 33</b>	Key issues for consideration on further development of UAS countermeasures.....	71
<b>Box 34</b>	International instruments (SALW control) .....	73
<b>Box 35</b>	Key issues for consideration on national policy or strategy.....	78
<b>Box 36</b>	Key issues for consideration on national coordinating entity and coordination mechanisms.....	79
<b>Box 37</b>	Key issues for consideration on national legislation and regulations.....	80
<b>Box 38</b>	Key issues for consideration on national administrative procedures and technical standards .....	82
<b>Box 39</b>	Key issues for consideration on cooperation, including information-sharing .....	83
<b>Box 40</b>	Key issues for consideration on regulation and control of manufacture.....	84
<b>Box 41</b>	UN Security Council 1267 Sanctions regime and arms embargo .....	86
<b>Box 42</b>	Key issues for consideration on transfer controls, including export, import, brokering, transit, or retransfer .....	88
<b>Box 43</b>	Key issues for consideration on customs and border controls .....	90
<b>Box 44</b>	Categorization of items’ attractiveness to criminal and terrorist organizations.....	91
<b>Box 45</b>	Key issues for consideration on security considerations for national stockpiles .....	92
<b>Box 44</b>	Categorization of items’ attractiveness to criminal and terrorist organizations.....	93
<b>Box 47</b>	Key issues for consideration on record-keeping .....	94
<b>Box 48</b>	Key issues for consideration on information collection, including investigations, and analysis system .....	95
<b>Box 49</b>	Key issues for consideration on incident scene exploitation, including registration and documentation .....	96
<b>Box 50</b>	Key issues for consideration on technical exploitation .....	97
<b>Box 51</b>	Key issues for consideration on information management .....	98
<b>Box 52</b>	Key issues for consideration on domestic tracing operations .....	99
<b>Box 53</b>	Key issues for consideration on international tracing operations .....	100
<b>Box 54</b>	Key issues for consideration on identifying acquisition modes, involved actors, entities, individuals, and perpetrators .....	102
<b>Box 55</b>	Key issues for consideration on criminal justice process.....	103
<b>Box 56</b>	Key issues for consideration on development of countermeasures .....	104

## List of select abbreviations and acronyms

<b>ACTO</b>	(ammunition) attractive to criminal or terrorist organizations
<b>C-IED</b>	counter-improvised explosive devices
<b>CMM</b>	capability maturity model
<b>CTC</b>	Counter-Terrorism Committee
<b>CTED</b>	Counter-Terrorism Committee Executive Directorate
<b>C-UAS</b>	counter unmanned aircraft system
<b>EOD</b>	explosive ordnance disposal
<b>GCS</b>	ground control system
<b>IATG</b>	International Ammunition Technical Guidelines
<b>IED</b>	improvised explosive device
<b>IEDD</b>	improvised explosive device disposal (or defeat)
<b>IM</b>	information management
<b>INTERPOL</b>	International Criminal Police Organization
<b>MANPADS</b>	man-portable air defence systems
<b>MOSAIC</b>	Modular Small-arms-control Implementation Compendium
<b>PGS</b>	Programme Global Shield
<b>SALW</b>	small arms and light weapons
<b>SVBIED</b>	suicide vehicle-borne improvised explosive device
<b>UAS</b>	unmanned aircraft systems
<b>UAV</b>	unmanned aerial vehicle
<b>UNCCT</b>	United Nations Counter-Terrorism Centre
<b>UNIDIR</b>	United Nations Institute for Disarmament Research
<b>UNOCT</b>	United Nations Office of Counter-Terrorism
<b>WAM</b>	weapons and ammunition management
<b>WCO</b>	World Customs Organization

# Foreword



**Mr. Vladimir Voronkov**  
Under-Secretary-General  
for Counter-Terrorism



**Mr. Weixiong Chen**  
Acting Executive Director  
of the Counter-Terrorism  
Committee Executive  
Directorate



**Mr. Robin Geiss**  
Director of the United  
Nations Institute for  
Disarmament Research

The threat of terrorism is complex, multifaceted, and evolving. Many factors play a role in exacerbating the nature of this threat, yet one in particular is central to the very modus operandi of terrorism and, indeed, of critical importance to the international community's response to prevent and combat it, namely, the acquisition of weapons by terrorists. The increasing turnover and diversion of small arms and light weapons (SALW) to terrorists, the rise in prominence in the use of improvised explosive devices (IEDs) in terrorist attacks, and the emerging issue of the use of unmanned aircraft systems (UAS) by terrorists are particularly concerning trends and developments – both old and new – that merit greater attention in our collective fight against terrorism.

Globally, SALW continue to be the weapons of choice for terrorists. In 2021, the Report of the United Nations Secretary-General on *Small arms and light weapons* (S/2021/839) noted that, in the past decade, terrorists have used SALW to carry out as many as 85,148 terrorist attacks. In 2018, the Secretary-General indicated in his Report on *Countering the threat posed by improvised explosive devices* (A/73/156), that during the period 2011–2018, over 150,000 casualties were reported in connection with IEDs, over 80 per cent of which were civilians. In the subsequent report (A/75/175) of 2020, the Secretary-General highlighted that incidents involving IEDs have been recorded in the context of conflict, crime, political unrest and terrorism in all regions of the world. In addition, he emphasized that some terrorist groups have learned to deploy IEDs using off-the-shelf UAS and acquired the ability to manufacture improvised fixed-wing UAS as IEDs against military and political targets.

Weapons and supporting technology risk falling into the hands of terrorists due to poorly secured stockpiles and weak border controls. The activities of foreign terrorist fighters further increase the chances of weapons and ammunition crossing borders. Moreover, weapons – including their parts, components and ammunition – are increasingly accessible for purchase and trade on a variety of platforms, including Darknet online marketplaces. The diversion of weaponry is another significant problem in many parts of the world. Access to diverted weapons and ammunition considerably enhances the military capacity of terrorist and other armed groups. Diversion may occur as a result of uncontrolled transfer, unauthorized re-transfer, theft, hand-outs to armed groups, or barter involving natural resources.

To tackle these challenges in a comprehensive manner, the United Nations Security Council adopted resolution 2370 (2017) with concrete measures to be undertaken by Member States. This is the first Security Council resolution specifically dedicated to preventing terrorists from acquiring weapons. The concerns have also been recognized by other relevant Security Council resolutions, such as 1373 (2001), 2395 (2017), 2462 (2019), 2482 (2019) and 2617 (2021).

Moreover, in 2021, the United Nations General Assembly in the Seventh Review of United Nations Global Counter-Terrorism Strategy (A/RES/75/291) strongly condemned the continued flow of weapons, including SALW, UAS and their components, and IED components, to and among terrorists; encouraged Member States to prevent and disrupt procurement networks for such weapons between terrorists; and called on Member States to find ways of intensifying and accelerating the exchange of information regarding trafficking in arms, and to enhance coordination of efforts on national, subregional, regional and international levels.

In order to support the implementation of the above framework, in 2020, the United Nations Global Counter-Terrorism Coordination Compact Working Group on Border Management and Law Enforcement relating to Counter-Terrorism launched a project to develop and promote technical guidance for Member States to facilitate and support the implementation of Security Council resolution 2370 (2017), relevant subsequent resolutions, good practices, and international standards. The project seeks to identify challenges and opportunities within and beyond existing frameworks and/or initiatives to strengthen preventative, preparedness and response measures and approaches, as well as cooperation in this regard.

The project is implemented by the United Nations Counter-Terrorism Committee Executive Directorate (CTED), as the Chair of the Working Group, together with the United Nations Institute for Disarmament Research (UNIDIR) and the United Nations Counter-Terrorism Centre (UNCCT) of the United Nations Office of Counter-Terrorism (UNOCT), in close cooperation and collaboration with members of the Working Group. Funding for the project is provided by UNCCT/UNOCT through the generous contribution of the Kingdom of Saudi Arabia.

The technical guidelines suggest an approach, which can support Member States in eliminating the supply of SALW and associated ammunition, IEDs and their components, UAS and components to terrorists. This approach includes upstream measures and activities aimed at preventing or deterring terrorists from acquiring such weapons, as well as downstream measures and activities associated with mitigation and the response to terrorist events involving such weapon categories or systems.

It is our collective aspiration that these guidelines will provide useful insights and contribute to global, regional, and national efforts to eliminate the supply of weapons to terrorists and, in doing so, deliver us one step closer to a world free of terrorism and violent extremism.

# Introduction

In 2001, the United Nations Security Council adopted the resolution 1373, which required States to “refrain from providing any form of support, active or passive, to entities or persons involved in terrorist acts, including by ... eliminating the supply of weapons to terrorists”.<sup>1</sup> Due to the constantly evolving nature of the operational environments of terrorist groups and terrorists however, denying them access to weapons has become a complex and multifaceted challenge.

In 2017, the Security Council Counter-Terrorism Committee held an open briefing on preventing terrorists from acquiring weapons. Subsequently, in the same year, the Security Council unanimously adopted resolution 2370, which called on all States to eliminate the supply of weapons – including SALW, military equipment, UAS and their components, and IED components – to those involved in terrorist acts. Resolution 2370 became the first Security Council resolution specifically dedicated to addressing this linkage.

The Security Council resolution 2370 made a number of specific recommendations to Member States. For example, it specifically urged Member States to act cooperatively to prevent terrorists from acquiring weapons, including through information and communications technologies, while respecting human rights and fundamental freedoms and in compliance with obligations under international law. It also encouraged Member States to enhance, in particular, their judicial and law enforcement cooperation. In addition, the resolution stressed the importance of cooperation with civil society and the private sector to prevent terrorist access to weapons and requests that technical assistance, capacity-building and other support are provided to States requiring it. The resolution also recognized the existence and value of implementing processes that have framed the implementation of other relevant resolutions, such as those focusing on the illicit trafficking of SALW, as well as those combating terrorism. It also called on all Member States to “consider becoming party to relevant international and regional instruments, with a view to help eliminate the supply of weapons to terrorists, and to fully implement their respective obligations under those to which they are a party”.<sup>2</sup>

In the 2018 Addendum to the 2015 guiding principles on foreign terrorist fighters (Madrid Guiding Principles) the Security Council introduced guiding principle 52 to provide States with elements and further guidance in their undertaking appropriate measures consistent with international law to address the illicit trafficking in SALW, in particular to terrorist groups.<sup>3</sup>

1 See Security Council, S/RES/1773 (2001), p. 2, para. 2, (a), <http://unscr.com/en/resolutions/doc/1373>

2 See Security Council, S/RES/2370 (2017), p. 3, para. 1, <http://unscr.com/en/resolutions/doc/2370>

3 See Letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373

Furthermore, in its resolution 2482 (2019), the Security Council urged Member States to adopt legislative and other measures, consistent with domestic marking laws and regulation, including criminal measures, to prohibit the illegal manufacture of unmarked or inadequately marked SALW, as well as the illicit falsification, obliteration, removal or alteration of the unique markings prescribed in the International Tracing Instrument. The resolution also urged Member States to adopt and implement the necessary legislative or other measures to establish as criminal offence under their domestic law: illegal manufacture; possession; stockpiling; and trade of all types of explosives, whether military or civilian, as well as other military or civilian materials and components that can be used to manufacture IEDs.<sup>4</sup>

In its resolution 2617 (2021), the Security Council noted with concern the increasing global misuse of UAS by terrorists to conduct attacks against, and incursions into, restricted commercial and government infrastructure and public places, and acknowledged the need to balance fostering innovation and preventing misuse of UAS as its applications expand.<sup>5</sup>

In 2021, the Seventh Review of United Nations Global Counter-Terrorism Strategy (A/RES/75/291) strongly condemned the continued flow of weapons including SALW, UAS and their components, and IED components, to and between terrorists, encouraged Member States to prevent and disrupt procurement networks for such weapons between terrorists.<sup>6</sup>

## About the joint project

This document has been developed as part of the joint project working towards Guidelines for Member States to facilitate the implementation of Security Council resolution 2370 (2017) and the relevant international standards and good practices on preventing terrorists from acquiring weapons, implemented by CTED as the Chair of the United Nations Global Counter-Terrorism Coordination Compact Working Group on Border Management and Law Enforcement relating to Counter-Terrorism, UNIDIR and UNCCT/UNOCT, which also provides the funding for the initiative. UNIDIR has been acting as substantive lead entity in the development of this document.<sup>7</sup>

## Methodological approach

The methodological approach applied in the development of this technical guidance document draws on a capability maturity model (CMM). CMMs have been widely adopted by institutions, administrations, and organizations, including by the United Nations, as they provide a disciplined framework to systematically assess the maturity of processes and practices, to identify gaps and

---

(2001) concerning counter-terrorism addressed to the President of the Security Council, S/2018/1177, 28 December 2018, para. 59, pp. 27-28, <https://undocs.org/en/S/2018/1177>.

4 See Security Council, S/RES/2482 (2019), p. 5, para. 2 (11), <http://unscr.com/en/resolutions/doc/2482>

5 See Security Council, S/RES/2617 (2021), p. 3, para. 5, <http://unscr.com/en/resolutions/doc/2617>

6 See the Seventh Review of United Nations Global Counter-Terrorism Strategy, p. 5, para. 6, A/RES/75/291 (2021), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/175/70/PDF/N2117570.pdf?OpenElement>

7 Support from UNIDIR core funders provides the foundation for all the Institute's activities. UNIDIR's work in this area has been supported by the Government of Germany.

areas for improvement, and to achieve progress in complex domains. A CMM can be considered a set of structured levels, describing how Member States can reliably and sustainably produce desired outcomes to prevent terrorists from acquiring weapons, including SALW and ammunition, UAS and components, and IED components.

## Disclaimer

This document constitutes a first attempt at the international level to work towards the development of technical guidance dedicated to facilitating the implementation of Security Council resolution 2370 (2017), relevant subsequent resolutions, good practices, and international standards. The document draws on existing norms under relevant international and subregional or regional arms control instruments, as well as relevant standards or guidelines and good practices. It is acknowledged that there are considerable variations across multilateral norms, instruments and standards that apply to the three categories of weapons and systems covered in this document. While multilateral norms, instruments and standards are well defined for SALW<sup>8</sup>, efforts are ongoing in this regard with regards to IEDs.<sup>9</sup> In contrast, the domain of preventing terrorists from acquiring UAS and components, small-to medium-sized weaponized UAS, continues to evolve, and efforts to develop multilateral norms and standards applicable to these systems are at an early stage of development.<sup>10</sup>

It is also recognized and should be acknowledged that there is not a “one-size-fits-all” approach in developing technical guidance at the international level, as threats associated with terrorist acquisition of weapons are multifaceted and specific contexts will require further context-specific measures to effectively counter terrorist acquisition of weapons.

This technical guidance document is non-binding, considered a living, working reference document that will be subject to further modifications, revisions, and updates based on feedback received from Member States and the technical community of practice following the initial roll-out, application, and use. The document is designed to facilitate self-assessment by States in their efforts to develop, refine and implement technical measures at the national level to prevent terrorists from acquiring weapons. The document may also be used by relevant United Nations entities to support Member States in such efforts, including to support the Counter-Terrorism Committee (CTC) assessments and in facilitation of technical assistance to States. The document represents one of several means and methods available to support Member States and the technical community of practice in preventing terrorists from acquiring weapons, including SALW and ammunition, UAS and components, and IED components.

While recognizing the obligations set by Security Council resolution 2370 (and relevant related and subsequent resolutions) and various sources of international law in subject matter areas, this guidance document does not impose any obligations on Member States.

This document is expected to serve as a practical tool to support the implementation of resolution 2370, relevant subsequent resolutions, good practices, and international standards and guidelines. It

---

8 For further information, see submodule III of this technical guidance document.

9 For further information, see submodule I of this technical guidance document.

10 For some further information, see submodule II of this technical guidance document.

is expected to form a basis for dialogue at different levels, including among regional and national stakeholders in their efforts to assess, develop, review, and refine regional and national measures to prevent terrorists from acquiring weapons.

## Rights of victims

In general, more civilians are injured than killed in terrorist incidents, which means that thousands of civilians require long-term medical help and rehabilitation. For victims of certain types of weapons or explosives, however, such as IEDs, there is no easily framed legal redress.

International law recognizes victim assistance under four areas of jurisprudence: international human rights law, customary human rights law, international humanitarian law, and normative frameworks. In legal terms, victim assistance is known as 'reparations' whose legal purpose is to remove the effect of any wrongdoing imposed.

Reparations come in three forms: restitution (returning the victim to a state that existed prior to the incident), indemnity (compensation for financially assessable losses), and satisfaction.

Victims are those who have physical, emotional, mental, economic, or other impediments that have impinged on fundamental human rights. International law does not only recognize victims as those who are directly involved in an incident, but also indirect victims who have suffered because of a loss of employment, for instance, or dependents of those who have died or whose livelihoods have been affected by the physical or psychological injury sustained by a victim of a suicide blast. Indirect victims further include those collectively affected, such as a community or group of people, and may even encompass organizations or institutions<sup>11</sup>.

There is also the principle of non-discrimination, which is embedded within international law, and which stipulates that State parties should not discriminate against or among victims of specific types of munitions, or between survivors of a specific type of munition and other persons with disabilities. This principle further stipulates that any difference in treatment should only be based on medical, rehabilitative, psychological, or socioeconomic needs of the victims. This principle extends to acknowledge that women, children, and those with disabilities are particularly vulnerable, and therefore provided with special protection, according to the Geneva Conventions, and Additional Protocols I and II, the Convention on the Rights of the Child, as well as the Convention on the Elimination of all Forms of Discrimination Against Women.

To different extents, the network of laws that pertain to victim assistance often places the perpetrator as both responsible and liable for remedies, including for the unlawful use of weapons. This legal position is more straightforward when a State, or a person within the State apparatus, is found guilty of the unlawful use of a weapon or of explosives. The complication lies in gaining reparations from non-State actors in the unlawful use of a certain device (from which most cases of IEDs stems, for example).

---

11 These definitions are included in the United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power (1985), and in the Basic Principles and Guidelines on the Rights to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law (2005 Basic Principles, Section VIII)

# Executive summary

The aim of the technical guidelines is to contribute to the enhancement of Member States' legislative, strategic, and operational capacities to prevent, detect and counter the acquisition, illicit trafficking and use of different weapons, systems, and components.

Noting that the trafficking of illicit goods, including SALW, their ammunition, as well as IED and UAS components, is exacerbated by weak border infrastructures, as well as other border control challenges, these technical guidelines also highlight the need to enhance effective border security and management as a means for preventing the cross-border flows and movement of illicit weapons, systems, and components.

The technical guidelines employ a CMM approach, which provides a clear and logical structure. Such an approach is particularly relevant as it addresses the difficulty of achieving consistent improvements in such complex domains. Such a general approach is tailored to address the particularities of different weapon categories, systems, and components that terrorists seek to acquire and use. Such an approach includes:

**Upstream measures**, focused on those measures and activities aimed at preventing or deterring terrorists from acquiring such weapons, components, and systems; and

**Downstream measures** and activities associated with mitigation and the response to terrorist events involving such weapon categories or systems.

The general premise of this approach is that the greater the maturity and effectiveness of upstream measures, the fewer downstream measures are required. Such an approach takes into account a critical feedback loop and lessons learnt mechanism, whereby the implementation of downstream measures informs the development, refinement, and implementation of upstream measures. This document is structured and consists of three sub-modules, each focusing on a particular type of weapons category:

## **Submodule I**

Towards technical guidance to facilitate the implementation of Security Council resolution 2370 (2017) in preventing terrorists from acquiring improvised explosive device (IED) components

### **Submodule II**

Towards technical guidance to facilitate the implementation of Security Council resolution 2370 (2017) in preventing terrorists from acquiring unmanned aircraft systems (UAS) and components

### **Submodule III**

Towards technical guidance to facilitate the implementation of Security Council resolution 2370 (2017) in preventing terrorists from acquiring small arms and light weapons (SALW) and ammunition

Each sub-module follows a common structure that introduces effective upstream and downstream measures to address terrorist acquisition and use of the type of weapon under discussion. To help users in assessing the maturity of national and/or organizational processes and measures, each sub-module provides a set of key issues for consideration in the form of guiding questions. The document is designed to facilitate self-assessment by States in their efforts to develop, refine, and implement national level technical measures to prevent terrorists from acquiring weapons. The guidelines may also be utilized by relevant United Nations entities and other international and regional organizations to support States in such efforts, including to support the assessment visits conducted by CTED on behalf of the CTC, as well as in the facilitation of technical assistance to States.

These technical guidelines are non-binding and should be considered living working reference document. They are expected to serve as a practical tool to support the implementation of Security Council resolution 2370, relevant subsequent resolutions, good practices, and international standards. They are also expected to form a basis for dialogue at different levels, including among regional and national stakeholders in their efforts to assess, develop, review, and refine regional and national measures to prevent terrorist acquisition of weapons. Following roll-out, application and use, the document will be subject to modifications, revisions, and updates, based on feedback received from States and the technical communities of practice.

Work towards these technical guidelines is part of a broader joint project which examines existing regulatory frameworks and effective measures to prevent illicit production, procurement networks, supply-chain management (including end use/r controls), data collection and analysis, information exchange, and enforcement. This may include the conduct of a stakeholder mapping of relevant stakeholders and sectors; as well as seeking to identify further options and exploring and assessing concrete ways forward in supporting the effective implementation of 2370 (2017) and relevant subsequent resolutions.

The project is conducted, and the present document and these technical guidelines have been developed, in compliance with Security Council resolutions on counter-terrorism and the Global Counter-Terrorism Strategy which strongly emphasize that all measures to counter terrorism must be in compliance with the rule of law and international human rights obligations as well as gender and age sensitive approaches.

# Submodule I

## Technical guidance to facilitate the implementation of Security Council resolution 2370 (2017) in preventing terrorists from acquiring improvised explosive devices and their components

### Introduction

Improvised explosive devices (IEDs) pose a global threat and challenge. The United Nations General Assembly noted in 2020 that, “the devastation caused by the increasing use of improvised explosive devices by illegal armed groups, terrorists and other unauthorized recipients ... has affected a large number of countries and has resulted in thousands of casualties, both civilian and military”.<sup>1</sup> IEDs represent a serious problem that challenges security, safety, stability, humanitarian and peace operations, and sustainable development in communities around the world. During the period 2011–2018, over 150,000 casualties of IEDs were reported, over 80% of which were civilians. IEDs account for over 50% of all casualties from explosive violence around the world. In the same period, over 9,000 IED incidents were recorded in over 50 countries. Among the countries that have been severely affected by IEDs in the past 10 years are Afghanistan, Burkina Faso, Iraq, Libya, Mali, Nigeria, Pakistan, Somalia, the Syrian Arab Republic, and Yemen.<sup>2</sup>

An IED is not a new weapon but has become a weapon of choice for illegal armed groups and terrorist groups. How such groups acquire, manufacture, and use IEDs is constantly evolving. In Iraq and the Syrian Arab Republic, for example, there has been industrial scale IED production by terrorist groups. Victim-operated IEDs have been used extensively to deny safe access of civilians to critical infrastructure and livelihoods, which has had a detrimental impact long after a conflict has ended. The technical sophistication of IEDs is limited only by the capability and imagination of the IED maker. Those employing IEDs have proved adept at manufacturing home-made explosives and misusing electronic systems from components and substances that are dual use in nature. Non-State armed groups and terrorists have also employed IEDs in adaptative and effective ways, including using unmanned air systems (UAS). UAS have also been used to guide suicide vehicle-borne IEDs in real time in attacks against high-value or protected targets, adding to the increasing complexity of attacks.

1 General Assembly, A/RES/75/59, 2020.

2 See General Assembly, Countering the threat posed by improvised explosive devices, Report of the Secretary-General, A/73/156, 2018; see also General Assembly, Countering the threat posed by improvised explosive devices, Report of the Secretary-General, A/71/2016, 2016.

A thorough understanding of specific IED systems,<sup>3</sup> and their possible links to other systems, is a prerequisite to developing effective IED countermeasures to prevent terrorist groups and other criminals from acquiring IEDs and related components.

## Terminology (1.1)

For the purposes of this submodule, the following IED description is used and applied:

A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores but is normally devised from non-military components.<sup>4</sup>

This submodule does not include a comprehensive list of IED terms and terminology, as these are already available.<sup>5</sup> Commonly referred to IED terms based on functions and list of principal IED components are included in sections 1.1.1 and 1.1.2 below.

### 1. Functional types of an IED (1.1.1)

---

IEDs may be classified using a variety of methods, but it is usual to define them by their method of function:

**Command.** A command IED is an IED where the precise time of initiation of the device is controlled by the perpetrator. A wide variety of command initiation methods are available, including radio control, command wire, command pull, and projectile control.

**Time operated.** Time-operated IEDs are designed to function after a predetermined delay. Time delays may be achieved through mechanical, chemical, electrical, or pyrotechnic means.

**Victim operated.** A victim operated IED is an IED that is activated by the actions of an unsuspecting individual. It requires the intended target to carry out some form of action that will cause the IED to function. A wide variety of victim-operated methods are available, including pressure plate, tripwire, light initiation, movement, collapsing circuit and anti-lift.

---

3 The term "IED system" is recommended to be understood in its broadest context here. For example, terrorist groups, and associated groups, employing IEDs have their own specific characteristics and nuances. Terrorist groups such as ISIL (Da'esh), and associated groups, operating transnationally, have very different approaches to the use of IEDs than do criminals using IEDs to protect or sustain production, distribution, or illicit trade in other illicit goods.

4 United Nations Mine Action Service, *Improvised Explosive Device Lexicon*, 2016, pp. 1, 56. Refers to a type of IED incident that involves a complete functioning device.

5 Note that there is no common international definition of an IED. A lexicon has been developed that is intended to provide the United Nations system with a coherent conceptual framework and operational vocabulary to address the IED threat worldwide. See United Nations Mine Action Service, *Improvised Explosive Device Lexicon*, 2016. Note that Article 2 (5) of the Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as amended on 3 May 1996 (Protocol II to the 1980 Convention on Certain Conventional Weapons, as amended on 3 May 1996), which is understood as covering improvised devices (IED) under "other devices", defines such "other devices" as "manually-emplaced munitions and devices including improvised explosive devices designed to kill, injure or damage and which are activated manually, by remote control or automatically after a lapse of time". Devices containing chemical, biological, radiological, or nuclear materials; conventional weapons; conventional ammunition (though high explosive shells, bombs and missile warheads may be incorporated into IED main charges); and mines (anti-personnel and anti-vehicle/tank, though unfuzed anti-tank mines may be incorporated into IED main charges), are considered outside the scope of this sub-module and the technical guidelines.

**Projected.** A projected IED is an IED that is launched from some form of improvised baseplate with the intention of defeating perimeter security measures. IEDs may also be delivered using unmanned aircraft systems.<sup>6</sup>

**Suicide.** A suicide IED is an IED initiated by an attacker at a time of their choosing in which they intend to kill themselves as part of the attack. Suicide IEDs are normally person or vehicle borne. 'Suicide IEDs' are different from so-called 'proxy IEDs'.<sup>7</sup>

## 1. Components of an IED (1.1.2)

---

All IEDs, no matter how they are designed to function, have the same principal five components: initiator, main charge, firing switch, power supply and container.

**Initiator.** The initiator is the critical part of the IED; it causes the main charge to function. All IEDs require some form of initiator, and it is usually in the form of a manufactured or home-made detonator. Effective State control of these items is a prerequisite to managing IED proliferation.

**Main charge.** The main explosive charge of an IED may be based on commercial or military explosive or may be a manufactured compound or explosive mixture produced by the IED maker.

**Firing switch.** The firing switch is the part of an IED that causes the initiator to function at the desired time and place. The exact method of functioning of the IED firing switch is dependent on the function of the IED, and it is usually configured for function by time, command, or victim operation. Most firing switches are based on commonly available electronic switches, but mechanical and electrochemical switches may also be employed.

**Power supply.** The IED power supply normally takes the form of an electric battery, but mechanical- and chemical-based systems may also be employed.

**Container.** The IED container may simply be the means by which the entire IED is concealed and transported to its designated target. The container may also be designed to contribute to the functioning of the IED, such as the provision of metal fragments in anti-personnel devices or the presence of flammable material in incendiary devices.

In developing effective strategies for the denial of IED components, consideration must be given to the dual-use nature of many IED components and precursors. Regulation and control of initiators, explosives and certain firing switches is likely to yield better results than trying to eliminate access to components that are widely available, such as power sources and containers.

---

6 This is covered in greater detail in Submodule II.

7 An IED described by its method of function as a 'suicide IED' is different from what is described as a 'proxy IED'. Whereas 'suicide IED' implies that the person (i.e., the attacker) acts voluntarily, a 'proxy IED' refers to cases where a person unwittingly or by coercion acts as a means of delivery of an IED. Such 'proxy IED' are usually person or vehicle borne. This includes frequent cases in which individuals, including women, and children, are coerced and used by terrorist groups to act as a means of delivery of an IED. See United Nations Mine Action Service, *Improvised Explosive Device Lexicon*, 2016.

## Objective of this submodule (1.2)

The primary objective of this submodule is to provide technical guidance to State officials, as well as other relevant and interested stakeholders, to facilitate the implementation of resolution 2370. In particular, this submodule aims to provide technical guidance to enable effective implementation of prevention and preparedness measures that aim to prevent terrorists from acquiring IED components and from using IEDs.

The document is designed to facilitate self-assessment by States in their efforts to (i) develop, refine, and implement technical measures to prevent terrorists from acquiring IED components and (ii) prepare against IED incidents at the national level. The document may also be used by relevant United Nations and other specialized entities to support States in such efforts, including to support national assessments and in facilitation of technical assistance to States. The document represents one of several means and methods available to support States and the technical community of practice in preventing terrorists from acquiring IEDs and related components.

## Methodological approach (1.3)

The methodological approach applied in this submodule draws on a capability maturity model (CMM). CMMs have been widely adopted by institutions, administrations, and organizations, including by the United Nations in the IED domain, as they provide a disciplined framework to systematically assess the maturity of processes and practices, to identify gaps and areas for improvement, and to achieve progress in complex domains.<sup>8</sup> A CMM can be considered a set of structured levels, describing how States can reliably and sustainably produce desired outcomes to prevent terrorists from acquiring IEDs and related components. As a guiding reference, capability maturity levels may range as follows:

**Initial:** processes are characterized as ad hoc and, occasionally, even chaotic. Few processes are defined, and success depends on individual effort.

**Repeatable:** basic management processes are established, and the necessary process discipline is in place to repeat earlier successes on projects with similar applications.

**Defined:** processes are documented, standardized, and integrated into the organization's overall processes.

**Managed:** detailed measures of processes and product quality are collected, and the products and processes are quantitatively understood and controlled.

**Optimizing:** continual process improvement is enabled by quantitative feedback from the processes and from piloting innovative ideas and technologies.

---

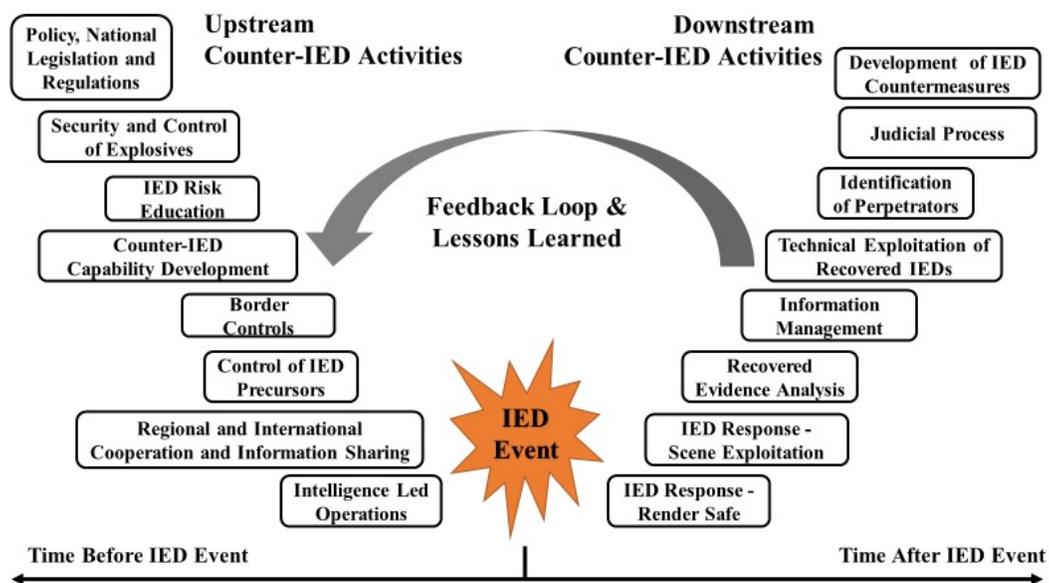
<sup>8</sup> B. Seddon and A. Malaret Baldo, Counter-IED Capability Maturity Model & Self-Assessment Tool, UNIDIR, 2020 (in particular, pp. 10–15).

These capability maturity levels, and their descriptions are guiding in nature. They may serve as a useful reference for users of this document when assessing the maturity of the national and/or organizational measures in place to prevent terrorists from acquiring IEDs and related components.<sup>9</sup>

## Structure of this submodule (1.4)

This submodule is divided into two subcategories: (i) upstream measures (section 2), focused on those activities aimed at preventing terrorists from acquiring IED components, and (ii) downstream measures (section 3), associated with mitigation and response to a particular IED event. The general premise of the CMM, which underpins this submodule, is that the greater the maturity and effective implementation by a State of upstream measures, the fewer downstream measures will be required. This is further reinforced by a critical feedback loop and lessons learned mechanism, through which downstream measures inform strengthened upstream measures. This is illustrated in Figure 1.

Figure 1. Upstream counter-IED measures and downstream counter-IED measures



IED = improvised explosive device.

<sup>9</sup> For a full and comprehensive assessment, refer to and use the Counter-IED Capability Maturity Model & Self-Assessment Tool, 2020, currently available in English, French, and Spanish: <https://unidir.org/publication/counter-ied-capability-maturity-model-and-self-assessment-tool>

Under each upstream and downstream measure covered by this submodule, a set of key issues for consideration is provided, in the form of guiding questions, to help users assess the maturity of national and/or organizational processes and measures to prevent terrorists from acquiring weapons.

## **Respecting human rights, fundamental freedoms, international humanitarian law, and gender- and age-related implications (1.5)**

Successful counter-IED approaches, measures, campaigns, and activities are based on the rule of law, the respect of human rights and fundamental freedoms, and in line with international humanitarian law, as their success is underpinned by the support of the population facing the IED threat. All upstream and downstream counter-IED measures described in this submodule are to be considered, used, and applied in full respect of existing obligations under international law, including international humanitarian and international human rights law.

Civilians are disproportionately affected by IEDs, in particular as relevant incidents are frequently carried out in populated areas, and IEDs can be employed in an indiscriminate manner or directly target civilians. Such use results in grave immediate-, short- and long-term harms on affected civilians and communities. While gender- and age-disaggregated data on victims of IEDs remains limited, women and children who fall victim to IED use may experience a range of human rights violations as a result of pre-existing gender and other inequalities and vulnerabilities. Gender- and age-related impacts and potential implications of upstream and downstream counter-IED measures described below are to be duly taken into account by users of this sub-module. Furthermore, relevant frameworks and tools must also consider the impact of related measures on groups and persons who may be marginalized or discriminated against, including members of ethnic, racial, religious, and other minorities as well as persons in vulnerable situations, such as those forcibly displaced or otherwise affected by armed conflict and other types of violence. In this respect, due account must be taken of the long-term impact of IEDs which may result, among others, in damage to private or public property, infrastructure, including electricity, water and sanitation grids, healthcare and education facilities. In armed conflict contexts, such incidents may affect objects critical to the survival of the civilian population. As such, relevant incidents may have long-term consequences on individuals and communities, including through impacting people's right to life, right to physical and mental health, housing, access to basic items such as shelter, food, or water as well as basic services.

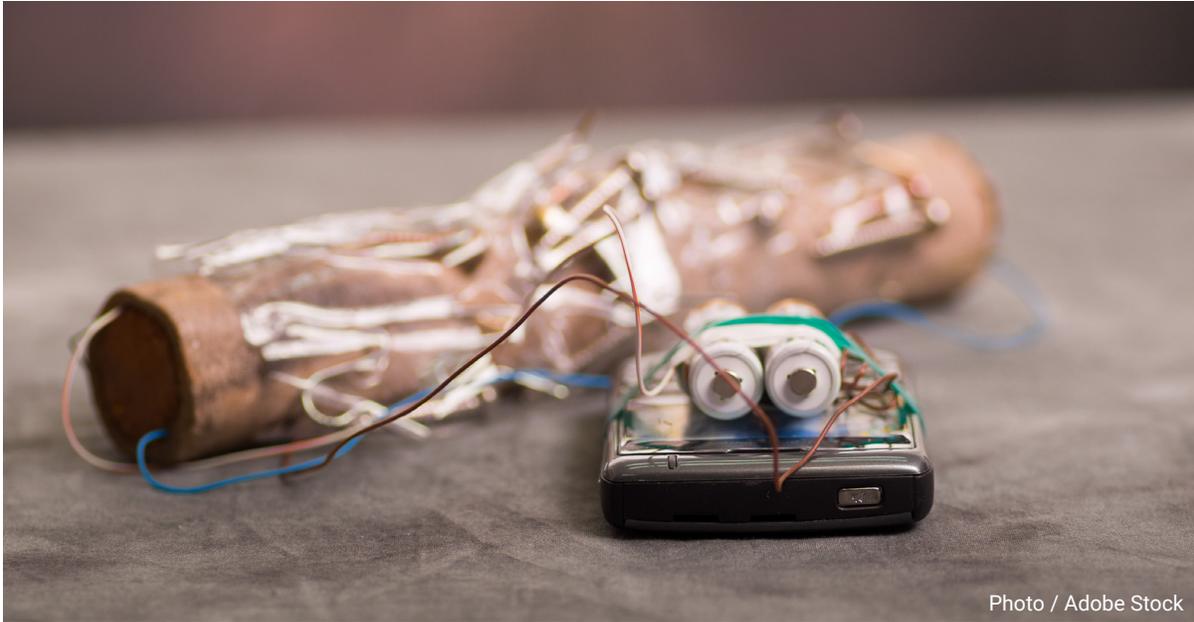


Photo / Adobe Stock

## Countering terrorist acquisition and use of IEDs and components: Upstream measures

---

### National policy, legislation, regulation, and administrative procedures (2.1)

#### 1. National policy or strategy (2.1.1)

---

The most successful national approaches to countering the threat posed by IEDs use an overarching policy that defines a whole-of-government strategy to preventing and mitigating the effects of IEDs used by terrorist groups and individuals. This is because an effective counter-IED strategy requires a coordinated, cross-government approach and is based on the conduct of regular, systematic assessments of capabilities, threats, and risks. An effective counter-IED strategy should ideally be led by a suitably resourced and empowered single government ministry or department.

#### 2. National coordinating entity and coordination mechanisms (2.1.2)

---

The conduct of an effective counter-IED campaign most often requires cooperation across several government departments, coordinated by a suitably resourced and empowered government ministry or department to avoid diffusion of responsibility (see section 2.1.1). The establishment of such a national coordinating entity, and effective inter-agency cooperation through a network of designated focal points within relevant national authorities, as well as the development of defined coordinating mechanisms, can significantly improve the coherence of cross-government counter-IED operations. The prosecution of time-sensitive intelligence-led counter-IED operations against terrorists manufacturing

and employing IEDs usually requires close cooperation between the State's intelligence entities, law enforcement, and specialist military support agencies. Robust and reliable processes must be established to allow the flow of information and intelligence between those entities that need it.

### 3. National legislation and regulations (2.1.3)

---

Effective security sector governance and compliance with applicable international law, including international human rights law and international humanitarian law, are fundamental to successful and legitimate counter-IED activities. It is essential that appropriate national legislation prohibits all activities associated with the acquisition of components and the development, manufacture, and use of IEDs. National legislation and regulations should also cover the lawful use of explosives and explosive precursors. These regulations should include:

- Lawful acquisition, control, transport, storage, and end use of explosives by civilian entities (e.g., industries associated with mining, quarrying, and exploration and extraction of oil and gas, as well as with civil engineering and demolition);
- Acquisition, storage, and use of ammunition and explosives by the armed forces and the law enforcement community; and
- Storage and transport of explosives.

The most effective regulatory regimes are those introduced with the cooperation and support of both commerce and government. In States where considerable quantities of commercial explosives are used in the extractive industries, it is important that adequate consideration is given to security and control from the point of manufacture or import to the point of end use.

#### Box 1. Key issues for consideration on national policy, legislation, regulation, and administrative procedures

- Is there a national counter-IED policy or strategy? Does it encompass an effective whole-of-government and whole of society approach to the IED problem? Is it based on a systematic assessment of the capabilities, threats and risks related to IEDs? Does it include a human rights impact assessment that is gender- and age-sensitive, including taking into consideration the needs and rights of victims?
- To what extent is there extant legislation prohibiting the acquisition of IED components and the manufacture and use of IEDs?
- Is there robust and comprehensive legislation governing the lawful acquisition, storage, transport and use of explosives and related items?
- Are the State regulations governing the control, storage and use of explosives and ammunition sufficient to prevent the illicit diversion of material?
- Does the State have a licensing system that assesses the suitability of persons to lawfully acquire and use explosives?

- To what extent does the State have regulations that cover the international movement or trans-shipment of explosives or identified IED precursors?
- Is there effective inter-agency cooperation, and are there sufficiently empowered coordination mechanisms? Are inter-agency cooperation arrangements ad hoc or formalized (e.g., through a written procedure)?
- Is there a suitably resourced entity within the State responsible for assuring compliance with legislation and regulations? If so, what is the frequency by which this entity inspects or reviews those acquiring, storing, and using explosives?

#### 4. National technical standards (2.1.4)

---

The development and adoption of national technical standards provides a means for States to standardize practices and procedures. This ensures a more effective and cohesive response to the IED threat across government departments and entities. In developing their own technical procedures and standards, States can refer to, and are encouraged to utilize, guidance contained within the United Nations Improvised Explosive Device Disposal Standards. These standards have been developed to fill a gap in the technical guidance required to respond to the expanding and increasing complexity of the IED problem.<sup>10</sup> They have been designed to assist States in mitigating the effects of IEDs and to help inform national policies and strategy. They aim to establish, inter alia, the minimum competencies required for personnel involved in the disposal of IEDs and provide guidance on planning, operational conduct, and capacity-building (e.g., training).

## Security and control of explosives (2.2)

Diversion of lawfully held explosives has been a significant source of explosives used by criminals and terrorist groups in IEDs; thus, the State should ensure that all legitimate stockpiles of manufactured explosive are denied as a source of explosives for IEDs. When regularly reviewing the effectiveness of explosive security and control measures, States need to consider every stage of the life cycle of explosives: from manufacture (or import), through and during marking or tagging,<sup>11</sup> transport, storage, and issue through to final use or final disposal.

<sup>10</sup> United Nations, United Nations Improvised Explosive Device Disposal Standards, 2018, [https://unmas.org/sites/default/files/un\\_iedd\\_standards.pdf](https://unmas.org/sites/default/files/un_iedd_standards.pdf).

<sup>11</sup> The Convention on the Marking of Plastic Explosives for the Purpose of Detection (Montreal, 1991) (colloquially also referred to as the MEX Convention) was adopted to help prevent the use of plastic explosives in terrorist attacks or by other criminals. As of April 2021, there are 156 States Parties to the Convention. Under the Convention, each State Party shall prohibit and prevent the manufacture in its territory of unmarked plastic explosives. Rather, plastic explosives shall be marked by introducing during the manufacturing process any one of the detection agents defined in the technical annex to the Convention. These agents help improve the detectability of plastic explosives using technology or explosives detection dogs. The Convention also requires each State Party to prohibit and prevent the movement into or out of its territory of unmarked explosives and to exercise strict and effective control over the possession of any existing stocks of unmarked explosives. See [https://www.icao.int/secretariat/legal/List%20of%20Parties/MEX\\_EN.pdf](https://www.icao.int/secretariat/legal/List%20of%20Parties/MEX_EN.pdf); see also <https://treaties.un.org/doc/db/Terrorism/Conv10-english.pdf>.

## 1. Security and control of State ammunition and explosive stockpiles (2.2.1)

---

The State requires a system to be in place to effectively secure and control its own stockpiles of ammunition and explosives,<sup>12</sup> which are usually held and managed by the armed forces, to eliminate all opportunities for unlawful diversion.

## 2. Security and control of explosives held by authorized civilian entities (2.2.2)

---

The illicit diversion of explosive material used in the extractive industries and for civil engineering and demolition constitutes another source of explosives that terrorists may seek to access and acquire for the manufacture of IEDs. It is therefore essential that only State-authorized entities are permitted to have access to commercial explosives and that rigorous security and control measures are in place throughout the material's life cycle (i.e., at the point of manufacture (or import), through and during marking or tagging, transport, and storage, through to the point of final use or final disposal).<sup>13</sup>

---

12 This subject falls largely under the generic heading of "physical security and stockpile management". For practical information see, for example, UNIDIR, *Utilizing the International Ammunition Technical Guidelines in Conflict-Affected and Low-Capacity Environments*, 2019; see also the UN SaferGuard Programme and the International Ammunition Technical Guidelines. States Parties to the Convention on the Marking of Plastic Explosives for the Purpose of Detection agree that stocks of unmarked plastic explosives held by their authorities performing military or police functions that are not incorporated as an integral part of duly authorized military devices are destroyed or consumed for purposes not inconsistent with the objectives of the Convention or are marked or rendered permanently ineffective, within a period of 15 years from the entry into force of the Convention in respect of that State.

13 States Parties to the Convention on the Marking of Plastic Explosives for the Purpose of Detection agree to destroy, mark, or render permanently ineffective all unmarked explosives not held by their authorities performing military or police functions within three years from the entry into force of the Convention in respect of that State.

### Box 2. Key issues for consideration on security and control of explosives

- Do the security forces have in place suitable security arrangements to safeguard ammunition and explosives attractive to criminal and terrorist organizations for use in the manufacture of IEDs?
- Are individuals with access to explosives suitably vetted?
- Are effective controls in place to prevent the diversion of explosives from civil users (for example, are there documented cases of terrorist groups, or associated groups, that deliberately target civil explosive stores with a view to obtaining explosives for use in IEDs)?
- Is there evidence from recovered IEDs that diverted civil or military explosives are being employed by terrorist groups manufacturing IEDs?
- Are civil and military explosives marked or tagged to aid detection or identification if they are subject to diversion? Is there an established timeline for when unmarked plastic explosives are going to be marked or rendered permanently ineffective or destroyed?

- Are there unguarded sources of military explosives available (e.g., uncleared mines or unexploded ordnance on military ranges or in conflict-affected or post-conflict settings)?
- Is there any evidence or intelligence to suggest that terrorist groups, or associated groups, are acquiring explosives from commercial or military sources? If so, is the trend increasing?
- Does the State employ United Nations Model Regulations, or similar, to cover the transport of explosives?
- Is there a suitably resourced entity within the State responsible for assuring compliance with legislation and regulations? If so, what is the frequency by which this entity inspects or reviews those acquiring, storing, and using explosives?

Where terrorists are known to be exploiting the availability of commercial explosives, States should consider mandating the use of explosives and initiators that are less prone to diversion and misuse. For example, certain types of non-electric detonator are much less easily adapted for use in IEDs than their older electrical equivalents. Similarly, bulk explosive mixing equipment, which mixes explosives at the site of final use, such as quarries and mines, reduces the risk of explosives being diverted along the supply chain.

### **3. Guarding or removal of unexploded ordnance, other explosive remnants of war and legacy minefields (2.2.3)**

---

The presence of unexploded ordnance and other explosive remnants of war in former conflict zones and on military ranges is another, often-neglected, source of explosives. Robust procedures must be established for the destruction of such unexploded ordnance and other explosive remnants of war, and legacy minefields should be either cleared or guarded.

## **IED risk awareness and education (2.3)**

IED risk awareness and education is important because it covers activities that reduce the risk of death and injury from IEDs through the raising of public awareness and the promotion of safe behaviour through public information campaigns, education and training, and liaison with communities. The dynamic nature of the IED threat requires that public risk awareness, education, and messaging be consistently and regularly updated as the tactics, techniques, and procedures, as well as the types of IED, employed by terrorists' change.

IED public risk awareness and education can reduce the number of civilian casualties caused by IEDs. Effective communication with affected communities is an essential prerequisite, and community involvement plays a crucial role in ensuring that public messaging is adequately targeted, assimilated, and integrated into behaviours. The three key characteristics of effective IED risk education are:

- collation and analysis of information on IEDs and other explosive threats;<sup>14</sup>
- community liaison and outreach;<sup>15</sup> and
- communication of safety messages.<sup>16</sup>

14 Collation and analysis of IED threats comes from the coordinated response and information gathered during the downstream IED response activities described in section 3 of this submodule.

15 Community liaison is concerned with identifying those key stakeholders in the target communities who are best placed to disseminate IED-threat-related information and provide critical feedback.

16 While local government officials, community elders and other senior stakeholders seem suitable conduits for IED risk education material, the importance of schools and the vital role that parents, and in particular women, play in ensuring children do not fall victim to IEDs should be considered. The key IED risk education messages must focus on the risk-taking behaviors of the target population, and the communication channel used needs to reach the maximum number of people within this target population.

### Box 3. Key issues for consideration on IED risk awareness and education

- To what extent does the State recognize that IEDs pose a threat to its general population?
- Does the State carry out injury surveillance and collect data on casualties caused by IEDs? Is such data gender- and age-disaggregated? Is the trend increasing or decreasing? Do the types of injury being encountered by health-care professionals indicate the nature and types of IEDs being employed by terrorist groups or associated groups?
- To what extent does the State carry out public information campaigns, education and training, and liaison with communities on the IED threat?
- Are IED public risk awareness messages updated as the threat posed by the use of IEDs changes?
- To what extent do other actors (e.g., humanitarian organizations or non-governmental organizations, including international ones) conduct IED risk awareness within the country or specific locations? Does the State meaningfully engage them in their own planning?
- Is there evidence that effective IED public risk awareness and education is leading to the increased reporting of detected IEDs?
- How does the State develop and conduct IED awareness training for the members of its relevant security forces and civilian services who are not counter-IED specialists?
- To what extent is the community involved in designing IED awareness public messaging?

IED public risk awareness and education messaging should be understandable, socially acceptable, context-specific, realistic, and persuasive.

IED public risk awareness and education also plays an important role in directly countering the ability of terrorists to operate covertly within a population. Appropriately targeted campaigns can highlight to the general population the types of behaviours, such as those associated with the illicit manufacture and testing of home-made explosives, that should be brought to the attention of relevant authorities. Confidential telephone lines and Internet-based applications may also encourage the anonymous reporting of suspicious activity, thus allowing States to identify terrorists planning to use IEDs at an

early stage. Often, this may be one of the few effective methods that can help identify “lone actors” plotting to use IEDs.

IED awareness and risk education is also required by the State’s security elements that are not directly involved in the clearance of IEDs or the exploitation of IED scenes. Other first responders, such as the civil police, fire and rescue service, and medical services, may also be targets of IEDs used by terrorists. These services should be provided with appropriate education and training so that they can identify, avoid, and report suspected IEDs.

## Counter-IED capability development (2.4)

The term “counter-IED capability development” covers all the measures needed by a State to acquire the full panoply of capabilities to counter the use of IEDs by terrorists. While the top-level national counter-IED strategy defines what is required to mitigate and defeat the terrorist use of IEDs, individual technical capabilities define how the terrorist use of IEDs is to be mitigated and prevented.

All individual counter-IED capabilities need to be developed within the context of the broader national strategy and fit the State’s security environment and legal framework. At its most basic and immediate level, the State must have personnel and teams capable of responding safely to the actual terrorist use of IEDs. This is usually through appropriately trained and equipped military or police IED disposal (IEDD) teams. These teams must be able to respond expeditiously to the terrorist use of IEDs and locate and render safe all types of IED. A related and equally important activity is the means to preserve IED scenes and to recover forensic evidence for further analysis and exploitation. This critical activity helps the State understand the nature of the threat it is facing. It underpins the development of IED countermeasures and, through the identification of perpetrators, supports intelligence-led counter-IED operations.

### Box 4. Key issues for consideration on counter-IED capability development

#### **Defeat the device**

- How effective is the inter-agency cooperation within the State in developing drills, tactics, techniques, procedures, and other protection measures to mitigate the use of IEDs?
- Does the State have trained and equipped teams to mitigate the effects of IEDs? If so, how suitable is their equipment and training to deal with the prevailing IED threat?
- Is there effective inter-agency cooperation between those entities responsible for responding to IED incidents (first responders), explosive ordnance disposal or IED disposal (IEDD) teams, and those responsible for the recovery and analysis of forensic evidence?
- How effective is the State procurement system in acquiring the necessary specialist IEDD equipment and protected vehicles to enable its security forces to operate in a high-threat IED environment?

- To what extent can the State develop its own equipment requirements and procure new equipment to respond to changes in the IED threat?
- How does the State disseminate IED awareness material to its population? Are there measures in place to inform the general population of new threats and how to avoid becoming the inadvertent victims of IED attacks?
- Is the State able to respond expeditiously and clear suspected IEDs reported by members of the local population in IED-affected areas?
- To what extent does the State have the support and confidence of the general population in the areas where IEDs are being employed?

#### **Engage the network**

- To what extent does the State have a clear understanding of the adversaries that are employing IEDs against it?
- Does the State maintain a positive relationship with the local population in IED-affected areas? Are members of the general population encouraged to report the presence of IEDs?
- Does the State have a strategy for identifying and exploiting the critical vulnerabilities in the organizations or individuals procuring, manufacturing, or employing IEDs?
- How does the State use the forensic and biometric intelligence gained from the exploitation of IEDs to identify those involved in the acquisition, manufacture, and deployment of IEDs?
- Does the State take measures to prevent terrorists from the exploitation of information and communications technology, including darknet markets, to counter the sharing of knowledge on the building of IEDs?
- Is the State able to mount and prosecute pre-emptive operations aimed at preventing adversaries from employing IEDs?

#### **Prepare the population, teams, and personnel**

- Does the State have an effective approach to IED risk education for its general population? For example, does the State have a means by which the effectiveness of IED public awareness-raising is measured? Does analysis of casualty data indicate that civilian casualties caused by IEDs are increasing? Does such analysis of data, civilian casualties and trends take into and include gender- and age-disaggregation?
- How effective is the State in preparing and training its personnel and organizations involved in all aspects of counter-IED? For example, does the State have facilities and suitably trained and equipped people to conduct the training of IED operators, IED searchers, and IED forensic responders? How many IED operators, IED searchers, and IED forensic responders does the State train each year?
- How does the State disseminate changes in own-force counter-IED tactics, techniques, and procedures as a result of changes in the IED threat?
- How does the State exchange, if it all, information on countering emerging IED threats with partner or neighbouring States?

Other counter-IED capabilities required by States are covered in greater detail in section 3 of this submodule. To determine the identity of those involved in the manufacture and use of IEDs, it is necessary for biometric evidence to be extracted from evidence recovered at IED scenes. The technical exploitation of IEDs requires States to develop the capabilities to analyse the chemical and blast properties of new explosive compositions. The use of complex electronics in some IEDs may require the State to develop sophisticated capabilities for the analysis of electronic switches and radio-controlled initiation systems. Technical analysis of recovered IEDs can also serve to inform the development of national countermeasure systems. Analysis of recovered IED components and post-incident analysis of terrorist attacks involving IEDs can also serve to inform IED risk education programmes as well as facilitate the exchange of information with regional and international partners. Finally, a key element of counter-IED capability development is horizon scanning and the development of timely responses to predicted future IED threats.

National counter-IED capability development is a potentially vast subject. One of the possible approaches is to consider this along the counter-IED lines of operations.<sup>17</sup>

## Customs and border control (2.5)

Effective border controls play a critical role in countering the transnational proliferation of IED components by stopping illicit flows. In countries where there is no domestic manufacturing capability for key IED dual-use items, effective border controls can significantly inhibit the ability of terrorist groups to manufacture IEDs. Open borders and free trade areas or zones need not compromise the imposition of effective common border controls, but they do require that legislation and regulations covering the security and control of explosives and IED precursors are enacted and enforced harmoniously at the regional level.

---

<sup>17</sup> NATO, Allied Joint Doctrine for Countering Improvised Explosive Devices, AJP-3.15, Edition C, Version 1, 2018.

### Box 5. Key issues for consideration on customs and border control

- Is the State's approach to border security and customs control coordinated across all relevant government departments? Is there a border security management strategy in place that includes addressing the threat, including cross-border, posed by IEDs?
- To what extent is it possible for people to enter the country, or free movement area, without passing through a recognized border control point?
- How porous are the State's borders? Does the State share a land or littoral border with a country where terrorist groups are active? Does the State share a land or littoral border with a country where groups manufacturing IEDs are active? How many cases of cross-border smuggling of illicit weapons and IED components, including dual-use items, have been detected by customs

and border forces in the past? Is the trend for smuggling of illicit materials increasing or decreasing? Are other illicit materials, such as illicit SALW or narcotics, smuggled across borders? Is there any evidence or intelligence to suggest that terrorist groups, or associated groups, exploit criminal supply chains (including in or across free trade areas or zones) for the passage of IED components?

- How effective are the customs controls and the screening of freight and parcels entering the country? For example, how much freight and what quantity is handled on a periodic basis by customs and border agencies? What percentage of shipments are subject to physical inspection, and what percentage of inspections lead to the detection of illicit material of all types? Are border security forces appropriately equipped with detection tools? Is there evidence or intelligence to suggest that terrorist groups, or associated groups, are exploiting the international freight or postal systems to acquire IED components?
- Is the border security force appropriately vetted and trained? Is there evidence to suggest that terrorist groups, or associated groups, have suborned customs or border officials to facilitate the smuggling of materials associated with the manufacture of IEDs?
- To what extent does the State participate in regional and international forums? (This is especially important when neighbouring States may already be facing a significant IED threat.)
- Does the State employ measures that permit the tracking of freight and parcels into the country, or through the country where trans-shipment from a port is taking place, to facilitate traceability? Are those measures included in the risk assessment methodology?

Internationally, the World Customs Organization (WCO) International Convention on the Simplification and Harmonization of Customs Procedures (commonly referred to as the revised Kyoto Convention, RKC), as well as the Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework), are means to standardize and facilitate legitimate trade and provide technical standards enabling States to secure their supply chains. The revised Kyoto Convention comprises several key governing principles for the transparency and predictability of effective customs controls.<sup>18</sup> The SAFE Framework provides further means for enhanced cooperation between customs and other relevant government authorities.<sup>19</sup>

In low-capacity and conflict-affected environments, the materials employed in the manufacture of IEDs tend to be imported. In these circumstances, effective border controls and proactive transnational tracking and monitoring of IED precursors may pay dividends in identifying those involved in the illicit supply and trafficking of IED components, including dual-use items and explosive precursors.

---

18 These principles include the use of risk management, coordinated interventions with other border agencies, and procedures and practices including the storage of dangerous goods.

19 In particular, the SAFE Framework calls for enhanced cooperation between customs and other governmental authorities, including aviation authorities, maritime and port security authorities, land transportation authorities, postal operators, and passenger control agencies.

## Control of IED precursors, raw materials, and components (2.6)

Effective controls on explosive precursors can significantly reduce the ease with which home-made explosive compounds and mixtures can be manufactured. Explosive precursors are chemical substances that can be used for legitimate purposes but may also be misused in the manufacture of home-made explosives. One of the issues all States face is the dual-use nature of most of the precursors used in the manufacture of IEDs. Home-made explosives fall into two broad categories: (i) explosive compounds, which are synthesized, and (ii) explosive compositions, which consist of a mechanical mixture of a fuel and an oxidizer.

Controls of IED precursors play an important part in inhibiting the ability of groups to manufacture effective IEDs. These controls assume even greater importance when the State already has effective control measures in place on military and commercial explosives, as terrorist groups using IEDs are forced to manufacture home-made explosives.

The most effective controls on IED precursors take place when the State and commerce operate in concert towards a common goal (i.e., preventing criminals and terrorists from acquiring IED precursors for illicit purposes). Consequently, depending on national legislation and responsibilities, transfer and border controls should also include verification of end use/r documentation and post-clearance audits.

Internationally, the WCO Programme Global Shield (PGS) is permanently monitoring the licit distribution and countering the illicit diversion of most relevant chemical explosive precursors and other material that could be used to manufacture IEDs. The programme provides a means to promote cooperation

### Box 6. Key issues for consideration on control of IED precursors, raw materials, and components

- What is the level of recognition by the State that certain materials may be misused in the manufacture of home-made explosives, and does the State regulate and license their acquisition?
- Does the State have a recognized list of identified IED precursors including chemical explosive precursors?
- How effective is the regulatory and licensing regime for the control of IED precursors including chemical explosive precursors that could be used in the manufacture of home-made explosives?
- Is there cooperation with and support from the commercial providers of potential IED precursors, including chemical explosive precursors, to prevent diversion?
- Is there cooperation with extractive industries that manufacture explosives on site (i.e., site mixing of ammonium nitrate or nitromethane-based compositions), and are there appropriate arrangements in place, to prevent and identify diversion? Is the use of commercial explosives by civil users in accordance with international best practices?

- Has there been evidence (from recovered IEDs) of terrorist groups, or associated groups, employing home-made explosives in the main charge of IEDs? If so, what is the composition of the explosives, and what are the likely sources of the IED precursors including chemical precursors used to manufacture the explosives?
- Does the State understand the materials used in the manufacture of IEDs? Does the exploitation of recovered IED components involve the dissemination of relevant information to entities such as the border protection forces?

among customs and police agencies in this regard.<sup>20</sup> At the practical level, PGS is raising awareness of chemical explosive precursors and IED components among customs and other border agencies. It also provides different types and formats of training for its members, including on risk assessments, profiling, detection methods, transport, labelling, handling, and storage of such goods. PGS has engaged with private sector stakeholders to establish best practice programmes to counter illicit diversion of chemical explosive precursors. Support for the PGS initiative has been further noted by the United Nations General Assembly, which recognizes the programme's important role in preventing the smuggling and illicit diversion of chemical precursors that could be used to manufacture IEDs.<sup>21</sup>

Controls on explosive precursors at the regional level vary. One regional approach, which has been adopted by the European Union, is the categorization of certain chemicals as “restricted explosive precursors”, which are not generally available to members of the public; their acquisition is subject to control and licensing. Other more commonly available materials that are prone to misuse as IED precursors are classified as “reportable explosive precursors”;<sup>22</sup> with these substances, the onus is placed on suppliers to report suspicious transactions.

## International and regional cooperation, including information-sharing (2.7)

International and regional cooperation, including information-sharing, are crucial to prevent terrorists from acquiring IED components and from using IEDs to perpetrate their attacks. Terrorists generally do not recognize international borders, and IED materials may be sourced in one country for misuse in another. Given the length and porosity of many international borders, a purely national approach to the control of IED components, including explosive precursors, is unlikely to be successful in covering the IED threat in its entirety. It is thus essential that a transnational approach is taken if these threats are to be effectively and comprehensively mitigated.

<sup>20</sup> PGS is partnering with INTERPOL, the US Defense Threat Reduction Agency, and other international organizations to strengthen information-sharing and analysis of precursor chemicals and of movements of other IED components.

<sup>21</sup> General Assembly, A/RES/72/36, 2017.

<sup>22</sup> European Union, Regulation (EU) 2019/1148, 2019.

### Box 7. Key issues for consideration on international and regional cooperation including information-sharing

- To what extent does the State recognize that the proliferation of IEDs is a transnational problem and requires coordinated international efforts?
- Is the State prepared to share information and develop capabilities in concert with regional and international partners?
- If the State is in receipt of international assistance, has it designated a national lead entity or focal point and has this information been communicated through appropriate channels to international stakeholders and partners?
- If the State is in receipt of international assistance, does it have a strategy for defining its own national priorities in terms of the acquisition of counter-IED capabilities?
- To what extent does the State centralize and collate IED reports and related information? Can it (does it) make such IED reports and related information available to regional and international partners?
- Does the State have a national IED or bomb data centre?
- Does the State have the means to securely receive, store, and process classified information relating to IED intelligence?
- To what extent has the State, in conjunction with international partners, been successful in curbing the ability of terrorist groups to operate across international borders?

Active cooperation and engagement with relevant international and subregional or regional organizations is critical to address the transnational nature of the IED threat. International cooperation in the area of enforcement, including law enforcement, is particularly important to counter threats posed by the transnational nature of IED supply chains. The WCO PGS (see section 2.6) and INTERPOL's Project Watchmaker are such initiatives.

Project Watchmaker has developed a regional-based model, in line with the current IED threats, that is derived from actual incident data. At the heart of the Project Watchmaker initiative is a database that includes information on known and suspected persons involved in the acquisition, manufacture or use of IEDs. This database allows INTERPOL to assist law enforcement agencies in detecting the transnational movement and operation of IED makers and facilitators. INTERPOL uses a series of colour-coded notices to communicate IED-related information with its members.

In addition to PGS, other relevant WCO international initiatives include the WCO's Regional Intelligence Liaison Offices, which also facilitate the exchange of intelligence across all six WCO regions. The WCO uses the Customs Enforcement Network, which was conceived to assist the customs enforcement community in gathering data and information, for intelligence purposes.

Cooperation, including the sharing of appropriate information with the private sector and industry, is also important in preventing terrorists from gaining access to IED precursors. This is particularly relevant as commercial entities may not be aware that their electronic systems or manufactured chemicals may have a dual use in the manufacture of IEDs.

## Law enforcement intelligence led operations (2.8)

Law enforcement intelligence led counter-IED operations, based on the rule of law, and carried out in compliance with international human rights law, underpin form an essential part of a state's efforts to prevent terrorist use of IEDs since the proactive use of intelligence to interdict individuals or groups before they can manufacture and deploy IEDs is one of the most effective upstream counter-IED measures. Questioning of suspects carried out in line with applicable international and domestic law may yield further information that State security forces can act on. In some circumstances involving armed conflict, the prevailing security situation may not be conducive to the use of pre-emptive arrest operations; military force, duly authorized by the State and employed in accordance with international humanitarian law, may then be necessary.

A plethora of useful information may be gained from the forensic exploitation of recovered components from IED incidents. Carefully planned and executed pre-emptive operations may disrupt IED networks and prevent those involved in the procurement of IED precursors, as well as the manufacture and supply of IEDs, from conducting successful IED-based operations. Intelligence-led operations can take many forms and may include the following:

- Identification and closure of IED and component supply chains, perhaps in cooperation with international partners;
- Identification and prosecution of those involved in the use of IEDs;
- Counter-radicalization initiatives aimed at reducing recruitment into organizations that use IEDs; and
- Measures to reduce the availability of technical knowledge relating to the construction and tactical use of IEDs.<sup>23</sup>

---

23 This, in practice, is almost impossible to achieve, but legislation prohibiting the possession of IED-related technical knowledge, such as the manufacture of home-made explosives, has proved effective in the prosecution of IED makers.

### Box 8. Key issues for consideration on law enforcement intelligence led operations

- To what extent is the State able to direct, collect, analyse, and disseminate IED-related intelligence? For example, does the State have a recognized and designated IED-related intelligence organization? What is the scope of its operations?
- Is there a national strategy that supports the use of intelligence-led operations to deny terrorist groups, and associated groups, material for manufacturing IEDs and to prevent them from using IEDs?
- How effective are the measures within the State at coordinating, analysing, and disseminating data and intelligence products from multiple domestic intelligence agencies? For example, are there written procedures for IED-related intelligence inter-agency cooperation?
- Are there successful examples of where the State has employed IED-related intelligence to interdict the sourcing of IED precursors including chemical precursors or the manufacture or deployment of IEDs by terrorist groups?

- Does the State have a domestic security organization capable of collating relevant forms of intelligence to interdict networks that use IEDs?
- Is the State able to adapt intelligence processes it has developed for countering other forms of transnational crimes to counter the use of IEDs?
- Is the State able to take the products from the analysis of recovered IED material and fuse this with other sources of intelligence, such as signals intelligence, human intelligence, and open-source intelligence?
- To what extent are there effective feedback loops between the persons recovering IED-related material and those physically conducting forensic and technical exploitation of recovered IED material?

The effective analysis and technical exploitation of IEDs and of their components is fundamental to developing future IED countermeasures and to determining whether changes in a State's own-force tactics, techniques and procedures are needed to address current developments or those predicted in the extremist use of IEDs.

Successful law enforcement intelligence-led counter-IED operations will enable the State to fuse the IED-related intelligence from its own intelligence agencies with that received from international partners. The coordination of national intelligence assets is also predicated on effective information management (IM) and requires secure means to store, process and disseminate intelligence products, usually within the context of a broader national and international security framework.

## Countering terrorist acquisition and use of IEDs and components: Downstream measures

---

### IED response: render safe (3.1)

The ability to neutralize IEDs and to deal safely with recovered explosive ordnance is a fundamental responsive capability needed by all States that face the threat of IEDs. In the early stages of an IED campaign, it is not unusual to see this role filled by military personnel who may have received training only in conventional munitions disposal. The United Nations, supported by Member States, has invested considerable effort in the development of standardized, progressive training programmes, which cover explosive hazard awareness, conventional munitions disposal, and IEDD.

IEDs vary significantly in their complexity and design, and there are no manufacturing standards for IED construction, although individual IED fabricators may have their own unique IED-making signatures. IED technology is disseminated widely via the movement of persons between countries where the use of IEDs is prevalent, as well as the spread of information over the Internet. Design is often determined by the technical ability of the IED maker.



Photo / Adobe Stock

#### Box 9. Key issues for consideration on IED response – render safe

- How mature or comprehensive are the State's policies, doctrine, and technical operating procedures for dealing with the threat posed by IEDs?
- Does the State have entities (generally, police or military units) trained and equipped to deal with IEDs? Are these entities deployed in such a manner that they can respond across the entirety of the State's territory? Is there ungoverned space where terrorist groups can manufacture and employ IEDs with impunity?
- Are other first responders provided with sufficient training and equipment to operate safely in an IED threat environment? How comprehensive is the training given to those who conduct IED render safe operations (e.g., what level of explosive ordnance disposal (EOD) and IED disposal (IEDD) training, and to what recognized international standards)? How many trained IEDD operators and IED searchers can the State call on?
- What types of equipment do EOD and IEDD teams use? Are the teams equipped with remote-controlled vehicles? Are teams equipped with electronic countermeasure systems to deal with the threat posed by radio-controlled IEDs?
- How effective is the State in analysing the IED attacks that have been conducted and modifying its capabilities accordingly?
- How effective are the State's capabilities in the search and IED detection areas? For example, does the State have personnel trained and equipped to search for IEDs in the threat environment that exists or is anticipated? Does the State collate statistics on IEDs that have been found? If so, is the trend increasing?

The immediate response to an IED is normally conducted by an explosive ordnance disposal (EOD) or an IEDD (or IED defeat) team.<sup>24</sup> The principal purposes of this team are to:

- Save lives;
- Prevent damage;
- Restore the situation to normal, or restore freedom of manoeuvre for military and security force units, as soon as possible; and
- Assist in the collection of items from IEDs that have been rendered safe in order to facilitate the technical development of IED countermeasures and to aid in the identification of IED manufacturers and facilitators.

### IED response: scene exploitation (3.2)

The preservation, collection and analysis of forensic evidence recovered from IED scenes is fundamental to the establishment of effective upstream and downstream measures for countering the proliferation of IEDs. IED scene exploitation starts at the point where an IEDD team has rendered an IED scene safe.

---

24 "IED disposal" and "IED defeat" are both commonly used terms and may be considered interchangeable.

#### Box 10. Key issues for consideration on IED response – scene exploitation

- To what extent does the State have viable forensic science capability, and is it able to preserve, collect, and analyse material recovered from IED scenes? For example, does the State possess certified and accredited forensic laboratories? If so, are they equipped and capable of conducting the analysis of IED-related material?
- To what extent does the State conduct joint training or exercises involving those entities responsible for IED render safe and scene exploitation?
- To what extent are IED disposal teams trained in the requirements of IED scene preservation and support for the recovery of IED-related material?
- How mature are the broader State capabilities for the analysis of forensic evidence? For example, is the State able to recover and record fingerprints and compare them to fingerprints stored in a national or international database?
- Is the State able to recover, analyse, and record DNA evidence and compare it to profiles in a national or international database?
- Is the continuity of evidence maintained from the point at which forensic evidence is collected to the point at which it may be required to support judicial proceedings?
- Are there examples of where the State has used information acquired from IED scenes in the successful prosecution of those using IEDs?
- Are forensic teams able to conduct effective post-blast investigations and collect evidence from scenes where IEDs have functioned?

It then covers all activities to the point when all relevant material and information from the scene has been recorded and recovered. The priority is always the preservation of life. Inappropriate risks to life should not be taken to preserve or collect forensic evidence.

Exploitation of IED scenes, including those where the IED has functioned, are undertaken and generally include the following:

- Evidence collection from IED scenes including the collection of physical evidence from parts of the IED itself or of the explosive residue, from which an assessment of the type of explosive employed by the maker can be made;
- Determination of the cause of an explosion, including identification of the type of explosive used (e.g., military, or home-made explosive), which assists in the development of counter-IED targeting strategies;
- Estimation of the type and size of explosive charge, which is important in aiding the development of technical countermeasures, including armour protection and other physical protective measures; and
- Assessment of the method of IED functioning, which yields information on how the IED was constructed and its method of functioning.

The quality of information and evidence collected from incidents and scenes is dictated by the training and level of forensic awareness of those conducting the process of IED render safe, and of those who then exploit the scene. Forensic evidence may be used not only in linking groups or individuals to

#### **Box 11. Key issues for consideration on recovered evidence analysis**

- Does the State have access to accredited forensic analysis laboratories (e.g., national capabilities, or services provided by a third party)?
- To what extent does the State possess technical abilities to conduct the following: chemical analysis of explosive compositions and soil samples from the site of IED explosions; analysis of visible forensic evidence (comparison and identification of IED components, fragments of IED containers, paints, body fluids); analysis of invisible forensic evidence (fingerprints, DNA, fibres, explosive vapour residues, microscopic fragments, and tool marks and abrasions); technical evaluation of electronic IED components?
- Does the State have a recognized training and qualification programme to ensure the competence of all personnel engaged in the analysis of forensic evidence?
- Are there examples of forensic evidence having been used to successfully prosecute the use of IEDs or other explosives-related offences?
- How effective is the feedback loop between those rendering safe and recovering IED components and those analysing material in accredited laboratories? For example, how does the exchange of information between those involved in the analysis of IED-related forensic evidence, those engaged in the rendering safe of IEDs, and those involved in the investigation of IED incidents take place? Are there defined protocols that govern the passage of information? Do regular,

formal meetings take place between those engaged in the analysis of forensic evidence and those at the forefront of counter-IED operations?

- Does the State use microanalytical techniques for processing “big data” associated with IED incidents? Is geospatial analysis or geographic risk mapping of incidents undertaken?

IEDs and assisting in counter-IED targeting (as part of a broader national approach to counter-IED) but also – if correctly collected, presented, and submitted – in criminal proceedings in a court of law (see section 3.7).<sup>25</sup>

### Recovered evidence analysis (3.3)

Thorough forensic analysis of recovered IED material is fundamental to determining how the IED was designed to function and, subsequently, who might be behind the attack. Manufactured explosive components, such as main charges and detonators, may be identified through the manufacturer’s markings. For electronic components, particularly on integrated circuits and microprocessors, identification and batch markings may indicate where and when the item was manufactured. The correct identification of IED components represents the first stage for subsequent investigations and the identification of the IED supply chain.

Analysis of material recovered from IED scenes informs a number of critical upstream counter-IED measures, such as identifying the potential sources of IED components and precursors; informing IED public awareness and risk education; and serving as a critical information source for developing proactive intelligence-led counter-IED operations.

The analysis of recovered IED components may pose technical challenges as special chemical analysis techniques may be required to determine the composition of explosive mixtures and chemical precursors. The electronic components of IEDs, particularly radio-controlled initiation systems used in radio-controlled IEDs, also require specific equipment, knowledge, and techniques so that the method and frequency of the operation of the IED can be determined.

### Information management (3.4)

A robust and effective approach to information management (IM) underpins most successful whole-of-government approaches taken to counter the terrorist use of IEDs. IM should be understood as the process of collecting, organizing, storing, and providing information within an organization.

---

<sup>25</sup> See also, UN CTED, Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved, and shared by the military to prosecute terrorist offences, 2019. Criminal-justice actors need “information” and “evidence” to understand who was responsible for a crime, and when and how the crime occurred. Here, “information” can entail, among other things, physical objects, statements from witnesses and suspects, electronic and forensic information, and intelligence. Information used in legal proceedings is called evidence. The term “evidence” is used here to describe information that complies with the legal rules of evidence and is used in judicial proceedings to prove or disprove an alleged crime.

Modern computer-based information systems and networked communications can improve the efficiency of information dissemination across geographically dispersed entities, but they are not a panacea. Information overload can be a problem, and it is essential that where automated data and intelligence collection systems are employed, police investigators and intelligence analysts are provided with automated collation and analysis tools to handle the ensuing large volumes of information.

Manual systems, while slower and less flexible, can be equally effective if they are structured and used appropriately. Effective IM processes are also a key prerequisite for the sharing and exchanging IED-related information and intelligence with relevant regional and international stakeholders and partners.

#### Box 12. Key issues for consideration on information management

- Does the State have a standardized format for the submission of IED incident reports? Do IED incident reports provide a permanent record of the technical make-up of the device, and do they record any casualties or damage caused by the IED? Are IED incident reports collated at a national IED or bomb data centre? Are these reports made available to regional and international partners?
- Are IED incident reports used as evidence in criminal justice proceedings?
- Does the State have a common format for the submission of forensic analysis reports?
- Is there a standardized method for the submission of physical exhibits collected from IED incidents?
- Are forensic exhibits (e.g., fingerprints and DNA) and police interview reports collected from those arrested and subsequently prosecuted for IED-related offences?
- Does the State make effective use of all-source intelligence reports pertaining to IED incidents or people suspected of involvement in IED-related offences? Do the State employ information systems to help in the storage, processing, and analysis of all-source intelligence? Do the State's information management processes permit the rapid and effective flow of IED-related information to those entities that need it?

### Technical exploitation of recovered IEDs (3.5)

The technical exploitation and characterization of recovered IEDs is intended to decipher the intentions of those building and deploying the IED. It aims to address the “so what” questions generated as a result of the formal forensic analysis of material recovered from IED incidents. It is primarily concerned with determining why an IED incident has happened and understanding the perpetrators' objectives in manufacturing and deploying an IED of that type.

- A thorough technical exploitation of the IED may achieve the following:
- Identify the source(s) of supply of specific IED components;

### Box 13. Key issues for consideration on technical exploitation of recovered IEDs

- Does the State have facilities for assessing the technical capabilities of IEDs? For example, are there ranges and instrumentation for evaluating the blast characteristics of new explosive compositions? Are there electronic analysis facilities to determine the method of operation of electronic items?
  - To what extent are there robust arrangements for the two-way transfer of knowledge between those involved in the rendering safe of IEDs and those conducting the technical analysis and exploitation of IEDs? Does this also take place regionally and/or internationally?
  - To what extent is the State able to call on support from scientists and engineers with appropriate expertise to understand the technical aspects of the IED threats being faced? Is there a single State entity responsible for the provision of this expertise? Does the State place legal obligations on non-State entities, such as academic institutions or commercial companies, to provide technical support when required?
- 
- Link incidents through the technical evaluation of specific IED maker signatures and other characteristics;
  - Inform the development of countermeasures; and
  - Inform the future training of IEDD teams and other members of the security forces.

Eventually, effective technical exploitation of IEDs enables the State to (i) establish a clear picture of the technical capabilities of those manufacturing and deploying IEDs and (ii) clearly discern and identify their method of operation. This clear picture can also help contribute to the prediction of future intentions.

## Identification of perpetrators (3.6)

The identification of those involved in the terrorist use of IEDs is a fundamental tenet of effective counter-IED operations and related accountability processes. The lawful questioning, in line with applicable international and domestic law, of those suspected of involvement in the illegal supply, manufacture, and use of IEDs may yield further information to support future counter-IED operations.

Individuals may be identified through a variety of intelligence techniques, such as human intelligence and signals intelligence, but it is the use of forensic and biometric intelligence that provides the most definitive method of identifying perpetrators and linking individuals to specific IED incidents. Fundamentally, forensic, and biometric intelligence is focused on the application of sound police investigative principles that are based on a valid forensic exploitation of recovered IED components. In many respects, once the initial explosive hazard has been dealt with, IED scenes are no different than other serious crime scenes.

#### Box 14. Key issues for consideration on identification of perpetrators

- To what extent does the State possess the fundamental core capabilities of forensic recovery, analysis, and technical exploitation of IEDs?
- Does the State follow good international practice for forensic recovery, analysis, and technical exploitation of IEDs?
- Does the State exchange information on techniques with international partners?
- Does the State effectively integrate the various sources of information and intelligence open to it to identify perpetrators?
- Are there successful examples of the State identifying perpetrators? If so, what were the critical success factors?
- Does the State use a technical profiling method (i.e., non-biometric) for the identification of IED maker signatures that are unique to a particular IED maker (or group of IED makers trained by a specific individual)?
- Does the State use geospatial or big data analysis techniques to develop intelligence to assist in the identification of those involved in the manufacture and employment of IEDs?

The perpetrators of IED crimes may be most easily identified from biometric evidence (principally, fingerprints and DNA) recovered from IED components, which is then matched to data stored in national and international databases.<sup>26</sup> Perpetrators may also be identified through the analysis of transactions, which may highlight links to the acquisition of specific batches of IED components. Other visible and invisible forensic evidence collected at IED scenes, such as fibres, tool marks and abrasions, and explosive residues, may also be used to link specific individuals to IED incidents.

A related but equally important use of recovered evidence is the fact that it may also be used to support the testimony of witnesses; this is particularly important in some judicial systems. Open-source intelligence derived from sources such as social media accounts and published propaganda materials may also yield considerable information to assist in the identification of perpetrators.

### Criminal justice process (3.7)

All IED incidents are crime scenes, and it is essential that forensic evidence is collected and managed in due cognizance of the law to bring perpetrators to justice. It is preferable that forensic evidence at IED scenes is collected by authorized and trained police forensic personnel. However, in many situations – especially in low-capacity and conflict-affected environments – this may not be possible and other personnel may have to collect evidence on behalf of the judicial authorities. In all circumstances, the

---

26 See United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, CTED and UNOCT, in association with the Biometrics Institute, 2018.

#### Box 15. Key issues for consideration on criminal justice process

- Is there a track record of successful prosecutions of persons involved in the illegal acquisition of IED precursors or the manufacture and use of IEDs?
- To what extent does the State criminal justice system permit the use of forensic evidence to support IED-related cases?
- Is there extant legislation prohibiting the acquisition of IED components and the manufacture and use of IEDs? Is the legislation fit for purpose?
- Are appropriate security measures in place to protect those involved in the administration and delivery of justice?

integrity of the forensic chain of custody is to be maintained in order that material recovered may be used to support the prosecution of perpetrators.

Most States require no special legislative or regulatory measures to deal with IEDs, as the application of the same procedures used for other serious crimes are normally sufficient.<sup>27</sup> It is, however, usually necessary for specialist techniques and procedures to be developed for the preservation, collection, and analysis of IED-related material.

---

<sup>27</sup> In the context of IED incidents during international civilian aviation, the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (also known as the Beijing Convention 2010) provides for key new offences, among them the illicit transport by air of explosives... material for unlawful purposes. The Convention also provides for expanded jurisdiction and for strengthened extradition and mutual assistance regimes. This legal instrument aims to ensure that a wider range of perpetrators can be brought to justice in aviation-related terrorist or proliferation activities than was formerly possible. The Beijing Convention, which entered into force on 1 July 2018, had 67 States Parties as of 1 April 2021. [https://www.icao.int/secretariat/legal/Docs/beijing\\_convention\\_multi.pdf](https://www.icao.int/secretariat/legal/Docs/beijing_convention_multi.pdf); [https://www.icao.int/secretariat/legal/List%20of%20Parties/Beijing\\_Conv\\_EN.pdf](https://www.icao.int/secretariat/legal/List%20of%20Parties/Beijing_Conv_EN.pdf)

#### Box 16. Key issues for consideration on development of IED countermeasures

- To what extent does the State monitor the use of IEDs by terrorist groups (and associated groups) and non-State armed groups? To what extent can the State respond expeditiously and effectively to changes in respective tactics, techniques, and procedures?
- How does the State develop IED countermeasures? For example, are there entities nominated and responsible for the development of counter-IED training (e.g., technical training for specialists or IED awareness training for non-specialists)? Is there an entity nominated for the specification of requirements and acquisition of equipment? Is there an entity nominated and responsible for the design of critical infrastructure to resist the effects of IEDs?
- How quickly is the State able to respond to changes in the use of IEDs? How quickly can the State acquire new capabilities or deliver updated training to mitigate new IED threats?

It is essential that States provide sufficient protection for those involved in the administration and delivery of justice against any credible threats, including those originating from terrorist groups and their use of IEDs. Judges, prosecution lawyers, prison officers, and investigating police officers have been targeted in the past, and due safety and protection consideration must be given to maintaining the integrity of the entire criminal justice process.

### **Development of IED countermeasures (3.8)**

The ability to respond to changes in the use of IEDs by terrorist groups, and associated groups, is fundamental to an effective counter-IED strategy as it adapts, updates, and strengthens the national response in line with the threat faced. The key elements of counter-IED maturity include the extent to which the State can respond to either predicted or actual changes in the terrorists' use of IEDs and is then able to develop effective countermeasures. Counter-IED maturity is, in effect, a measure of the capacity of the State to implement a feedback loop to learn and respond appropriately and consistently. The recovery of IED components is essential in aiding understanding of the effectiveness of IEDs against friendly force protected structures and vehicles. The recovery of components from radio-controlled IEDs is also crucial in informing the development of electronic countermeasure systems.

To maintain the support of the general population in areas where IED use is prevalent, it is important that IED awareness material is updated as IED threats change. Changes in the tactics, techniques and procedures employed by terrorist groups and other criminals also need to be brought to the attention of members of the State's security forces who are not counter-IED specialists. There is then also a need to update and adapt capacity-building strategies and activities for the State's security forces and other agencies. Finally, it should also be recognized that effective IED countermeasures facilitate the delivery of principled humanitarian activities to populations in need.

## Submodule II

# Technical guidance to facilitate the implementation of Security Council resolution 2370 (2017) in preventing terrorists from acquiring unmanned aircraft systems and components

## Introduction

---

The acquisition of UAS and components by terrorist groups and individuals poses an international threat and challenge to international peace and security. By 2020, at least 20 armed non-State actors, including terrorist groups, have reportedly obtained, or acquired UAS and components.<sup>28</sup> Through resolution 2370 (2017), the United Nations Security Council strongly condemns the continued flow of UAS and components to and between terrorist groups (or associated groups) and criminals. United Nations Security Council resolution 2370, and relevant subsequent resolutions, calls on all States to eliminate the supply of these systems and components to those involved in terrorist acts.

The Security Council, in its resolution 2617 (2021), noted with concern the increasing global misuse of UAS by terrorists to conduct attacks against, and incursions into, restricted commercial and government infrastructure and public places, acknowledging the need to balance fostering innovation and preventing misuse of UAS as its applications expand.

In recent years, the proliferation of inexpensive, primarily small-sized UAS and components, as well as their use and weaponization by terrorist groups has increased sharply. In Iraq and the Syrian Arab Republic, for example, ISIL (Dae'sh) reached a high level of sophistication in production of weaponized UAS and frequently used them in attacks. In other parts of the world, for example in the Middle Eastern and across parts of the African region, terrorist groups have also used weaponized UAS to attack targets. In conflict-affected settings, this can be considered one of the most concerning developments and threats facing States in countering terrorism.<sup>29</sup> The means and methods through which terrorist groups acquire and use UAS and components, including their weaponization, continue to evolve. Delivery methods are in some cases and contexts also becoming more complex – for example, the combined use of UAS and IEDs– illustrating the constantly evolving nature of the operational terrorist environment.

---

28 See 'Use of Armed Drones for Targeted Killings', Report of the UN Special Rapporteur on extrajudicial, summary, and arbitrary executions, UN Doc. A/HRC/44/38, 15 August 2020, para. 9.

29 See US Central Command, "MEI Engagement with General Kenneth F. McKenzie Jr.", 11 June 2020, <https://www.centcom.mil/MEDIA/Transcripts/Article/2216473/mei-engagement-with-general-kenneth-f-mckenzie-jr>.

A thorough understanding of a specific terrorist group's system<sup>30</sup> through which it acquires UAS and their components, and the possible links to other such systems, is a prerequisite to developing effective measures to prevent terrorists and terrorist groups from acquiring and using UAS and components.

## Terminology (1.1)

A UAS may be described as:

A system whose components include the necessary equipment, network, and personnel to control an unmanned aircraft. UASs are remotely piloted, pre-programmed, or controlled vehicles that can perform an array of tasks such as, surveillance, reconnaissance and targeting support.<sup>31</sup>

Multiple terms or definitions are used for UAS and their components.<sup>32</sup> An unmanned aerial vehicle (UAV), or "drone" as they are sometimes known, represents the aircraft component of UAS.<sup>33</sup> The three principal components of UAS are described below.

### 1. Components of UAS (1.1.1)

---

UAS have three principal components:

**Unmanned aerial vehicle (UAV).** UAVs are the airborne components of UAS; a UAV consists of the airframe, the navigation system, the power system, and the payload. The airframe provides the structure within which all the other airborne components of UAS are mounted. Lift may be provided by fixed wings or (multi) rotors. UAS power may be provided either by batteries alone or by a combination of batteries and liquid-fuelled engines or rocket motors. UAS may navigate autonomously using external navigation systems provided by satellites or by inertial methods using on-board accelerometers and gyroscopes to provide inputs to an autopilot. Alternatively, a UAV may operate under direct control by a human operator, commanded over a ground-to-air communications channel. UAVs also employ a flight computer fed by on-board sensors such as inertial measurement units and gyroscopes (similar to those found in a smartphone) to maintain the altitude of the aircraft within defined parameters and to make the system easier to operate.

---

30 The term "system" should be understood in a broad context here. For example, terrorist groups, and associated groups, employing and using weaponized UAS have their own specific characteristics and nuances. Terrorist groups such as ISIL (Da'esh), and associated groups, operating transnationally have different approaches, methods, ways and means for the acquisition of UAS and components than, for example, criminals using UAS to protect or sustain production, distribution, or illicit trade in other illicit goods.

31 US Department of the Army, Techniques for Combined Air Defense, US FM ATP 3-01.8, 2016.

32 The International Civil Aviation Organization's definition of an aircraft is as follows: "Any machine that can derive support in the atmosphere from the reactions of their air other than the reactions of the air against the earth's surface". ICAO proposes to define and describes an "unmanned aircraft system" as an "aircraft and its associated elements which are operated with no pilot on board". See International Civil Aviation Organization, Unmanned Aircraft Systems (UAS), Cir 328-AN/190, (ix), 2010.

33 Note also that the term "uncrewed aerial vehicle" is increasingly used by some States instead of "unmanned aerial vehicle", as a more gender-neutral term.

**Ground control system (GCS).** The GCS allows the human controller to either control the UAV in flight or program the UAV before flight with a predetermined flight plan. Most GCSs enable human operators to communicate with and command the UAV or its payload when in flight by way of a radio frequency link. GCSs vary in complexity. Some may be as simple as an application on a smartphone or tablet device. Others may consist of a dedicated remote controller, often accompanied by a screen that provides a live view from the drone's camera. More complex GCSs, such as those used to operate large drones, may include complete cockpit-like control hardware and sophisticated communication infrastructure.

**Payload.** UAVs can carry a wide range of payloads. For the purposes of this document, two types of payloads are especially relevant to terrorist use of drones: cameras and explosives.<sup>34</sup> Typically, UAVs employ some form of camera system. Imagery may be passed to the GCS in real time via a communication channel for navigation, enabling operators to see the drone's location and surroundings, and to gather real-time intelligence. Imagery can also be stored in non-volatile memory on board the UAV for use after the flight (e.g., for further intelligence analysis or for the creation of propaganda). Some UAS might be equipped with infrared or thermal-imaging cameras, which can enable operations at night (e.g., to detect humans, vehicles, and other heat signatures).

Explosive payloads with small UAVs observed in usage by terrorist groups have typically had a high explosive content of less than 1 kg and have often been based on modified military munitions. While a focus on the high explosive carriage capacity of payloads is useful, even payloads with small high explosive content may have inversely larger effects on targets.

## 2. Types of UAVs used in terrorist attacks (1.1.2)

---

Most approaches for categorizing UAVs do so by weight, with reference made to additional performance characteristics, such as operating altitude, velocity, and operational endurance.<sup>35</sup> While larger categories of UAVs have generally been used by State militaries only, terrorist groups generally operate small UAVs.

Small UAVs typically carry relatively small payloads, can operate at a low level and altitudes of 1,500 m or higher, and beyond the visual line of sight of the operator. A distinction is made between 'fixed-wing' and 'vertical take-off and landing' (VTOL) UAVs. Small VTOL UAV require little space and can launch vertically.

An even smaller category of systems – micro-UAVs – may only weigh a few hundred grams and are typically used purely for intelligence, surveillance and reconnaissance and most often operate at an altitude of less than 500 m and within visual line of sight of the operator.

---

34 There are concerns about non-State actors' use of UAS and components as a delivery vehicle for chemical, biological, and radiological agents. United Nations Security Council resolution 1540 (2004) decides that States shall adopt and enforce appropriate effective laws that prohibit any non-State actor from manufacturing, acquiring, possessing, developing, transporting, transferring, or using nuclear, chemical, or biological weapons and their means of delivery. It also requires States to enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, and biological weapons and their means of delivery. Devices and payloads containing chemical, biological, radiological, or nuclear materials are considered out of the scope of this sub-module and the technical guidelines.

35 See Joint Air Power Competence Centre, "Annex A: NATO UAS Classification Table" in *A Comprehensive Approach to Countering Unmanned Aircraft Systems*, pp. 510–511.

### 3. Types of terrorist use of UAS (1.1.3)

---

Terrorist use of UAS has increased sharply in recent years. Small-sized UAS have provided terrorists with a simple and low-cost method of facilitating, supporting, or executing attacks. Small drones are difficult to detect and counter using existing surveillance and air defence systems. The principal ways in which terrorists use UAS are:

**Intelligence, surveillance, and reconnaissance.** UAS are used to acquire information, conduct surveillance on areas of interest, reconnoitre “over the hill or around the corner” and monitor potential targets from a stand-off distance.

**Targeting support.** UAS may be used to guide the employment of other weapon systems, such as indirect fire systems and suicide vehicle borne IEDs (SVBIEDs). When used in support of indirect fire systems, such as artillery, free-flight rockets, or mortars, UAS allow operators to observe the point of impact and adjust the aim accordingly. When used in conjunction with SVBIEDs, UAS may be able to provide real-time aerial imagery to operators driving SVBIEDs in order for them to avoid defensive measures en route to their target.

**Direct or indirect attack.** There are two basic modes in which UAS may be employed in the attack of targets. In an indirect attack, the UAV is flown towards the target and drops an explosive device on command or at a predetermined position. In the direct mode of attack, the UAV itself contains an explosive device, and the complete UAV is guided onto an identified target, somewhat like a loitering munition or cruise missile. This latter category of systems is sometimes colloquially referred to as “suicide drones”. Alternatively, the impact of the UAV alone may cause serious injury or damage in direct attack mode.

**Swarm attack.** One of the forms of terrorist use of UAS that could be hardest to defend against is a swarm attack, where large numbers of UAVs, some perhaps operating in different modes, are launched at a target to overwhelm defensive measures, achieve greater kinetic effect on the target or cover a wider area in attack.<sup>36</sup>

## Objective of this submodule (1.2)

The primary objective of this submodule is to provide technical guidance to State officials, as well as other relevant and interested stakeholders, to facilitate the implementation of resolution 2370. In particular, this submodule aims to provide technical guidance to enable effective implementation of prevention and preparedness measures aiming to prevent terrorists from acquiring UAS and components, as well as from using weaponized small UAS.

The document is designed to facilitate self-assessment by States in their efforts to develop, refine, and implement technical measures to prevent terrorists from acquiring UAS and components and to prepare against incidents at the national level. The document may also be used by relevant United

---

36 At the time of writing, most cases of reported non-State “drone swarms” may not actually be “swarms” in the technical sense of the term and available, proposed definitions, but rather large agglomerations of individually controlled drones. See, for example, M. Ekelhof and G. Persi Paoli, *Swarm Robotics: Technical and Operational Overview of the Next Generation of Autonomous Systems*, UNIDIR, 2020.

Nations and other specialized entities to support States in such efforts, including to support national assessments and in facilitation of technical assistance to States. The document represents one of several means and methods available to support States and the technical community of practice in such efforts.

### Methodological approach (1.3)

The methodological approach applied in this submodule draws on a CMM. CMMs have been widely adopted by institutions, administrations, and organizations, including by the United Nations, as they provide a disciplined framework to systematically assess the maturity of processes and practices, to identify gaps and areas for improvement, and to achieve progress in complex domains.<sup>37</sup> A CMM can be considered a set of structured levels, describing how States can reliably and sustainably produce desired outcomes to prevent terrorists from acquiring UAS and components. As a guiding reference, capability maturity levels may range as follows:

**Initial:** processes are characterized as ad hoc and, occasionally, even chaotic. Few processes are defined, and success depends on individual effort.

**Repeatable:** basic management processes are established, and the necessary process discipline is in place to repeat earlier successes on projects with similar applications.

**Defined:** processes are documented, standardized, and integrated into the organization's overall processes.

**Managed:** detailed measures of processes and product quality are collected, and the products and processes are quantitatively understood and controlled.

**Optimizing:** continual process improvement is enabled by quantitative feedback from the processes and from piloting innovative ideas and technologies.

These capability maturity levels, and their descriptions are guiding in nature. They may serve as a useful reference for users of this document when assessing the maturity of the national and/or organizational measures in place to prevent terrorists from acquiring UAS and components.<sup>38</sup>

### Structure of this submodule (1.4)

This module is divided into two subcategories: (i) upstream measures (section 2), focused on those activities aimed at preventing terrorists from acquiring small UAS and components, and (ii) downstream measures (section 3), associated with mitigation and response to a particular terrorist event involving a small UAS. The general premise of the CMM, which underpins this submodule, is that the greater the maturity and effective implementation by a State of upstream measures, the fewer downstream

---

37 B. Seddon and A. Malaret Baldo, Counter-IED Capability Maturity Model & Self-Assessment Tool, UNIDIR, 2020 (in particular, pp. 10–15).

38 For a full and comprehensive assessment of the capability maturity model, refer to and use the Counter-IED Capability Maturity Model & Self-Assessment Tool, 2020, currently available in English, French, and Spanish: <https://unidir.org/publication/counter-ied-capability-maturity-model-and-self-assessment-tool>

measures will be required. This is further reinforced by a critical feedback loop and lessons learned mechanism, through which downstream measures inform strengthened upstream measures.

Under each upstream and downstream measure covered by this submodule, a set of key issues for consideration is provided, in the form of guiding questions, to help users consider further and/or assess national or organizational processes and measures to prevent and mitigate terrorist acquisition and use of UAS and components.

## **Respecting human rights, fundamental freedoms, and international humanitarian law, and gender and age-related implications (1.5)**

Although there are differences in preventing and mitigating terrorist acquisition and use of UAS and components in conflict-affected and non-conflict settings, as well as different rules and bodies of law that apply in each case, the right to life and the protection of civilians in line with international humanitarian law as well as the full respect for human rights in line with international human rights law is a priority in any environment and under any circumstances.

Given the risks posed to the right to life by terrorist use of UAS and components, efforts by States to prevent such use is critical from a human rights perspective.<sup>39</sup>

At the same time, in addressing the risks posed by malicious, criminal, and terrorist use of UAS and components through the development of capabilities, systems and techniques to counter UAS, States must respect their obligations under applicable domestic law and international law.

States must comply with international human rights law<sup>40</sup> as well as consider and address potential risks to the protection of these laws, including the right to privacy (and where personal data are involved, via data protection). Human rights implications should also be duly considered with respect to licensing and approval regimes. Preventing and mitigating threats posed by terrorist use of UAS and components requires States to take necessary and adequate measures to prevent, combat, and punish related criminal acts in the context of their duty to protect persons within their jurisdiction from undue interference with their human rights by third parties. This obligation must be carried out in line with international human rights law.<sup>41</sup> Among others, it is critical that capabilities, including systems and techniques, developed, and authorized by States to counter UAS acquisition and use by terrorists do not subject individuals to arbitrary or unlawful interference with their privacy, family, or home. Any

---

39 As the UN Special Rapporteur on extrajudicial, summary, or arbitrary executions has noted, at least 20 non-State armed actors, including terrorist groups, have reportedly obtained armed and unarmed drone systems. See 'Use of Armed Drones for Targeted Killings', Report of the UN Special Rapporteur on extrajudicial, summary, and arbitrary executions, UN Doc. A/HRC/44/38, 15 August 2020.

40 Internationally protected human rights include the protection of privacy. Prominent protection for privacy is found in international treaties, including article 12 of the Universal Declaration of Human Rights (1948) and article 17 of the International Covenant on Civil and Political Rights (1966).

41 See, for example, ALADDIN, D3.2 – Data protection, Social, Ethical and Legal Frameworks – V2, 2019, [https://aladdin2020.eu/wp-content/uploads/2020/08/ALADDIN\\_D3.2\\_DataProtectionSoEL\\_FrameworkV2\\_PU\\_V10.pdf](https://aladdin2020.eu/wp-content/uploads/2020/08/ALADDIN_D3.2_DataProtectionSoEL_FrameworkV2_PU_V10.pdf).

limitations on the right to privacy must be provided by law (which may require prior authorization by a competent judicial authority) and must be necessary and proportionate to the legitimate aim pursued.

All possible different impacts and potential implications of upstream or downstream measures described in this submodule on women, minors, groups, and persons who may be marginalized or discriminated against, including members of ethnic, racial, religious, and other minorities, as well as persons in vulnerable situations, such as those forcibly displaced or otherwise affected by armed conflict and other types of violence, are to be duly taken into account by all users of this submodule.

All upstream and downstream measures described in this submodule are to be considered, used, and applied in full respect of obligations under international law, including international human rights law, international humanitarian law as well as the rule of law.

## **Countering terrorist acquisition and use of UAS: upstream measures**

---

### **National policy, legislation, regulation, and administrative procedures (2.1)**

#### **1. National policy or strategy (2.1.1)**

---

The State should have an overarching policy that defines a comprehensive whole-of-government strategy to countering UAS. This is because a State's overall ability to counter UAS threats is significantly hindered by variations in policies, the development and use of different standards, and the procurement and/or deployment of differently capable counter systems. Likewise, the fragmented or inconsistent application of such policies poses further significant challenges to a state's ability to adequately counter UAS threats. The upstream and downstream measures described in this submodule must all be implemented in concert; none of them on their own will suffice to prevent and mitigate terrorist acquisition and use of UAS and components.

For such a strategy to be effective, it must be based on regular, systematic assessments of threats and risks, as well as corresponding countermeasures and technologies, at different (e.g., national, subnational, and local) levels and in defined contexts and locations domestically. Given the rapid technological evolution, it is necessary that such a strategy is regularly reviewed nationally through an all-inclusive – and possibly subregional or regional and/or international – multi-stakeholder consultative process, and that the strategy is subsequently updated. States may designate a suitably resourced and empowered ministry or department, which may be identical to the entity leading national coordination (see section 2.1.2), to lead the development, implementation, and review of such a strategy.

Given the complexity of the subject and the sheer number of governmental agencies involved, ICAO's UAS Toolkit<sup>42</sup> recommends an approach whereby States put forward a whole-of-government UAS strategy seeking to achieve the following goals:

- A roadmap that identifies safety, security, and economic objectives of the future UAS industry
- A government interdepartmental UAS committee to share information and help departments operating UAS to plan their activities
- A methodology to align the needs of the industry with government resources
- Coordination activities to enhance industry stakeholders' access to funding to explore new technologies and market applications.<sup>43</sup>

---

42 Source: <https://www.icao.int/safety/UA/UASToolkit/Pages/default.aspx>

43 Additionally, when making efforts to protect civil aviation infrastructure from acts of unlawful interference carried out with unmanned aircraft, it is recommended that States take also into consideration measures described in the ICAO Aviation Security Manual, Doc 8973, Chapter 19 – Protection of civil aviation infrastructure against unmanned aircraft



Photo / Adobe Stock

## **2. National coordinating entity and coordination mechanisms (2.1.2)**

---

Effective prevention and mitigation of the acquisition and use by terrorists of UAS requires cooperation by a wide range of actors, including domestically between government ministries or departments, ideally coordinated by a suitably resourced and empowered lead entity to avoid diffusion of responsibility among stakeholders. The designation, or establishment, of a national coordinating lead entity and designated points of contact across and within all concerned national authorities at different levels (e.g., national, subnational, and local levels), as well as defined coordinating mechanisms, can significantly improve the efficiency and coherence of cross-government approaches to counter threats posed by terrorist use of UAS, as well as ensure effective coordination in response to an incident.

### Box 17. Key issues for consideration on national policy or strategy

- Does the State have a national policy or strategy for countering UAS threats? If so, does it encompass an effective whole-of-government approach to counter-UAS?
- Is the national counter-UAS policy or strategy based on assessments of the threats and risks related to terrorist use of UAS and components? Have these assessments been undertaken systematically and following a standard or predefined methodology at different (e.g., national, subnational, and local) levels domestically, in different contexts and at defined locations?
- Has an ex-ante impact assessment (e.g., of all safety, security, legal, human rights, including privacy and other aspects related to the impact of UAS countermeasures, systems, and technologies) been undertaken for the development, or evaluation and review, of such a national policy or strategy?
- Does the State have a mechanism in place to ensure that its national counter-UAS policy or strategy is regularly reviewed through an all-inclusive multi-stakeholder process and subsequently updated? Specifically, does this process include the actors developing and implementing the policy or strategy, as well as those impacted by its implementation?

While airspace control (e.g., licensing the lawful use of UAS) is generally best managed by the competent aviation authorities, and enforcement by law enforcement, the evaluation and assessment of threats posed by terrorist use of UAS at different national levels, locations, and specific contexts should be handled by a national entity with a capacity to collect, collate and analyse terrorist- and UAS-related intelligence. A variety of techniques may be used to assess and evaluate such threats. Most of them include a combination of assessing terrorist capabilities, intentions, and opportunities to strike a target.

Close cooperation and coordination are required between the State's intelligence entities, law enforcement, and specialist military support agencies for the prosecution of time-sensitive intelligence-led operations against individuals involved in the procurement, development, and operation of UAS and components by terrorist groups. Robust and reliable processes must also be established to allow the flow of information and intelligence between those entities that need it.

### 3. National legislation and regulations (2.1.3)

---

States should develop or put in place legislation or regulations for the prevention and mitigation of threats posed by malicious, criminal, and terrorist use of UAS and components. The legislation or regulations should identify the competent and responsible national authorities that are authorized to detect and, if necessary, intercept and/or disable UAS and components. As the UAS domain is evolving rapidly, most legislators and regulators are unable to keep up with the developments in capabilities of counter-UAS technologies, and the corresponding national legislation and regulations often lag behind

#### Box 18. Key issues for consideration on national coordinating entity and coordination mechanisms

- Has the State designated a national counter-UAS coordinating lead entity that is suitably resourced and empowered to ensure coordination among all relevant national authorities (including civilian and military authorities) and domestic actors?
- To what extent are the roles and responsibilities of national authorities at different levels involved in counter-UAS (e.g., national, subnational, and local level) defined and coordinated (e.g., by and through a national lead entity and coordinating mechanisms)?
- Does the State have a designated national entity responsible for the authorization, or the delegation of authorizations, of any active measures taken to counter UAS?
- Does the State have a designated counter-UAS point of contact at the national level that is competent and responsible for sharing information with and receiving information from international stakeholders? Has the State communicated this point of contact to relevant international stakeholders (e.g., through official communication channels)?
- Does the State actively cooperate internationally with relevant regional and international organizations, including for the development of its counter-UAS strategy or policy?
- Is there effective inter-agency cooperation and sufficiently empowered coordination mechanisms? To what extent do such coordination mechanisms cover the national, subnational, and local levels? Are such inter-agency cooperation arrangements and coordination mechanisms ad hoc or formalized (e.g., through a written procedure)?

technical developments. Different counter-UAS technologies can potentially be subject to a wide range of regulations at various levels and from distinct bodies of law. This requires that:

- Regular, inclusive national legislative review processes are undertaken;
- Relevant national legislation and regulations are regularly and accordingly updated; and
- Continual awareness-raising takes place among State and non-State entities, including private sector and other entities, of applicable national legislation and regulations, as well as the factors determining their application to counter-UAS systems, technologies, users, and use.

The development, implementation and enforcement of civil aviation legislation and regulations can support States in narrowing down the number of possible use case scenarios and better identify high-risk use case scenarios (e.g., terrorist use of UAS). While terrorists and criminals will not abide by and comply with such legislation and regulations, the development, effective implementation, and enforcement of such legislation and regulations can contribute towards the prevention and mitigation of high-risk cases of UAS use by terrorist groups or individuals.

The Convention on International Civil Aviation explicitly affirms individual States' responsibility to authorize the operation of pilotless aircraft and to ensure that the operation of such aircraft is controlled

so as to obviate dangers to civil aircraft.<sup>44</sup> National policies for drone use vary significantly, both in terms of substance and maturity; some States have been developing these policies for over a decade, while others have only begun more recently. Most UAS regulations have four basic elements:

- Licensing requirement for operators;
- Registration for operators or aircraft (or both);
- Designation of restricted airspace zones and limits on drone operations; and
- Insurance requirements for certain types of aircraft or operation<sup>45</sup> (for UAS operations that are not regulated as part of the certified category of operations,<sup>46</sup> States should apply a risk-based, operation-centric approach<sup>47</sup>)

Many States have designated restricted airspace – “no-drone zones” – around airports, critical infrastructure, sensitive facilities, and major public events. Limits on use may include requirements for the UAV to be operated:

- Within visual line of sight;
- During daylight hours only; and
- Below a certain altitude ceiling

---

44 Article 8, Pilotless Aircraft, of the Convention on International Civil Aviation, 2006.

45 T. Jones, International Commercial Drone Regulation and Drone Delivery Services, Rand Corporation, 2017.

46 “Certified category of operations” refers to a high-risk operation that requires certification of UAS, a licensed remote pilot and an operator approved by the competent authority in order to ensure an appropriate level of safety. The International Civil Aviation Organization is developing standards for such operations.

47 See the tools of the Safety Management System framework, as laid out in International Civil Aviation Organization, Annex 19: Safety Management, 2016, and International Civil Aviation Organization, Safety Management Manual, 4th ed, Doc 9859, 2018. See also Joint Authorities for Rulemaking on Unmanned Systems, JAR Doc 06 SORA (package) and tools, 2019, <http://jarus-rpas.org/content/jar-doc-06-sora-package>.

### Box 19. Key issues for consideration on national legislation and regulations

- To what extent do extant legislation and regulations identify the competent and responsible State authorities authorized to detect and, if necessary, intercept and/or disable UAS and components in specific circumstances and contexts?
- Are there robust and comprehensive civil aviation legislation and regulations in place that are fit for purpose and cover the lawful use, including by civilians, of specific and defined categories of UAS and components in defined airspace zones?
- Has the State incorporated State use of UAS into the national aviation legislation or regulations (e.g., military use, use by law enforcement, components in defined airspace zones)?
- Does the State have a system in place for licensing the commercial use of UAS? If so, does it define specific areas where defined categories of UAVs are not to be operated? Have the conditions which apply to licensing, both in substance and procedure, been subject to human rights analysis? Are electronic remote identification and geo-fencing configurations considered part of licensing criteria for commercially produced UAV use by the emergency services (e.g., during fire emergencies) in restricted airspace and urban environments?

In some States, operators can seek exemptions from these restrictions (e.g., for experimental flights or for emergency response operations). Where restricted areas (or operating zones) are established, defined operators and categories of UAS are authorized to fly safely (e.g., for UAS supply corridors and for military and humanitarian use) as part of a broader UAS traffic management system.<sup>48</sup>

In licensing the commercial use of UAS, national regulatory authorities may consider defining specific areas where UAVs may not be operated and mandating that commercially produced UAVs are configured with electronic remote identification systems and geo-fences so that the UAV is unable to operate within specified areas.<sup>49</sup> Although geo-fences may prevent those with limited technical skills from operating UAS in prohibited areas, terrorists may adapt or modify commercially available UAVs to overcome geo-fences.

#### 4. National technical standards (2.1.4)

Currently, there are no technical standards at the international level for Counter-UAS. Efforts to standardize specific aspects of countering UAS and technologies (e.g., their design, testing and assessments, procurement, use and evaluation) are beginning to take form at the subregional or regional and international level, within the civilian and military domains.<sup>50</sup> The development of technical standards is one possible means for States to standardize practices and procedures in the counter-UAS

48 See International Civil Aviation Organization, Unmanned Aircraft Systems Traffic Management (UTM) – A Common Framework with Core Principles for Global Harmonization, Edition 3, <https://www.icao.int/safety/UA/Documents/UTM%20Framework%20Edition%203.pdf>; see also US Department of the Army, "Chapter 3: Airspace Management" in Unmanned Aerial Vehicles (UAV), FM 34-25-2, <https://fas.org/irp/doddir/army/fm34-25-2/25-2ch3.pdf>.

49 Geo-fencing is usually employed in conjunction with satellite-based GNSS (Global Navigation Satellite System) so that the flight control system of the UAV prevents the system from entering prerecorded out-of-bounds areas.

50 One specific regional example from the civilian sphere includes the European Union Aviation Safety Agency manual, Drone Incident Management at Aerodromes, which offers some guidance on the procurement and testing of counter-UAS technology to competent national authorities of the Agency's Member States; see <https://www.easa.europa.eu/newsroom-and-events/press-releases/easa-issues-guidelines-management-drone-incidents-airports>.

#### Box 20. Key issues for consideration on national administrative procedures and technical standards

- Do relevant national authorities document good practices and lessons learned from the design, development, assessment and testing, procurement, use, and evaluation of counter-UAS systems and technologies? Does the State share and exchange relevant good practices with international stakeholders in relevant international forums?
- Does the State have access to and use available good practices shared or being further developed internationally to safely and securely respond to a malicious, criminal, or terrorist incident involving a small (e.g., recreational, commercial, or bespoke) UAV?
- Does the State have access to and use available good practices shared or being further developed internationally to safely and securely respond to a malicious, criminal, or terrorist incident involving other categories of UAS and components?

domain. It is also a possible means for States to strengthen cooperation with private sector industry by providing a level playing field, to facilitate interoperability, as well as overall more effective and cohesive approaches to preventing and mitigating UAS threats.

In developing their own technical standards for responding to an incident involving a small drone, States can refer to, and are encouraged to use, technical guidance contained within the INTERPOL Framework for Responding to a Drone Incident. This framework has been developed to fill a knowledge gap at the international level and increase the capacity of law enforcement globally – in particular, of first responders and digital forensic practitioners – and other interested stakeholders to safely and effectively respond to an incident involving malicious, criminal, or terrorist use of small (recreational, commercial, or bespoke) UAVs.<sup>51</sup>

## Capability, normative, and operational development for countering UAS (2.2)

The development of a capability to counter UAS covers all actions that a State is required to undertake to prevent the terrorist use of UAS. This topic is much broader than the adoption of UAS technical countermeasures (see section 3.1). Generally, a coherent and coordinated whole-of-government approach is the most effective.

Denying terrorists access to UAS and components is the most straightforward passive countermeasure. This may be achieved through the comprehensive implementation of the upstream measures detailed in this document. The introduction of a regulatory regime based on licensing and the effective control of borders could potentially help prevent terrorists from gaining access to UAVs with significant capabilities. The creation of “no-drone zones” and restricted airspace (see section 2.1.3) (as well as actual and enforced prohibition or restrictions for individuals to operate UAVs in such zones and airspace, accompanied by accountability measures for misuse), for example, is a straightforward method of drawing attention to those with malicious, criminal, or terrorist intent. This is in addition to targeted public awareness-raising activities on UAS-related threats and risks.<sup>52</sup> The use of electronic remote identification systems, as well as geo-fencing in commercial UAS, though in the latter with some limitations, reduces the ease with which restricted airspace can be breached.

Passive and active counter-UAS technologies are covered in greater detail in section 3.1. A national entity, which may be identical to the above-mentioned national lead coordinating entity (see section 2.1.2), should be designated and responsible for the authorization, or the delegation of authorizations, of any active measures taken to inhibit or defeat UAS and components. Such active measures are also described in section 3.1.

---

51 See INTERPOL, Framework for Responding to a Drone Incident, 2020; see also INTERPOL, Global Guidelines for Digital Forensics Laboratories, 2019.

52 See E. Miasnikov, Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects, Center for Arms Control, Energy and Environmental Studies, Moscow Institute of Physics and Technology, 2005, pp. 23–24.

A capability to counter UAS must be adaptable, as terrorist tactics, techniques, and procedures change, and threat environments evolve. Critical activities can include:

- Institution of a monitoring system of UAS and components acquired and used by terrorist groups and individuals;
- Monitoring by national authorities of the available, corresponding, or required counter-UAS technologies and equipment; and
- Periodical reviews and, if needed, adjustments to counter-UAS technologies and equipment to respond to evolving threats.

At its most basic and immediate level, the State must have:

- Specialist and trained personnel capable of managing a coordinated (and likely interoperable) use of counter-UAS technologies (e.g., by law enforcement and the military);

#### Box 21. Key issues for consideration on capability, normative and operational development for countering

##### **Detect and mitigate the device**

- Can the State use, in compliance with domestic law, and other applicable law, in-service equipment in a counter-UAS role (e.g., electronic countermeasures, air defence systems, signals intelligence systems, international mobile equipment identity detection, or international mobile subscriber identity catcher systems)? Can obsolescent systems be repurposed for use in countering UAS threats?
- How effective is the State's system for acquiring (e.g., through procurement) or accessing (e.g., through renting, as may be the case in certain contexts) the necessary counter-UAS technologies and equipment, as well as in providing end users with integrated logistical and operational support, to enable its personnel to operate in a high-threat environment?
- How effective is the inter-agency cooperation within the State in developing drills, tactics, techniques, and procedures to mitigate terrorist and criminal use of UAS?

##### **Engage the network**

- To what extent does the State have a clear understanding of the terrorist groups and individuals that are employing and weaponizing UAS and components?
- To what extent does the State have a clear understanding of the networks and individuals suspected or confirmed to be involved in the procurement, development, or operation of UAS components by a terrorist group or individuals?
- Does the State have a strategy for identifying and exploiting the critical vulnerabilities in the organizations or individuals involved in the procurement, development, and operation of UAS components by a terrorist group or individuals?
- Does the State have a procedure for periodic reviews and, if needed, adjustments of counter-UAS technologies and equipment to respond to evolving threats? If so, is this procedure codified (e.g., in the form of a written procedure)?
- How does the State use forensic (including biometric and digital) intelligence gained from

the exploitation of recovered or retrieved UAS and components to identify those involved in the procurement, development, and operation of terrorist UAS?

- Does the State take measures to prevent terrorists from the exploitation of information and communications technology, such as online and darknet markets, to counter the sharing of knowledge on the building and weaponization of UAS?
- Is the State able to mount and prosecute pre-emptive operations aimed at preventing terrorist groups and individuals from acquiring and using UAS and components, including use through weaponization?
- How does the State exchange, if it all, information on countering existing or emerging UAS-related terrorist threats with relevant international partners?

#### **Prepare the population**

- Does the State have an effective approach to UAS public risk awareness and education? For example, does the State have a means by which the effectiveness of such UAS public risk awareness and education is measured?
- To what extent is the State undertaking measures to enhance public trust by improving transparency regarding the use of UAS and components, as well as potential risks?

#### **Prepare teams and personnel**

- How effective is the State in preparing and training its personnel and organizations involved in counter-UAS? For example, does the State have facilities and suitably trained and equipped individuals to conduct the training of counter-UAS system managers and operators, first responders, and digital and biometric forensic specialists? How many counter-UAS systems managers, operators, first responders, and digital and biometric forensic specialists does the State train each year?
- How does the State disseminate changes in its own forces, law enforcement and other agencies' counter-UAS tactics and procedures as a result of changes in the UAS terrorist threat?

- Authorized and trained personnel and teams capable of operating counter-UAS technologies and equipment to detect, and if necessary, interdict and/or disable UAS;
- Trained and equipped personnel and teams capable of safely and securely responding to an incident; and
- Trained specialist personnel and teams capable of technical exploitation, including the undertaking of (biometric and digital) forensics on recovered UAS and components.

Another critical activity is horizon scanning of emerging threats posed by terrorist acquisition and use of UAS and components, domestically and possibly also internationally. This is to promptly assess, and where required, develop, or adjust measures and to anticipate and adapt counter UAS capabilities that will be required to respond to predicted future terrorist threats.

Other counter-UAS capabilities required by States are also covered in greater detail in the downstream section of this submodule (see section 3).

## Considerations pertaining to specific areas and activities (2.3)

### 1. Customs and border control (2.3.1)

---

Border controls can be a means of denying terrorists access to UAS, especially where there is no indigenous UAS manufacturing capability. One of the key prerequisites, however, is the development and implementation of an adequate legislative and regulatory regime that specifies the types of UAS, or associated components and subsystems, that are controlled.

In January 2020, the World Customs Organization (WCO) published amendments to the International Convention on the Harmonized Commodity Description and Coding System,<sup>53</sup> which came into force on 1 January 2022. These amendments, for the first time, provide definitions and guidance on the classification of UAS and components, which could assist in the implementation of specific legislation or regulations at State or regional level.

---

53 International Convention on the Harmonized Commodity Description and Coding System, 1983.

#### Box 22. Key issues for consideration on customs and border control

- Do the State and relevant national authorities understand the UAS and components sought, acquired, and used by terrorist groups (or associated groups) or criminals?
- Is the State's approach to border security and customs control coordinated across all relevant government departments? Is there a border security management strategy in place that includes addressing different cross-border threats posed by the misuse and terrorist use of UAS and components?
- How porous are the State's borders? Does the State share a land or littoral border with a country where terrorist groups using UAS, and components are active? Is there any evidence or intelligence to suggest that terrorist groups (or associated groups) or criminals use UAS to smuggle illicit goods across borders? Is there a previous record of smuggling of illicit goods into the country?
- Is there evidence to suggest that terrorist groups (or associated groups) or criminals have suborned customs or border officials to facilitate the passage of illicit goods across borders?
- To what extent does the State participate in relevant regional and international forums? (This is especially important where neighbouring States may already be facing a significant threat posed by terrorist use of UAS and components.)

The WCO Programme Global Shield, described in Submodule I of this document, which focuses on countering the terrorist use of IEDs, may also be able to address emerging threats, including those posed by the terrorist acquisition and use of UAS and components.

## 2. Control of UAS and key subsystems (2.3.2)

It is a decision for individual States to determine what level of regulation they apply to the commercial and non-governmental use of UAS within their national borders. Regulation and control of fully manufactured UAS is relatively straightforward and can be based on easy-to-measure characteristics. The situation with the control of UAV components is more difficult. In some respects, the control of UAS subsystems has similarities to the control of IED precursors in that many UAS components are dual use in nature and have legitimate uses beyond embodiment in UAVs. The type of subsystems that States may consider regulating include the following: complete UAV airframes for UAVs above a specified mass; aircraft engines above a specified level of thrust; inertial measuring units; long-range air-to-ground communication systems; aircraft autopilot systems; and aircraft weapon carriage systems and associated control systems. The situation with the control of UAS technology is even more challenging. States may consider enhancing coordination and strengthening export control mechanisms, possibly through regional or international organizations, to exchange critical information and to develop and enforce rules against the transnational illicit proliferation of certain UAS and technology.<sup>54</sup>

54 See Global Counterterrorism Forum, Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems, p. 12, <https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/2019/Berlin%20Memorandum%20EN.pdf>.

### Box 23. Key issues for consideration on control of UAS and key subsystems

- Does the State cooperate and coordinate with non-State entities, including the private sector and industry, as well as specialist non-governmental organizations and academia, to identify and analyse trends in the technological development and applications of UAS, as well as their impact on terrorist-related threats and risks?
- Does the State cooperate with non-State entities, including the private sector and industry, to develop different measures for increasing the resilience of small (e.g., commercial, recreational, or bespoke) UAS and components against misuse and illicit use?
- To what extent does the State cooperate and coordinate with non-State entities, including the private sector and industry, to develop and implement technologies and techniques
- for electronic remote identification and geo-fencing configurations of UAS as part of broader UAS traffic management?
- To what extent does the State cooperate with and raise awareness among the private sector and industry to highlight risks and encourage the exercise of enhanced due diligence when exporting UAS and components to zones where terrorist groups operate?

## Law enforcement intelligence led operations (2.4)

Law enforcement intelligence led operations, based on the rule of law and carried out in compliance with international human rights law, underpin some of the most effective preventative measures to counter terrorists' acquisition and use of weaponized UAS and components.<sup>55</sup> Such operations rely on effective implementation of downstream measures (see section 3) and the identification of those involved in the procurement, development, and operation of UAS components that are employed by terrorists (section 3.6).

55 See Global Counterterrorism Forum, Recommendations for Using and Protecting Intelligence Information in Rule of Law-Based, Criminal Justice Sector-Led Investigations and Prosecutions, <https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/2016%20and%20before/GCTF-Rabat-Good-Practice-6-Recommendations-ENG.pdf>; see also Global Counterterrorism Forum, The Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector (in particular Good Practice 6, p. 7), <https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/2016%20and%20before/GCTF-Rabat-Memorandum-ENG.pdf>.

### Box 24. Key issues for consideration on law enforcement intelligence led operations

- To what extent is the State able to direct, collect, analyse, and disseminate intelligence related to malicious, criminal, and terrorist use of UAS and components? For example, does the State have one or several recognized and designated entities for intelligence related to terrorist UAS threats and use of UAS?
- Does the State have a national strategy that supports the use of law enforcement intelligence-led operations, conducted in line with applicable international law standards, to prevent terrorist groups and individuals from procuring, developing, operating, and using UAS and components, including weaponization?
- How effective are internal State measures in coordinating, analysing, and disseminating data and UAS-related terrorist threat intelligence products from multiple domestic intelligence agencies? For example, are there written procedures for inter-agency cooperation on UAS-related terrorist threat intelligence?
- Are there successful examples of where the State has employed UAS-related terrorist threat intelligence to arrest individuals involved in the procurement, development, and operation, as well as use, including weaponized terrorist use, of small UAS?
- Does the State have a domestic security or law enforcement organization capable of collating relevant forms of intelligence and of interdicting persons involved in the procurement, development, and operation of terrorist UAS and components?
- Is the State able to take the products from the analysis of recovered UAS and components and fuse this with other sources of intelligence, such as human intelligence and open-source intelligence?
- Does the State use geospatial or big data analysis techniques to develop intelligence to assist in the identification of those involved in terrorist operations and use of UAS?

For example, in contexts where terrorists are already employing UAS, it is essential that any recovered material is subject to thorough analysis and that the information thus gleaned is fused and disseminated to those capable of taking timely action, including close sources of supply. It is always preferable for suspects to be taken into custody by the State security forces so that further information may be gleaned through lawful questioning. Such lawful questioning and investigation must comply with international law, including international human rights law and international humanitarian law.<sup>56</sup>

A key factor in sustaining effective law enforcement intelligence led operations is the production of actionable or releasable intelligence. In some States, the use of intelligence to proactively degrade the effectiveness of such networks is a line of operation known as “attack the network”. The best intelligence collection and analysis system in the world is of no value if dissemination of timely and actionable intelligence does not take place.

## **International and regional cooperation, including information-sharing (2.5)**

Many terrorist threats, including those posed by terrorist groups using weaponized UAS, are transnational in nature, which underpins the requirement for cooperation – including the sharing of relevant information – domestically but also subregionally, regionally, and internationally.

Cooperation by State entities with a wide range of non-State entities (including private sector industry and commercial entities, civil society including academia, and non-governmental organizations) is essential to ensure that (i) the design and development of relevant legislation and regulations are fit for purpose and do not preclude a legitimate user from employing defined categories of UAS and (ii) counter-UAS technologies are safe and effective, while complying with the applicable domestic and international legal environments. Specialist non-governmental organizations can also play an important role in supporting the development and implementation of several downstream measures, such as the technical exploitation of retrieved or recovered UAS and components; the identification of supply chains used for the acquisition, procurement and development of terrorist operations and use of small UAS and components; and the post facto evaluation of the application of different countermeasures.

Cooperation with the private sector, including industry and commercial entities that have an interest in preventing the misuse of their products for malicious, criminal, and terrorist activities, while simultaneously bringing the most significant technical know-how on UAS, is critical in several other ways. First, engagement with the private sector is key in the design, development and testing of counter-UAS technologies. Second, where some technology, such as communication systems, is dual use in nature, the private sector can assist States in identifying and reporting suspicious transactions that require further investigation. Third, cooperation with the private sector may also play a role in

---

<sup>56</sup> Such questioning and investigation, including any questioning of persons not charged with potential offenses, must comply with the right to liberty and the right to privacy. In particular, State agencies need to ensure that any interference with the privacy of persons not charged with offenses goes no further than necessary and proportionate in service of the legitimate aims pursued by a criminal investigation.

preventing terrorists from exploiting the Internet and worldwide supply chains to source small UAS and components and/or acquire or exchange knowledge on how to build and/or weaponize them.

Generally, cooperation is also critical to fostering a better global understanding of the nature and scale of the evolving threats posed by malicious, criminal, and terrorist use of small UAS. This requires the identification, development or use of appropriate existing cooperative frameworks, allowing the exchange of relevant, eventually structured information (e.g., baseline information and databases). This, in turn, necessitates the identification of shareable informational elements, based on common understanding of defining terms and terminology. States should consider and are encouraged to join such existing efforts, initiated by other States, in cooperation with relevant international and regional organizations.<sup>57</sup>

---

<sup>57</sup> See, for example, Global Counterterrorism Forum, Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems, p. 12, <https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/2019/Berlin%20Memorandum%20EN.pdf>.

#### **Box 25. Key issues for consideration on international and regional cooperation, including information-sharing**

- To what extent does the State recognize that the threats posed by terrorist acquisition and use of UAS and associated components is a transnational problem and requires cooperative and coordinated international efforts? Is the State prepared to share relevant information and develop capabilities in concert with regional and international partners?
- If the State is in receipt of international assistance for countering malicious, criminal, or terrorist use of UAS and components, does it have a counter-UAS strategy for defining its own national priorities in terms of counter-UAS capabilities?
- Does the State have an official list that categorizes and defines UAS and components, as well as terminology? Does the State contribute to, or draw from and integrate, categorizations or defining terminology developed in relevant international forums and through regional or international organizations?
- Does the State cooperate with the private sector, including commercial entities, to raise the awareness of vendors of commercially produced UAVs to identify and report suspicious transactions?
- To what extent does the State centralize and collate reports of malicious, criminal, and terrorist use of UAS as well as related information?
- Does the State have a dedicated national counter-UAS centre or facility? Does the State have access to a regional or international centre (through established cooperation)?
- Does the State have the means to securely receive, store, and process classified information on UAS-related terrorist threat intelligence?
- To what extent has the State, in conjunction with international partners, been successful in curbing the ability of terrorist groups and individuals operating transnationally to acquire and use UAS and components?

# Countering the terrorist acquisition and use of UAS: downstream measures

---

## Counter-UAS, systems and techniques (3.1)

Counter-UAS refers to systems that are aimed at detecting and, if necessary, interdicting and/or disabling UAS.<sup>58</sup> This complex process includes at least four broad steps: detection, identification, location, and tracking; human decision-making; mitigation system activation, including interdiction; isolation and retrieval. These steps involve interactions between several systems, as well as between these systems and human operator(s).<sup>59</sup> Counter-UAS relies on a variety of techniques; the main ones are summarized in Table 1 below. Most effective counter-UAS approaches adopt a “layered approach” that appropriately and adequately integrates the necessary counter-UAS technologies for the detection and mitigation of UAS threats. Most counter-UAS technologies will only be effective if employed in a specific context or environment that is well suited to the capabilities of the system, and if embedded within a broader concept of operations.<sup>60</sup>

At the same time, there are several significant challenges regarding counter-UAS technologies, their use and application. Generally, these relate to policy (see section 2.1.1), the legal and regulatory basis (see section 2.1.3), effectiveness (e.g., detection and interdiction effectiveness), safety, operational aspects (e.g., enforcement of existing law and regulations) and practicality (e.g., the distinction between legitimate and illegitimate drone use).<sup>61</sup>

Generally, a risk-based, operation-centric approach is important, as technical counter-UAS measures and counter-UAS technologies may cause hazards including safety hazards that are equal to or (far) exceed the potential hazards posed by possible terrorist use of UAS.<sup>62 63</sup>

---

58 See A.M. Holland, Counter-Drone Systems, 2nd ed., Center for the Study of the Drone at Bard College, 2019, p.1, <https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf>. Note that these systems are sometimes also referred to as “C-UAS”, “counter-drone technology” or “counter-UAV technology”.

59 See A.M. Holland, Counter-Drone Systems, 2nd ed., Center for the Study of the Drone at Bard College, 2019, pp. 3–4, <https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf>. These systems are sometimes also referred to as “counter-UAS”, “counter-drone technology” or “counter-UAV technology”.

60 In some States, this is elaborated in a concept of operations that explains the goals, scope, and operational concept; lists and explains the roles of the various stakeholders; and provides the definitions and purposes of the technologies envisioned.

61 A.M. Holland, Counter-Drone Systems, 2nd ed.

62 See, for example, Global Counterterrorism Forum, “Section IV: Developing Tactical Countermeasures and Technical Solutions” in Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems, p. 15, <https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/2019/Berlin%20Memorandum%20EN.pdf>.

63 See A.M. Holland, Counter-Drone Systems, 2nd ed., Center for the Study of the Drone at Bard College, 2019, pp. 3–4, for more information and a description of each technique. This submodule and document is technology neutral and does not provide advice or technical guidance for or against any specific counter-UAS technology or technical measure.



**Detection, identification, location, and tracking.** This sometimes includes an initial detection by a first sensor (e.g., a wide-area radar or a radio frequency detector) and a secondary sensor system (e.g., cameras or electronic identification elements) that the object is a UAV; determination of the object’s precise location; and tracking of its movements. Secondary sensor systems may also provide information supporting the determination of criminal or terrorist intent (e.g., a camera capturing weaponization including by explosives). The location of the operator may also be achieved by certain electronic sensors.<sup>64</sup>

**Decision-making.** A decision must then be made by a human operator, oftentimes in a very short time frame, on how to respond to the incoming UAV and initiate necessary follow-up actions.<sup>65</sup> The detection time for small-sized UAVs may in most cases be later and the decision-making time shorter than for larger UAVs (i.e., there is a smaller “response window”).

**Mitigation system activation, including interdiction.** If a threat is determined, a mitigation system is activated to intercept the UAV. This may have a range of possible effects, depending on the technique used (e.g., the UAV landing on the ground; “return to home” mode activation; drone

---

64 A.M. Holland, *Counter-Drone Systems*, 2nd ed., Center for the Study of the Drone at Bard College, 2019.

65 A.M. Holland, *Counter-Drone Systems*, 2nd ed.

Table 1. C- UAS techniques	
Purpose	C-UAS techniques
Detection, tracking, and identification	Include radar, radio frequency, electro-optical, infrared, acoustic, and combined sensors
Interdiction	Include radio frequency jamming, GNSS (Global Navigation Satellite System) jamming, spoofing, dazzling, laser, high-power microwave, nets, projectile, collision drone, or combined interdiction elements
A distinction can be made between platform types, including (and listed in no particular order) ground-based fixed, ground-based mobile, hand-held, and UAV based.	

capture; or partial or complete destruction, for example through lasers, projectiles, collision UAVs or high-powered microwaves).<sup>66</sup>

**Isolation and retrieval.** Following interception and depending on the circumstances and the context, the UAV and other components have to be isolated and retrieved. The processing of such UAVs and other components is covered in downstream measures (see section 3.2 onwards).

A wide variety of active measures may be taken to inhibit or defeat the terrorist use of UAVs. Electronic countermeasure systems can inhibit the communication systems associated with the command and imagery channels on board UAVs. Electronic countermeasure systems employ a variety of techniques, some of which are more damaging to legitimate users of the radio frequency spectrum than others. Constant inhibitors transmit a signal that permanently jams specified frequency bands. Responsive inhibitors, or those that employ specialist techniques to exploit the communications protocols of UAS, have a lower impact on legitimate users but are more complex to implement and are necessarily target specific. Some high-powered directed energy systems and laser-based systems have been fielded, but at high cost and with some technical limitations. A real problem with all forms of electronic or directed energy attack is the fratricidal impacts on other electronic systems. Particularly around airports, the jamming of communication systems, instrumented landing systems and aircraft navigation systems can have potentially catastrophic impacts. Many electronic warfare-based counter-UAS techniques pose significant problems when used in busy electronic environments. In many situations, wholesale jamming of significant proportions of the electromagnetic spectrum is simply unacceptable to authorized users of the same spectrum. Poorly configured and inadequately maintained electronic countermeasure systems may also have adverse impacts on aircraft navigation and communications systems.

66 A.M. Holland, Counter-Drone Systems, 2nd ed. Alternate descriptions and terms may be used to describe counter-UAS processing chains (e.g., detect, track/locate, classify/identify, mitigate; detect, track, identify, defeat; sense, assess, detect, track, neutralize; find, fix, track, mitigate, defeat). See, for example, U.S. Department of Homeland Security, National Urban Security Technology Laboratory, Counter-Unmanned Aircraft Systems, 2019, pp. 14–15, [https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide\\_final\\_28feb2020.pdf](https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf).

#### Box 26. Key issues for consideration on counter-UAS systems and techniques

- Does the State have a designated national authority that is authorized and responsible for the coordination of assessment, testing and evaluation of counter-UAS technologies and equipment? Has the State developed metrics for evaluation and performance criteria?
- Are assessments and evaluations undertaken prior to, as well as after, the operationalization of authorized counter-UAS technologies and equipment (e.g., to evaluate how the counter-UAS technology and equipment interacts with a specific environment)?
- Does the State have a designated national authority that is authorized and responsible for the coordination of training of personnel on counter-UAS technologies, techniques, and equipment?
- Does the State have facilities and suitably trained and equipped individuals to conduct the training of counter-UAS technology managers and operators?
- How does the State evaluate incident response time?
- To what extent can the State develop its own counter-UAS system and equipment requirements and execute its own acquisitions (to rent, replace and/or procure more mature systems and equipment) to respond to changes in the UAS-related terrorist threat?
- To what level does the State cooperate and engage with the private sector and industry in the design and/or assessment and testing of specific counter-UAS technologies?
- Does the State have a designated national authority that is authorized and responsible for the evaluation of counter-UAS technologies, including electronic systems, to determine (or verify) their capability and utility in specifically identified contexts and locations?

Gun- and missile-based “hard kill” systems may have a role to play in defeating the terrorist use of UAS, but they must always be employed with great care and in line with the applicable domestic and international law, including international human rights and humanitarian law, mindful in particular of the risks posed to life and limb when UAVs or falling debris or ordnance fall to the ground. UAVs may be interdicted or destroyed using a variety of kinetic systems, such as gun and cannon systems and conventional air defence missile systems. However, it is important to take into account that all kinetic systems can potentially present significant risks of collateral damage, especially if deployed in populated areas (from, as noted before, falling debris, wayward ordnance, etc.). One of the most important challenges is maintaining effective airspace control measures and ensuring that non-target aircraft do not inadvertently enter gun or missile engagement zones. Therefore, gun and missile counter-UAS systems should only be used in conjunction with control measures based on carefully managed weapons control status and rigid rules of engagement. Any laxity in control measures may lead to the attack of non-target aircraft with catastrophic consequences. Fallout on residential property of debris associated with gun projectiles and missile debris may also cause significant safety issues.

States should designate a national authority authorized and responsible for the conduct of assessments and testing, training on, and evaluation of C-UAS technologies, including electronic systems, to determine (or verify, if undertaken in public-private cooperation) their capability and utility in specifically identified contexts and locations.

Initial or interim capabilities to counter small UAVs are likely to include a combination of fixed (or semi-fixed) systems, mounted or mobile systems, and dismounted hand-held systems. However, the maturity level of all these will have to be reviewed continually, and possible replacements made, as systems mature, or new systems become available.

## UAS incident scene: safety and security (3.2)

### Box 27. Key issues for consideration on UAS incident scene – safety and security

- How effective is the State in preparing and training first responders? How many first responders does the State train each year? Are first responders adequately equipped to deal with explosive and other hazards of retrievable or recoverable UAVs?
- Is there effective inter-agency cooperation between those entities responsible for responding to an incident involving UAS (i.e., first responders) and those responsible for the recovery and preservation of forensic (e.g., biometric) evidence?
- Has the State integrated UAS incident scene safety, security, and response into a specific crisis management strategy (or into a broader crisis management strategy)?
- To what extent are the counter-UAS systems, technologies, and procedures of relevant national authorities (e.g., military or law enforcement) interoperable?
- Are there examples of where the State has used information acquired from incident scenes in the successful prosecution of those using UAS?

When relevant national authorities encounter UAS on the ground – either through proactive intelligence-led operations, by interdiction using countermeasure systems, or because a system has crashed during operational use by terrorists – the priority is to ensure that any UAS components are safe to move and free from explosive and other hazards.

The determination that an item is safe and free from explosive hazards should be conducted by an appropriately trained explosive ordnance disposal operator or team, preferably with training in the safe handling of other UAS (and component) safety hazards, as terrorists have demonstrated the ability to hide IEDs inside UAVs with the express intention of targeting those involved in the recovery and subsequent forensic analysis of systems.

Among other safety hazards are those stemming from small UAV propellers (e.g., if they are still rotating) and batteries (e.g., damage or improper handling could cause injury or fire), which require special approaches and handling by the operator or examiner to ensure nobody is at risk of harm. It is recommended that the device is subsequently powered down.

UAVs that have been configured for intelligence, surveillance, and reconnaissance missions should then be relatively straightforward to examine, though radiographic equipment may be required to ensure that sealed compartments do not contain hidden IED components.

## Recovery and preservation of evidence (3.3)

### Box 28. Key issues for consideration on recovery and preservation of evidence

- To what extent does the State possess the fundamental core capabilities of recovery and preservation of: (i) physical evidence of UAS and components; (ii) biometric evidence of UAS and components; and (iii) digital evidence of UAS and components?
- If not domestically, does the State have access to fundamental core capabilities of recovery and preservation of digital evidence of UAS and components abroad (e.g., through established cooperation with international partners)?
- Is the continuity of evidence maintained from the point at which forensic evidence is collected to the point at which it may be required to support judicial proceedings?
- Does the State have access to good practice shared or being developed internationally for digital forensic exploitation and analysis of UAS and components?
- Does the State effectively integrate the various sources of information and intelligence open to it to identify all those involved in the actual operation of UAS, as well as those involved in procurement, development, and terrorist operations of UAS?

Control of incident scenes is paramount, and the collection of information as well as recovery and preservation of evidence critical.<sup>67</sup> The procedures for preservation and recovery of evidence from UAS components possibly or confirmed to have been used by terrorists have many similarities with those used for the preservation and recovery of evidence at IED scenes. Once recovered items are confirmed as safe and secured, it is recommended that before any technical analysis takes place, biometric evidence, such as fingerprints and DNA, is recovered and preserved.

Even if recovered UAS are not found with explosives, the recovery and preservation of evidence of a release mechanism can show that they have been modified to contain explosives. On commercially produced UAVs, analysis of manufacturer details and serial numbers may yield information that can help identify the source of supply of major components and thus contribute to future intelligence-led operations.

Larger UAVs that have been disrupted in flight or been subject to a crash landing may be badly fragmented, with widely dispersed evidence, which can be problematic. In such cases, the adoption of techniques like those applied in civil aircraft incident investigation may be more appropriate.

---

<sup>67</sup> See also, UN CTED, Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved, and shared by the military to prosecute terrorist offences, 2019. Criminal-justice actors need “information” and “evidence” to understand who was responsible for a crime, and when and how the crime occurred. Here, “information” can entail, among other things, physical objects, statements from witnesses and suspects, electronic and forensic information, and intelligence. Information used in legal proceedings is called evidence. The term “evidence” should be considered as information that complies with the legal rules of evidence and is used in judicial proceedings to prove or disprove an alleged crime.

## Technical exploitation of recovered UAS and components (3.4)

The technical exploitation of UAS and components requires specialist skills and capabilities, which are generally not present in most general-purpose forensic science laboratories and require the establishment or integration of a digital forensic capability.

At an initial stage, to assist in the technical exploitation of recovered UAS, States may enlist civilian experts from the domestic aerospace, electronic or other relevant sector or experts from national military research and development organizations, or States may contract and authorize independent civilian experts with the necessary expertise and specialist skills.

In further developing such a capability, a digital forensic laboratory may be contracted or established at an appropriate physically secured location or integrated within an existing forensic capability and sufficiently resourced. For such a laboratory to perform effectively, a clearly established case management procedure is required, and adequate staffing is needed (i.e., vetted and security-cleared, appropriately trained staff and experts). Generally, drone forensics is conducted along four phases: (data) acquisition, examination, analysis, and presentation.<sup>68</sup> It is essential that the chain of custody of the evidence is always maintained, and the integrity of the evidence secured along the process.<sup>69</sup>

---

68 Technical exploitation of recovered or retrieved UAS and components, including through drone forensics, considers a wide range of sources of evidence. Primary sources of evidence of small (commercial) UAS may typically include UAS (all physical components), the GCS, the counter-UAS system or technology, sensor(s), cloud storage (e.g., for streaming back via commercial service), and vendors.

69 See INTERPOL, *Global Guidelines for Digital Forensics Laboratories*, 2019.

### Box 29. Key issues for consideration on technical exploitation of recovered UAS and components

- To what extent does the State possess the fundamental core capabilities of technical exploitation and analysis of: (i) physical evidence of UAS and components; (ii) biometric evidence of UAS and components; and (iii) digital evidence of UAS and components?
- If not domestically, does the State have access to fundamental core capabilities of technical exploitation and analysis of these types of evidence of UAS and components abroad (e.g., through established cooperation with international partners)?
- Does the State have access to good practice shared or being developed internationally for digital forensic exploitation and analysis of UAS and components?
- Does the State effectively integrate the various sources of information and intelligence open to it to identify all those involved in the actual operation of UAS, as well as those involved in the procurement, development, and terrorist operation of UAS components?
- Does the State exchange information on good practices and techniques in relevant international forums with other States and international partners?
- Does the State use a technical profiling method (i.e., non-biometric) for the identification of individual signatures that are unique to a particular weaponized UAS “builder” or “maker” (or a group of such builders and makers trained by a specific individual)?

Generally, technical exploitation of recovered UAS and components includes the following three broad focus areas:

**Electronic systems associated with aircraft navigation and communications systems.** These may yield a plethora of useful information about where, when, and how the system was previously used, including the telemetry data, time, duration, and location of flights. Specialist techniques are likely required to access these cached data, which could be encrypted.

**Analysis of UAS communication systems.** This can provide critical information to inform the development of electronic countermeasure systems. This is because many commercially available UAS use commercial cellular communication systems, and the analysis of information recovered from subscriber identity modules may provide insights into the broader terrorist network behind those physically launching UAS and components, including weaponized UAVs.

**High-resolution imagery stored in non-volatile memory on board the UAV.** This may be accessed at the completion of the mission. Analysis of recovered imagery may yield valuable intelligence on how terrorists are employing UAS and the locations where the recovered UAV has been used before, and it may also provide means of visually identifying people involved in the launch, operation, or recovery of UAVs.

## Information management (3.5)

A robust and effective approach to information management (IM) underpins most effective national approaches to counter the threat posed by terrorists' use of weaponized UAS. IM should be understood as the process of collection, organization, storage, and provision of information within an organization.

Modern information systems and networked communications can improve the efficiency of information collection and dissemination across geographically dispersed entities, but they are not a panacea. Information overload can be a challenge. It is essential that where automated data, information, or intelligence collection systems are employed, law enforcement investigators and

### Box 30. Key issues for consideration on information management

- Does the State have a system in place for the relevant national authorities to be called on in cases of suspected or confirmed malicious, criminal, or terrorist use of UAS?
- Does the State have a system in place for the relevant national authorities to report incidents of suspected or confirmed malicious, criminal, or terrorist use of UAS?
- Does the State have a standardized format for the submission and transmission of incident reports of malicious, criminal, or terrorist use of UAS?
- Are such incident reports collated centrally by one national authority? Or are incident reports collated by several authorities at the national level? If so, is there a written procedure in place for inter-agency information or intelligence-sharing?

- Is information from such collated reports made available to regional and international partners (e.g., declassified key information, or parts thereof, where feasible)?
- Are incident reports of criminal or terrorist use of UAS permitted and used as evidence by the judicial system?
- Does the State have a common format for the submission and presentation of digital forensic reports?
- Is there a standardized method for the submission of physical exhibits collected from incidents of malicious, criminal, and terrorist use of UAS and components?
- Are forensic exhibits (e.g., fingerprints and DNA) and law enforcement interview reports collected from those arrested and subsequently prosecuted for UAS-related offences?
- Does the State make effective use of all-source intelligence reports pertaining to UAS incidents or individuals suspected of involvement in UAS-related criminal or terrorist offences?
- Does the State employ information systems to help in the storage, processing, and analysis of all-source intelligence?
- Do the State's information management (IM) processes permit the rapid and effective flow of UAS-related threat information and intelligence to those entities that need it, nationally?
- Do the State's IM processes permit the rapid and effective flow of UAS-related threat information and intelligence to regional and/or international partners (under established cooperative frameworks)?

intelligence analysts are provided with automated collation and analysis tools to process the ensuing of large volumes of information.<sup>70</sup>

A wide range of useful and pertinent information can be gleaned from UAS incidents to both support criminal investigations and aid in broader intelligence-led efforts to deny terrorists access to UAS and components.

IM is a critical enabler of several upstream measures required to prevent terrorists from gaining access to UAS and components. It also underpins domestic and international information-sharing and is the bedrock on which successful law enforcement intelligence led operations are developed. Most upstream and downstream measures to counter UAS and components, including counter-UAS technologies, rely on information and data. Information and data security must therefore be ensured.

---

70 See, for example, Global Counterterrorism Forum, Recommendations for Using and Protecting Intelligence Information in Rule of Law-Based, Criminal Justice Sector-Led Investigations and Prosecutions, <https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/2016%20and%20before/GCTF-Rabat-Good-Practice-6-Recommendations-ENG.pdf>. See also Global Counterterrorism Forum, The Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector (in particular, Good Practice 6, p. 7), <https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/2016%20and%20before/GCTF-Rabat-Memorandum-ENG.pdf>.

## Identification of perpetrators (3.6)

The identification of individuals and the broader network involved in the procurement, development, and operation of UAS, and components employed by terrorists may be achieved through a variety, and possibly a combination, of law enforcement investigative and intelligence techniques, applied in due cognizance of and in compliance with international human rights law and rule of law principles.

Those involved in the supply of systems and components may be identified through the identification and tracing of specific UAS and components.

They may be also identified through an analysis of a commercial UAS digital activation process (e.g., as many commercial UAS require activation by registration).

The analysis and use of biometric evidence (e.g., DNA and fingerprints) from UAS components recovered after operational use may support the identification of these individuals and the linking of individuals to other incidents.

Those involved in the operations of UAS (e.g., the “builders” or “makers”) may be identified through the analysis of imagery or communications data recovered and extracted from the non-volatile memory in the electronic systems of UAVs.

### Box 31. Key issues for consideration on identification of perpetrators

- To what extent does the State possess the fundamental core capabilities of recovery, preservation, and analysis of: (i) physical evidence of UAS and components; (ii) biometric evidence of UAS and components; and (iii) digital evidence of UAS and components?
- Are there successful examples of the State identifying perpetrators? If so, what have been the critical success factors?
- Does the State effectively integrate the various sources of information and intelligence available to it to identify those involved in the procurement, development, and terrorist operation of UAS?
- Does the State exchange information on good practices and techniques in relevant international forums with other States and international partners?
- Is a technical profiling method (i.e., non-biometric) used for the identification of individual signatures unique to a particular (including weaponized) UAS “builder” or “maker” (or a group of such builders and makers trained by a specific individual)?
- Does the State use geospatial or big data analysis techniques to develop intelligence to assist in the identification of those involved in terrorist operations and use of UAS?

Open-source intelligence, derived from open sources, such as social media accounts and published propaganda materials, may also yield considerable information to assist in the identification of perpetrators. Depending on the context, intelligence derived from information collected and provided by human sources, as well as the application of document cross-examination and extraction techniques, can also support such efforts. The exploitation of other types of intelligence, such as signals and electronic intelligence, may provide real-time information on where and how terrorists are employing UAS.<sup>71</sup>

In applying such law enforcement investigative and intelligence techniques, care must be taken to ensure that interferences with human rights, in particular the rights of persons who are not directly involved as perpetrators, are restricted only such as necessary and proportionate to legitimate aims (such as public order, public safety, or national security) pursued by a criminal investigation.

### Criminal justice process (3.7)

States should evaluate the effectiveness of their criminal justice system and processes to adequately address terrorist and criminal uses of UAS and components. In doing so, they should consider whether they have the requisite legislation to conduct human rights and rule of law-based investigations and prosecutions of those suspected of involvement in the misuse of UAS for terrorist purposes. While the terrorist use of weaponized UAVs is probably covered by most domestic legislation relating to the misuse of explosives, the use of UAS to underpin intelligence, surveillance, and reconnaissance may be more problematic, and – unless covered by material support law – specific legislation may be required.

---

71 Signal-based intelligence should be complemented with human intelligence and should not be the only source of intelligence.

#### Box 32. Key issues for consideration on criminal justice process

- Is there a track record and are there examples of successful prosecutions of individuals who have unlawfully used and weaponized unmanned aerial vehicles or of persons involved in the procurement, development, and operation of UAS and components for use in terrorist acts?
- Is there extant legislation allowing the prosecution of individuals illegally and criminally misusing UAS and components (e.g., through weaponization by explosives, use in attacks), and is this legislation fit for purpose?
- To what extent does the State criminal justice system permit the use of forensic biometric evidence in court in cases of suspected or alleged or confirmed malicious, criminal, or terrorist use of UAS and components?
- To what extent does the State criminal justice system permit the use of forensic digital evidence in court in cases of suspected or alleged or confirmed malicious, criminal, or terrorist use of UAS and components?

In addition to a forensic report, some jurisdictions require an expert testimony and expert witness (and expert status may be decided on a case-by-case basis by the judge or by appointment by the legal institution of an individual responsible for any case within this specific area of expertise) when prosecuting those suspected of involvement in the misuse of UAS. It is important that experts assuming such a role are proficient in the presentation of forensic evidence and the application of criteria for admissibility of electronic evidence in court<sup>72</sup> and that they are familiar with the respective legislation, the court procedures, and their rights and duties in such a role.

It may also be helpful to work with specific criminal justice actors to raise their awareness and strengthen their understanding of how terrorists employ UAS. While a detailed understanding of the technical aspects of UAS will not be required, making specific criminal justice actors aware of the principal means by which terrorists employ UAS may be useful, especially in contexts where the misuse of UAS by terrorists and criminals is recurrent.

### Development of UAS countermeasures (3.8)

The ability to respond to changes in the acquisition and use by terrorist groups of UAS and components is fundamental to an effective counter-UAS strategy and capability as it adapts, updates, and strengthens the national response in line with the threat faced. It is, in effect, a measure of the capacity of the State to implement a feedback loop – effectively implementing downstream measures and feeding back lessons learned into upstream measures – to learn, adapt, innovate, and respond appropriately and consistently over time.

---

72 Criteria for the admissibility of electronic evidence in court differ from one jurisdiction to another, but they generally include authenticity, completeness, reliability, convincingness, and proportionality. See INTERPOL, *Global Guidelines for Digital Forensics Laboratories*, 2019, p. 52.

#### Box 33. Key issues for consideration on further development of UAS countermeasures

- To what extent does the State systematically monitor the acquisition and use of UAS and components by terrorist groups? To what extent can it respond expeditiously and effectively to changes in respective terrorist groups' tactics, techniques, and procedures?
- To what extent can the State implement a feedback loop and, through generated results of the effective implementation of downstream measures, inform the strengthening of relevant upstream measures? How does the State adjust or further develop corresponding countermeasures and capabilities?
- How quickly is the State able to respond to changes in the use of UAS and components by terrorist groups and to adapt or acquire new capabilities, technologies, or equipment, and/or deliver updated training to detect and mitigate new UAS-related threats by terrorists?

## Submodule III

### **Technical guidance to facilitate the implementation of Security Council resolution 2370 (2017) in preventing terrorists from acquiring small arms and light weapons, and associated ammunition**

The rapid developments and evolution of UAS technology will continue to require adaptation of counter-UAS capabilities and technologies at an equally rapid pace, including to prevent their acquisition and mitigate their use by terrorist groups. As regards counter-UAS technologies, improvements to robust (non-hackable and/or non-jammable) communication systems as well as improvements to propulsion and power components (resulting in better speed, agility, and endurance) are worth noting. Continuous horizon scanning of existing or emerging and related threats posed by terrorist use of UAS and components, as well as other uncrewed systems including uncrewed vehicles,<sup>73</sup> is critical. Horizon scanning should include the possible diffusion of technology, adaptations of technologies and systems by terrorist groups through their own means, as well as risks posed by the proliferation, potential acquisition and use by terrorist groups of larger categories of UAS and components. Further, among the broad technological developments that are key are (in a non-exclusive manner and listed in no specific order) miniaturization, swarming, artificial intelligence, and autonomous systems, and robotics.

Changes in tactics, techniques, and procedures employed by terrorists to acquire and use UAS and components, as well as changes in acquired UAS and components in use by terrorists, need to be brought to the attention of the relevant State authorities, security forces and other agencies. Counter-UAS strategies, as well as counter-UAS capabilities including technologies and equipment, must then be revised (and, if need be, adapted) continually; capacity-building strategies and activities must then also be adapted and updated accordingly.

---

<sup>73</sup> Other categories may include larger (than small-sized) UAS and components, which have already been observed in use by non-State armed groups in specific countries and in specific subregions and regions. There are risks that larger UAS and components or technologies may be diverted and proliferate respectively diffuse to terrorist groups. Other unmanned vehicles may include unmanned ground vehicles, such as remote-controlled vehicles, or unmanned marine vehicles, either on underwater or surface platforms.

# Introduction

---

The acquisition and use of small arms and light weapons (SALW), and ammunition by terrorists continues to pose an international threat and challenge to peace and security.<sup>74</sup> Globally, SALW continue to be the weapons of choice for terrorists.<sup>75</sup> The United Nations General Assembly has recognized “the urgent need to maintain and enhance national controls ... to prevent, combat and eradicate the illicit trade in small arms and light weapons, including their diversion to illicit trade [and to] terrorists”.<sup>76</sup>

The ways and means through which terrorists acquire SALW are often complex, multifaceted, and dynamic. Trends are also context specific, varying between subregions and regions and between conflict and non-conflict settings. In non-conflict contexts, dynamics appear to be largely influenced by access to illegal markets and the crime–terror nexus.<sup>77</sup> In conflict-affected settings, battlefield captures, loss of material from national holdings, poor stockpile management or, more broadly, absent, or weak State authority, among other factors, help facilitate terrorist acquisition of SALW, and ammunition, for use in terrorist acts.

It is generally recognized that international instruments to prevent, combat and eradicate the illicit trade in SALW in all its aspects provide for and contain effective measures that can be implemented at each stage in the life cycle of SALW, and ammunition, to prevent their diversion to illicit trade and to unauthorized end users, including to terrorist groups and individuals. Resolution 2730 calls upon Member States to “consider becoming a party to the related international and regional instruments, with a view

---

74 See General Assembly, A/RES/75/241, 2021, p. 3, para. 2, <https://undocs.org/A/RES/75/241>.

75 See, for example, Global Terrorism Database, University of Maryland, <https://www.start.umd.edu/gtd> (last accessed 29 September 2021).

76 General Assembly, A/RES/75/241, 2021, p. 3, para. 2, <https://undocs.org/A/RES/75/241>.

77 See, for example, Wilton Park, The Nexus between SALW, Organized Crime, and Terrorism, 2019, <https://www.wiltonpark.org.uk/wp-content/uploads/2020/09/WP1671-Report.pdf>; see also, Triggering Terror Illicit Gun Markets and Firearms Acquisition of Terrorist Networks in Europe, Flemish Peace Institute, Brussels, 17 April 2018.

## Box 34. International instruments (SALW control)

- The United Nations Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects (adopted in 2001; politically binding)
- The International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons (adopted in 2005; politically binding)
- The Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition (entry into force in 2005; legally binding for States Parties)
- The Arms Trade Treaty (entry into force 2014; legally binding for its States Parties)

to help eliminate the supply of weapons to terrorists, and to fully implement their respective obligations under those to which they are a party".<sup>78</sup> International SALW control instruments are listed in Box 34.<sup>79 80</sup>

As noted in the general introduction of this document, this submodule constitutes a first attempt at the international level to draw from these instruments, existing good practices, and international standards to work towards the development of technical guidance dedicated to facilitating the implementation of relevant provisions of resolution 2370.

States and users of this submodule can refer to and are encouraged to use existing, comprehensive international technical guidance contained within the United Nations Modular Small-arms-control Implementation Compendium (MOSAIC) and the UN SaferGuard International Ammunition Technical Guidelines (IATGs),<sup>81</sup> related guidance, as well as technical guidance contained in sub-/regional good practice guidelines and standards.

A thorough understanding of the context and of the system through which a specific terrorist group acquires SALW, and their ammunition, and the possible links with other systems through which other types of weapons and components are acquired,<sup>82</sup> is a prerequisite for developing and implementing effective preventative and preparedness and response measures.

## Terminology (1.1)

For the purposes of this submodule, the following description of SALW is used and applied:

Any [human]-portable lethal weapon that expels or launches, is designed to expel, or launch, or may be readily converted to expel or launch a shot, bullet, or projectile by the action of an explosive, excluding antique SALW or their replicas.<sup>83</sup>

---

78 See Security Council, S/RES/2370 (2017), p. 3, para. 1, <http://unscr.com/en/resolutions/doc/2370>

79 In the outcome document to the third UN Conference to Review Progress Made in the Implementation of the PoA (A/CONF.192/2018/RC/3, annex), Member States declared their particular concern about the use of SALW in terrorist attacks and underlined the essential contribution made through the full and effective implementation of the UN PoA and the ITI to the global fight against all forms of violence and crime, including terrorism, and in that regard resolved to strengthen their implementation and coordination efforts.

80 While not explicitly referenced in resolution 2370, arms control elements of the Arms Trade Treaty (ATT) are relevant to preventing terrorists from acquiring weapons. The ATT is a global, legally binding instrument for its State Parties to regulate the trade in conventional arms, including SALW, and underlines "the need to prevent and eradicate the illicit trade in conventional arms and to prevent their diversion to the illicit market, or for unauthorized end use and end users, including in the commission of terrorist acts". ATT article 7 requires, if an export is not prohibited under Article 6 of the Treaty, for States Parties "prior to authorizing the export of conventional arms, including SALW, assess the potential that the conventional arms or items: ... could be used to ... commit or facilitate an act constituting an offence under international conventions or protocols relating to terrorism to which the exporting State is a Party" (article 7, 1. b) iii), <https://thearmstradetreaty.org/treaty-text.html?templateId=209884>

81 See Modular Small-Arms-Control Implementation Compendium, <https://www.un.org/disarmament/convarms/mosaic/#:~:text=MOSAIC%20is%20the%20result%20of%20a%20decade%20of,the%20world%20to%20improve%20their%20small-arms%20control%20measures;see%20UN%20SaferGuard,International%20Ammunition%20Technical%20Guidelines,https://unsafeguard.org/>.

82 Including those described in Submodules I and II of this document.

83 General Assembly, International Tracing Instrument, 2005, para. 4. The Firearms Protocol similarly and legally defines a firearm as "any portable barrelled weapon that expels, is designed to expel or may be readily converted to expel a shot, bullet or projectile by the action of an explosive, excluding antique firearms or their replicas [manufactured before 1899]." Regional instruments provide descriptions and legal definitions comparable to the description used in this sub-module.

A “small arm” is described as any human-portable weapon designed for individual use. Small arms include revolvers and pistols, rifles and carbines, submachine guns, assault rifles, and light machine guns, as well as their parts, components.

A “light weapon” is described as any human-portable weapon designed for use by two or three persons serving as a crew.<sup>84</sup> Light weapons include heavy machine guns, hand-held under-barrel and mounted grenade launchers, portable anti-tank and anti-aircraft guns, recoilless rifles, portable launchers of anti-tank and anti-aircraft missile systems, and mortars of less than 100 mm, as well as their parts, components.<sup>85</sup>

For the purposes of this document, the term “small arms and light weapons” (SALW) is considered, used, and applied to cover and include “small arms”, “firearms”, “light weapons”, their parts and components, as well as ammunition corresponding to these SALW, except where noted and where the context indicates otherwise.

This submodule does not include a comprehensive list of small arms, firearms, light weapons, parts, components and ammunition definitions and terms, which are available in international (and regional/sub-regional) instruments, standards, and technical guidelines.<sup>86</sup>

## Objective of this submodule (1.2)

The primary objective of this submodule is to provide technical guidance to State officials, as well as other relevant and interested stakeholders, to facilitate the implementation of resolution 2370. In particular, this submodule aims to provide technical guidance to enable effective implementation of preventative and response measures to terrorist acquisition and use of SALW and ammunition.

The document is designed to facilitate self-assessment by States in their efforts to (i) develop, refine, and implement technical measures to prevent terrorists from acquiring SALW and (ii) prepare against and respond to incidents at the national level. The document may also be used by relevant United Nations and other specialized entities to support States in such efforts, including to support national assessments and in facilitation of technical assistance to States. The document represents one of several means and methods available to support States and the technical community of practice in preventing terrorists from acquiring SALW and ammunition.

---

84 Some “light weapons” may be carried and used by a single person.

85 See General Assembly, Report of the Panel of Governmental Experts on Small Arms, A/52/298, 1997, paras 25–27; General Assembly, International Tracing Instrument, 2005, para. 4; Modular Small-arms-control Implementation Compendium, Glossary of Terms, Definitions and Abbreviations, MOSAIC 01.20, Version 1.5, 2018 (in particular, pp. 17 and 23).

86 A comprehensive list of terms and definitions applicable to SALW is available in the Modular Small-arms-control Implementation Compendium, Glossary of Terms, Definitions and Abbreviations, MOSAIC 01.20, Version 1.5, 2018, available at [www.un.org/disarmament/convarms/mosaic](http://www.un.org/disarmament/convarms/mosaic). A comprehensive list of terms and definitions applicable to SALW ammunition is available in the International Ammunition Technical Guidelines (IATG 01.40, Glossary of terms, definitions and abbreviations), available at [www.un.org/disarmament/ammunition](http://www.un.org/disarmament/ammunition).

## Methodological approach (1.3)

The methodological approach applied in this submodule draws on a capability maturity model (CMM). CMMs have been widely adopted by institutions, administrations, and organizations, including by the United Nations, as they provide a disciplined framework to systematically assess the maturity of processes and practices, to identify gaps and areas for improvement, and to achieve progress in complex domains.<sup>87</sup> A CMM can be considered a set of structured levels, describing how States can reliably and sustainably produce desired outcomes to prevent terrorists from acquiring SALW and ammunition. As a guiding reference, capability maturity levels may range as follows:

**Initial:** processes are characterized as ad hoc and, occasionally, even chaotic. Few processes are defined, and success depends on individual effort.

**Repeatable:** basic management processes are established, and the necessary process discipline is in place to repeat earlier successes on projects with similar applications.

**Defined:** processes are documented, standardized, and integrated into the organization's overall processes.

**Managed:** detailed measures of processes and product quality are collected, and the products and processes are quantitatively understood and controlled.

**Optimizing:** continual process improvement is enabled by quantitative feedback from the processes and from piloting innovative ideas and technologies.

These capability maturity levels, and their descriptions are guiding in nature. They may serve as a useful reference for users of this document when assessing the maturity of the national and/or organizational measures in place to prevent terrorists from acquiring SALW and ammunition.<sup>88</sup>

## Structure of this submodule (1.4)

This submodule is divided into two subcategories: (i) upstream measures (section 2), focused on those activities aimed at preventing terrorists from acquiring SALW and ammunition, and (ii) downstream measures (section 3), associated with the response to a particular terrorist event or incident involving illegal and/or illicit SALW and ammunition. The general premise of the CMM, which underpins this submodule, is that the greater the maturity and effective implementation by a State of upstream measures, the fewer downstream measures will be required.

Under each upstream and downstream measure covered by this submodule, a set of key issues for consideration is provided, in the form of guiding questions, which can help users assess national and/or organizational processes and measures aimed at preventing terrorists from acquiring SALW and ammunition.

---

87 B. Seddon and A. Malaret Baldo, Counter-IED Capability Maturity Model & Self-Assessment Tool, UNIDIR, 2020 (in particular, pp. 10–15).

88 For a full and comprehensive assessment, refer to and use the Counter-IED Capability Maturity Model & Self-Assessment Tool, 2020, currently available in English, French, and Spanish: <https://unidir.org/publication/counter-ied-capability-maturity-model-and-self-assessment-tool>

## Respecting human rights, fundamental freedoms, international humanitarian law, and gender- and age-related implications (1.5)

States must ensure that any measures taken to prevent and mitigate terrorist acquisition and use of SALW and ammunition comply with all their obligations under domestic and international law, in particular international human rights law, international humanitarian law, and international refugee law.

Comprehensive approaches should also take into account gender and age sensitivities, including that the human rights consequences of arms transfers on women and girls may be disproportionate and that the widespread availability of SALW increases the risk of sexual and gender-based violence,<sup>89</sup> as well as the differential impact of terrorism on the human rights of women and girls.<sup>90</sup> The need for “robust and effective regulation of the arms trade, in addition to appropriate control over the circulation of existing and often illicit ... arms, including small arms” in order to address their misuse in conflict-related gender-based violence and domestic violence has repeatedly been stressed.<sup>91</sup>

Respect for human rights, fundamental freedoms, and the rule of law are complementary and mutually reinforcing with effective measures to counter terrorist acquisition and use of SALW and constitute an essential element of such efforts. All upstream and downstream measures described in this submodule are to be considered, used, and applied in full respect of international law, including international human rights law, international humanitarian law, and international refugee law.<sup>92</sup> As such, these measures must duly consider the impact on and be responsive to the needs of groups and persons who may be marginalized or discriminated against, including women, members of ethnic, racial, religious, and other minorities as well as persons in vulnerable situations, such as those forcibly displaced or otherwise affected by armed conflict and other types of violence.

Globally, SALW is the category of weapons most implicated in human rights violations and abuses, including gender-based violence.<sup>93</sup> SALW and ammunition are also often used by terrorists to facilitate the commission of abuses and human rights violations against marginalized groups and persons such as ethnic, racial, religious, and other minorities as well as persons in vulnerable situations. Terrorists directly target women and girls, employing SALW in gender-based violence and related coercive acts to dehumanize religious and ethnic minorities, notably through the perpetration of rape, sexual

---

89 A/HRC/RES/32/12, para. 2. See also A/HRC/RES/41/20.

90 S/RES/2242 (2015)

91 See General recommendation No. 30 on women in conflict prevention, conflict and post-conflict situations, Committee on the Elimination of Discrimination against Women, Convention on the Elimination of All Forms of Discrimination Against Women, CEDAW/C/GC/30, 2013, p. 25.

92 In this sense the Draft Principles on the prevention of human rights violations committed with small arms, elaborated by the Special Rapporteur on the prevention of human rights violations committed with SALW may provide useful guidance. See A/HRC/Sub.1/58/27/Add.1.

93 See Human Rights Council, Impact of Arms Transfers on Human Rights, Report of the United Nations High Commissioner for Human Rights, A/HRC/44/29, 2020.

slavery, and forced marriage.<sup>94</sup> The gendered and age-related impacts, as well as the specific risks and vulnerabilities associated with the misuse of SALW by terrorists, are to be duly taken into account by all users of this submodule.<sup>95</sup>

## Countering terrorist acquisition of SALW and ammunition: Upstream measures

---

### National policy, legislation, regulation, and administrative procedures (2.1)

#### 1. National policy or strategy (2.1.1)

---

As part of their national security policy framework, many States already have separate national policies or strategies to address the illicit proliferation of SALW, weapons and ammunition management (WAM), counter-terrorism, and the prevention and response to violent extremism. In such cases, it is advisable that these documents provide national coherence regarding the prevention of terrorist acquisition of SALW and ammunition.

Furthermore, in such cases, it will in most cases not be deemed necessary to prepare a national strategy or policy solely to address terrorist acquisition of SALW and ammunition. It is recommended that the national security policy framework provides the strategic outlook on this issue, based on a comprehensive assessment and analysis of the context and SALW-related, and possibly broader weapons-related, terrorist threats, risks and impacts faced by the State both domestically and internationally (see section 2.7).

The appropriate national strategic policy approach will inform the designation of a lead national coordinating entity and effective institutional architecture. A designated national lead entity<sup>96</sup> at the strategic level within the government's national security architecture should be responsible for overall political coordination and policy direction on preventing terrorist acquisition of SALW and ammunition. It is for each State to decide on the designation of an existing entity or establish a new arrangement for such a national lead entity (e.g., with responsibilities for national security or interior or internal affairs).

It is important that this lead entity has oversight of an existing national commission or coordinating body on SALW control or WAM, and agencies and coordinating mechanisms for counter-terrorism. The

---

94 Human Rights Council, A/HRC/44/29, 2020.

95 See Modular Small-Arms-Control Implementation Compendium, Women, Men and the Gendered Nature Of Small Arms and Light Weapons, MOSAIC 06.10, <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/MOSAIC-06.10-2017EV1.0.pdf>; Modular Small-Arms-Control Implementation Compendium, Children, Adolescents, Youth and Small Arms and Light Weapons, MOSAIC 06.20, <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/MOSAIC-06.20-2018EV1.0.pdf>.

96 This is sometimes also referred to as the "national lead authority".

### Box 35. Key issues for consideration on national policy or strategy

- Has the State undertaken a systematic assessment and analysis of the nature and dynamics of SALW-related terrorist threats, risks and impacts across its territory?
- Has the State designated a national entity that is sufficiently empowered and resourced and has capacity to provide political coordination and policy direction on all matters related to the prevention of terrorists from acquiring SALW and ammunition?
- Under which national strategic and policy frameworks does the State consider the prevention and mitigation of SALW-related terrorist risks and threats and define its objectives and priorities in terms of capabilities and measures to counter them? For example, does a national policy or strategy for SALW control, WAM, or counter-terrorism that takes into account such threats and risks? Are such threats and risks considered, for example, as part of a national action plan or other strategic or policy framework on these issues? Are SALW control, WAM, and counter-terrorism strategic or policy frameworks connected?
- Does the State have a mechanism in place to ensure that relevant national policies or strategies are regularly reviewed through an inclusive, participatory, and multi-stakeholder process and subsequently updated? Does this process include the actors designing and developing, as well as the actors implementing, the policy or strategy?

commission or coordinating body needs to be sufficiently empowered, resourced and authorized to ensure the necessary coordination, including information and SALW and firearms-related intelligence-sharing through appropriate national mechanisms (see section 2.1.2), as well as international cooperation (see section 2.2).

### Box 36. Key issues for consideration on national coordinating entity and coordination mechanisms

- Are there effective cooperation mechanisms, duly mandated and sufficiently resourced, to coordinate both at the strategic or policy level and the operational or tactical level measures to prevent, prepare against, mitigate, and respond to terrorist acquisition and use of SALW? To what extent do such mechanisms cover the national, subnational, and local levels?
- Are inter-agency cooperation arrangements and coordination mechanisms at the strategic or policy level ad hoc or formalized (e.g., through a written procedure)?
- Are inter-agency cooperation arrangements and coordination mechanisms at the operational or tactical level ad hoc or formalized (e.g., through a written procedure)?

The implementation of downstream measures described in this submodule can generally be strengthened through a defined, cohesive and effective national approach for the systematic and complete processing of SALW, and treatment of ammunition, and related items and material recovered



from the illicit and/or illegal sphere, including from terrorist groups and individuals (from initial recovery to registration, technical exploitation, analysis, tracing, investigations, judicial processing, and disposal including destruction).<sup>97</sup>

## 2. National coordinating entity and coordination mechanisms (2.1.2)

---

At the strategic level, the coordination of all measures to prevent, prepare against, mitigate, and respond to terrorist acquisition and use of SALW and ammunition should be overseen and coordinated by the appropriate national lead entity (see section 2.1.1).

---

<sup>97</sup> Such a national approach should be broad in scope and include recoveries not only from terrorist groups and individuals but also from criminals, pirates, non-State armed groups, and other illicit and/or illegal or unauthorized actors and individuals. The term “recovery” is used throughout this document and understood to include SALW and ammunition seizures and/or confiscations (e.g. by law enforcement, border and customs agencies, security and defense forces, or other services); captures (e.g. in the military, including military counter-terrorism operations by national and/or international security forces); recovered caches (from suspected or confirmed terrorist groups or associated groups and individuals); and surrenders respectively collections (i.e. from illegal non-State armed groups and elements known or suspected to have links to a terrorist group).

Strong national coordination through the establishment of clearly defined, robust coordination mechanisms, including information-sharing mechanisms, is essential and needed for, as well as applicable to, effective implementation of the upstream and downstream measures described in this submodule. Specific coordination mechanisms, including specific information-sharing mechanisms, at the operational level may be required to implement specific upstream or downstream measures.

It is a decision for individual States, depending on the context and based on the threat and risk analysis, to decide whether using an existing national coordination mechanism (e.g., on SALW control, WAM or counter-terrorism) is appropriate and adequate for the task, or if a special committee (e.g., at the strategic level) and/or a task force, technical working group, or similar entity (e.g., at the operational level) is required. In making this decision, it is critical to recognize that measures described in this submodule require close cooperation and coordination between law enforcement, intelligence and specialist military agencies, border and customs agencies, and others. Robust and reliable processes must be established to allow the flow of information and intelligence between those entities that need it.

### 3. National legislation and regulations (2.1.3)

---

Relevant international SALW control instruments oblige or call on States to put in place adequate national legislation and regulations to regulate and control the full life cycle of SALW, including their manufacture or production, transfers (including export, import, transit, trans-shipment, re-export and brokering), stockpiling, (end) use and final disposal including destruction (or deactivation), to prevent

#### Box 37. Key issues for consideration on national legislation and regulations

- Are the obligations pursuant to international SALW control instruments, and counter-terrorism instruments, as well as policy commitments under relevant instruments, incorporated into national legislation and regulations?
- To what extent does the national legislative and regulatory framework applicable to SALW, and ammunition, adequately cover their full life cycle (e.g., from manufacture, transfers, stockpiling, (end) use and final disposal including destruction or deactivation)?
- To what extent does the national legislative and regulatory framework include mandatory and additional enforcement and criminalization provisions, in line with the applicable international law, including arms control and counter-terrorism instruments?
- Are there adequate and suitable enforcement and oversight mechanisms to address violations of relevant legislation and regulations? Do they exist for legislation and regulations applicable to State-owned SALW and ammunition? Do they exist for legislation and regulations applicable to firearms and ammunition acquired and held by licensed and authorized civilians and civilian entities?

diversion and access by unauthorized end users, including terrorists. Terrorist groups and individuals may actively exploit gaps in national legislation and regulations.

National legislation and regulations should contain criminalization and enforcement provisions to ensure that law enforcement and judicial measures at the national level can be effective in pursuing terrorists and associated individuals seeking to acquire and use SALW and ammunition. It is equally important that national legislation or regulations contain provisions for international cooperation and mutual legal assistance, in particular to enable the bilateral and multilateral sharing of information relating to several measures described below (e.g., for weapon tracing and for investigations that have an international dimension, as discussed in sections 2.2, 3.5 and 3.6).

Another key consideration for the regulatory framework is the definition and categorization of SALW, parts and components, and ammunition. This includes clearly defining items that are only permitted for possession by government authorities, and those that can be possessed by non-State entities. It is also important for States to have a national control list in place that defines the items to be subject to transfer controls (see section 2.4).

When evaluating and reviewing the scope, application, and effectiveness of national legislation and regulations, it is important that national regulatory authorities take into account existing or emerging risks and threats related to terrorist acquisition of SALW, parts and components, and ammunition. Depending on the context this might include, for example, the conversion and reactivation of deactivated firearms, sharing of knowledge or acquisitions through or facilitated by the use of social media online platforms, or the darknet, as well as 3D printing and manufacturing of SALW, parts and components.

Evaluating the scope, application, and effectiveness of national legislation and regulations to counter terrorist acquisition of SALW, and ammunition, in line with the obligations and requirements of international legally binding instruments requires:

- Undertaking periodic and inclusive national legislative review processes;
- Updating relevant national legislation and regulations, including national administrative procedures and technical standards; and
- Undertaking continual awareness-raising among all relevant national actors, including State and non-State entities, of the applicable international legally binding instruments, policy commitments under relevant instruments, and relevant international standards.

#### **4. National administrative procedures and technical standards (2.1.4)**

---

The review, development, and adoption of administrative procedures and national technical standards, which clearly define the respective authorities, roles, and responsibilities of relevant national authorities, provide an important means for States to standardize practices and procedures to ensure an effective and cohesive national approach. In reviewing, developing, and adopting their own administrative procedures and technical standards, States can draw from existing technical guidance developed by and

### Box 38. Key issues for consideration on national administrative procedures and technical standards

- To what extent does the State, and its relevant national authorities, possess the necessary technical capacity and expertise to review, codify, and develop national administrative procedures and technical standards? Does the State have access to external technical expertise for the review, codification and development of technical standards or operating procedures?
- Does the State have access to and use available international standards, technical and good practice guidelines developed internationally, subregionally, or regionally?
- Do relevant national authorities document good practices and lessons learned in addressing and preventing existing or emerging SALW-related terrorist acquisition threats or risks? Does the State share and exchange these practices and lessons with international stakeholders and partners in relevant international forums?

within the United Nations,<sup>98</sup> other international organizations, subregional and regional organizations, and expert non-governmental organizations. Technical guidance developed by subregional and regional organizations may be particularly useful when addressing subregional and regional context-specific terrorist risks and threats.

Areas of upstream and downstream measures described in this submodule where administrative procedures and technical standards are particularly relevant include:

- Regulation of the manufacture of SALW (e.g., licensing procedures);
- Regulation of civilian access to small arms (e.g., licensing procedures);
- Transfer controls (e.g., procedures for transfer control risk assessment);
- Stockpile management (e.g., procedures for management and security of stocks);
- Marking, record-keeping, profiling, and tracing;
- Processing of recovered SALW and the treatment of recovered ammunition;
- Information-sharing (e.g., domestic, and international sharing and exchange of information); and
- Disposal (e.g., procedures for destruction and deactivation).

## Cooperation, including information-sharing (2.2)

International and subregional or regional cooperation, including information-sharing, is crucial because terrorist groups generally do not recognize international borders. SALW and ammunition may be sourced in one country for misuse in another. Therefore, many measures described in this submodule rely to a greater or lesser extent on effective international cooperation, including the sharing or exchange of information.

---

98 As noted above, States can refer to and are encouraged to use existing comprehensive guidance contained within MOSAIC, the UN SaferGuard's International Ammunition Technical Guidelines, and related guidance.

### Box 39. Key issues for consideration on cooperation, including information-sharing

- To what extent does the State recognize that terrorist SALW acquisition is a transnational problem and requires cooperation as well as coordinated international efforts?
- Is the State prepared to cooperate and share information with other States, relevant regional and international organizations, and other entities to prevent and counter terrorist acquisition of SALW and associated ammunition? Are appropriate and adequately resourced entities in place?
- To what extent does the State participate in relevant cooperative frameworks that allow for cooperation between States in the area of tracing of SALW and ammunition?
- Does the State actively participate in relevant international forums and exchange lessons learned and good practices in preventing terrorist acquisition of SALW? Does the exchange of such lessons learned include good practices to address emerging trends and threats?

Given the often transnational nature of SALW-related terrorist threats, risks, and impacts, it is important to have relevant national focal points to facilitate active cooperation and engagement with relevant United Nations entities (see section 2.1.2), as well as bilaterally with other States and with international and subregional or regional organizations. As noted above, designating an authorized national focal point or focal points (see section 2.1.2), and making their contact details known to relevant partners is an important first step in ensuring effective international communication. The focal point needs an appropriate mandate for internal and external cooperation and information-sharing, as well as sufficient resources and capacity to effectively coordinate international cooperation, including the sharing or exchange of information. Cooperation is also encouraged with the private sector and civil society.

### Regulation and control of manufacture (2.3)

While most SALW and ammunition that end up in terrorist hands have originally been legally, industrially manufactured, terrorists may also seek to access and acquire “craft-produced” SALW, converted and reactivated weapons, or 3D printing technology or 3D-printed SALW. Different context-specific national approaches and measures exist and are applied by States to regulate and address these forms of illicit manufacture.

For example, national regulatory authorities, in cooperation with private sector industry, should consider introducing regulations that require companies that produce 3D printing technology to adopt certain technical limits and to consider regulating blueprints required for 3D printing of SALW. The illicit possession, uploading and downloading of such blueprints, as well as illicit printing, should then be criminalized and prosecuted.<sup>99</sup>

---

99 Conference of the Parties to the United Nations Convention against Transnational Organized Crime, Investigative and Prosecutorial Approaches in Countering Illicit Firearms Trafficking and Related Forms of Crime within and across Jurisdictions, CTOC/COP/WG.6.2020, 2020.

#### Box 40. Key issues for consideration on regulation and control of manufacture

- Does the State employ measures to stop terrorists exploiting information and communications technology, including darknet markets, to prevent and counter acquisitions through or facilitated by the darknet? If so, can good practices be shared?
- Does the State employ measures to prevent terrorists from using information and communications technology tools to print 3D SALW, parts and components? If so, can good practices be shared?
- Does the State employ measures to prevent SALW craft production, conversion, and reactivation of deactivated SALW, ammunition, parts, and components? If so, can good practices be shared?

As indicated above, these issues should be considered by national legislative authorities when evaluating and reviewing the scope, application, and effectiveness of national legislation and regulations (see section 2.1.3). Accordingly, the relevant national authorities should then develop, implement, and enforce the appropriate countermeasures.

### Transfer controls, including export, import, brokering, transit, or retransfer (2.4)

The 2018 addendum to the Madrid Guiding Principles called on Member States to undertake “all appropriate measures to prevent the diversion of [SALW and ammunition] when authorizing their international transfer”.<sup>100</sup> There is a large body of international guidance on establishing and maintaining a national transfer control system to control and regulate the export, import, transit or trans-shipment, brokering, and re-export of SALW and ammunition to prevent, combat, and eradicate diversion and the illicit arms trade. Section 2.1 introduced the need for a national legal framework to regulate international transfers. Therefore, this section focuses on appropriate measures to be taken at the pre-shipment stage in the transfer chain to prevent an international transfer being diverted to terrorists.

An effective national transfer control system is critical in preventing the diversion of an authorised transfer, or an illicit international transfer, of SALW and ammunition to terrorists. It is recommended that a competent national authority undertakes a robust and comprehensive risk assessment before deciding whether to authorize or refuse the import, export, transit, or trans-shipment, brokering, or re-export of SALW and ammunition. If the risk assessment determines there is a significant risk that a potential international transfer of SALW and ammunition could be used to commit or facilitate an act constituting an offence under international conventions or protocols relating to terrorism, or could be diverted for such use, competent national authorities should not authorize the transfer.<sup>101</sup>

---

<sup>100</sup> Security Council, S/2018/1177, 2018 (Guiding Principle 52, p. 28).

<sup>101</sup> Modular Small-arms-control Implementation Compendium, National Controls over the International Transfer of Small Arms and Light Weapons, MOSAIC Module 03.20, 2014.

One approach that some States use to minimize the risk of SALW diversion to terrorists is to only authorize transfers to States or to entities explicitly authorized to act on their behalf. Such an approach still requires an assessment of the risk of diversion before deciding whether to authorize or deny the proposed transfer. Another related option is to restrict the types of SALW and ammunition that can be delivered to or transferred with the involvement of non-State actors. For example, many States adopt stricter transfer controls for international transfers of man-portable air defence systems (MANPADS) and other types of shoulder-fired guided missiles than for other types of SALW, agreeing to prohibit their transfer to non-State actors.<sup>102</sup>

---

102 See Wassenaar Arrangement, Elements for Export Controls of Man Portable Air Defence Systems, 2007, para. 3.1; Organization for Security and Co-operation in Europe, Principles for Export Controls of MANPADS (Updated), 2008; Asia–Pacific Economic Cooperation, Guidelines on Controls and Security of Man-portable Air Defense Systems (MANPADS), 2004; Organization of American States, Guidelines on Controls And Security Of Man-Portable Air Defense Systems (MANPADS), 2005; and International Civil Aviation Organization, Resolution A36-19, 2007, para. 5, which “urges all Contracting States to apply the principles defined in the Elements for Export Controls of MANPADS of the Wassenaar Arrangement”.

#### Box 41. UN Security Council 1267 Sanctions regime and arms embargo

The United Nations Security Council 1267 sanctions regime and arms embargo requires all States “to prevent the direct or indirect supply, sale and transfer from their territories or by their nationals outside their territories ... or using their flag vessels or aircraft, of arms and related materiel of all types, spare parts, and technical advice, assistance, or training related to military activities, to designated individuals and entities”. There are no exemptions to the arms embargo and its measures, which must be applied by all States with respect to ISIL (Da’esh), Al-Qaida and other individuals, groups, undertakings, and entities associated with them, as designated on the ISIL (Da’esh) and Al-Qaida Sanctions List. Acts or activities indicating that an individual, group, undertaking or entity is associated with ISIL (Da’esh) and Al-Qaida include “... supplying, selling, or transferring arms and related material to ... ISIL (Da’esh), Al-Qaida or any cell, affiliate, splinter group or derivative thereof”.

The basic elements of a risk assessment for the diversion of SALW should consider the predictability and reliability of the importing State, the ultimate end user and the other actors involved in the transfer. Such a risk assessment will examine the parties to the transfer with regard to their record of diversion or direct supply to terrorists, as well as the attractiveness to criminal or terrorist organizations of the SALW and ammunition to be transferred.<sup>103</sup> A variety of government ministries, departments and agencies (i.e. customs, law enforcement, justice, intelligence, financial intelligence units, and defence and trade ministries) provide information for such national diversion risk assessments and decision-making processes. The risk assessment should draw on information generated through the national implementation of downstream measures described in section 3 (see, for example, section 3.6), participation in information-sharing and international cooperation mechanisms, as well as open-

---

103 B. Wood and P. Holtom, The Arms Trade Treaty: Measures to Prevent, Detect, Address and Eradicate the Diversion of Conventional Arms, ATT Issues Brief 2, UNIDIR, 2020, p. 17 (more information on pp. 16–22).

source information, including the reports of the 1267 Committee's Analytical Support and Sanctions Monitoring Team (see box 41).<sup>104</sup>

The documentation provided in support of an application for an authorization to undertake an international transfer is a particularly important source of information, particularly end use/r documentation.<sup>105</sup> Exporting States request such documents to be provided by government-authorized end users with information on the items to be transferred and the parties to the transfer, but also require assurances and undertakings that place restrictions on the use and re-export of the transferred SALW and ammunition.

One can categorize such re-export clauses as either:

- Prohibition of re-export;
- Prohibition of re-export unless approval has been received from the original exporting State that re-export is permitted under certain conditions, such as authorization from the export licensing authorities of the State in which the end user or importer is located; or
- Assurance that re-export will only take place after authorization has been received from the export licensing authorities of the original exporting State.

Importing States should ensure that they have robust certification processes for end use/r documentation to prevent fraud and misuse, while competent authorities in exporting States and those in which brokers involved in the proposed transfer are located should authenticate the document and verify its contents as part of the risk assessment process.

Because end users and importing States do not always abide by assurances and undertakings on re-export, more States are including provisions in end use/r documentation that provide for post-delivery cooperation between exporting and importing States (e.g., on-site inspections of transferred arms in the country of import by the exporting State). This approach can be used selectively for cases involving SALW that are attractive for terrorist organizations and for transfers to regions where there is a high risk that SALW and ammunition could be – inadvertently – diverted to terrorists after delivery in the country of import.<sup>106</sup>

The effective implementation of national transfer control system relies on good communication and cooperation with key actors involved in the arms trade, such as companies in the defence industry and

---

104 See sanctions measures in Security Council, Security Council Committee Pursuant to Resolutions 1267 (1999) 1989 (2011) and 2253 (2015). Concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and Associated Individuals, Groups, Undertakings and Entities, <https://www.un.org/securitycouncil/sanctions/1267>; Security Council, Arms Embargo: Explanation of Terms, 2015, [https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/eot\\_arms\\_embargo\\_english.pdf](https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/eot_arms_embargo_english.pdf).

105 End user documentation "comprises documents whose purpose is to identify, authorize, commit to certain undertakings and verify delivery". For further information, see Modular Small-arms-control Implementation Compendium, National controls over the end-user and end-use of internationally transferred small arms and light weapons, MOSAIC Module 03.21, 2014, p.3. For more information on different types of end use/r documentation, see P. Holtom, H. Giezendanner and H. Shiotani, Examining Options to Enhance Common Understanding and Strengthen End Use and End User Control Systems to Address Conventional Arms Diversion, UNIDIR, 2015, pp. 42–44.

106 For more information on items considered attractive for terrorist groups see Box 43 (ACTO box)

**Box 42. Key issues for consideration on transfer controls, including export, import, brokering, transit, or retransfer**

- As part of its national risk assessment, does the State ensure that the competent national authorities in other states in the transfer chain have authorised the transfer and verified the bona fides of entities involved in the proposed international transfer and of the end user?
- As part of its national risk assessment, does the exporting State examine the reliability of the importing State, end user, and entities involved in the proposed international transfer – i.e. does it examine their record with regard to respect for re-export clauses in end use/r documentation, respect for international counter-terrorism instruments, and other relevant obligations under international law, including international human rights law and international humanitarian law and commitments to prevent terrorist acquisition of SALW and ammunition?
- Does the State, as part of its export risk assessment, examine the risk or potential that SALW, parts, components, and ammunition could be used to commit acts constituting an offence relating to terrorism and/or serious violations of international human rights law and international humanitarian law? If the assessment determines that there is a significant risk of such an occurrence, what measures and steps (e.g., refusal of an application for an export authorization, mitigation measures and safeguards) are considered and taken?
- Does the State ban all transfers of man-portable air defence systems (MANPADS), including their essential components, and other types of shoulder-fired guided missiles to non-State end users? Does it apply more stringent controls in State-to-State transfers of MANPADS? Does it apply more stringent controls for other types SALW and associated ammunition?
- Does the State have a procedure in place to issue end use/r documentation for government end users? Does the State's template end use/r documentation include all the essential informational elements recommended by international good practice?
- Does the State have a procedure in place to issue and/or certify end use/r documentation for non-governmental end users?
- Does the State authenticate end use/r documentation received as part of an application for an export authorization?
- Does the State verify the contents of use/r documentation received as part of an application for an export authorization as part of its national risk assessment?
- Does the State include restrictive provisions on re-export in its end use/r documentation?
- Does the State cooperate with other States in post-delivery cooperation exercises as (i) an importing State and/or (ii) an exporting State?
- Does the State conduct outreach to relevant industry actors on measures to prevent diversion to terrorists?
- Does the State take effective measures to control and regulate brokering and prevent, combat, and eradicate illicit brokering?

those in banking, finance, law, transport, and other services that provide practical support for arms trading activities (i.e., arms brokers). Most of these entities should be subject to national legislation and regulations in the jurisdictions in which they operate, should be aware of provisions for registration and authorization to conduct international arms trade activities, and put in place internal compliance programmes to ensure that their activities are compliant with arms transfer law and regulations and thus do not contribute to terrorist acquisition of weapons. The Addendum to the Madrid Guiding Principles calls on Member States to take “effective measures to prevent and combat the illicit brokering of [SALW]”.<sup>107</sup> In this regard, States should consider defining in their national legislation and regulations what constitutes a broker and brokering (and associated activities), the scope and types of weapons covered, and jurisdiction. To ensure that such entities are not engaged in facilitating international transfers that could be delivered or diverted to terrorists, international information-sharing and cooperation is essential (e.g., sharing information on registered brokers and authorizations for brokering transactions).

## Customs and border controls (2.5)

To effectively prevent, detect, and intercept illicit cross-border movements of SALW, including those destined for terrorists, it is important to ensure that countering illicit arms trafficking is integrated into a national border security strategy that also requires relevant law enforcement and security agencies (i.e., border control, customs, immigration, police) to cooperate and coordinate within the national border and with counterparts across the border. Effective border controls require an adequate legislative and regulatory framework that specifies items to be subject to transfer controls (see section 2.1.3 and 2.4), allowing the distinction between legal and authorized transfers on the one hand and diverted transfers and illicit trafficking on the other. In cases where the SALW are being illegally moved across borders for terrorist use, States can impose higher penalties and sanctions than for arms trafficking more generally to deter those involved in illicit arms trafficking from supplying terrorist entities.

Law enforcement and security agencies face several challenges in facilitating legitimate trade and, at the same time, detecting and intercepting diverted and illicitly trafficked SALW and ammunition. These broad challenges include:

- Limited technical knowledge of SALW, ammunition and in particular their parts and components;
- Time constraints for conducting rigorous checks on items, especially in transit and trans-shipment cases;
- Lack of appropriate infrastructure for screening containers and vehicles, as well as for safely and securely storing seized or confiscated items; and
- Other priorities for agencies tasked with addressing arms trafficking (e.g., collecting revenues on licit trade and detecting other forms of cross-border criminality).

---

<sup>107</sup> Security Council, S/2018/1177 (Guiding Principle 52, p. 28); Group of Governmental Experts, A/62/163 and A/62/163/Corr.1, 2007.

As it is not possible to screen every shipment at the border, it is important to establish, maintain, and update risk profiles to aid detection and interception efforts. Effective national information- and intelligence-sharing mechanisms can help identify shipments to be subject to physical inspections with minimum disruption to the legitimate free flow of goods. These risk profiles can be updated with information shared between agencies on seizures at the national level, as well as international exchanges, because actors, methods, and routes for diversion and trafficking can change quickly. For example, fast parcel post is currently viewed as posing a particular risk for the delivery of SALW, parts and components, and ammunition for criminals and terrorists.

#### Box 43. Key issues for consideration on customs and border controls

- Is the State's approach to border security and customs control coordinated across all relevant government departments? Is there a border security management strategy in place that includes addressing cross-border threats posed by the terrorist acquisition of SALW and ammunition?
- To what extent is it possible for people to enter the country, or free movement area, without passing through a recognized border control point?
- How porous are the State's borders? Does the State share a land or littoral border with a country where terrorist groups are active? Does the State share a land or littoral border with a country where unregulated SALW and ammunition production occurs (or where there is a dynamic illicit arms market)?
- How many cases of cross-border smuggling of illicit SALW have been detected by customs and border forces in the past? Is the trend increasing or decreasing? Are other illicit materials smuggled across borders? Is there any evidence or intelligence to suggest that terrorist groups and individuals exploit criminal supply chains?
- How effective are the customs controls and the screening of freight and parcels entering the country? For example, how much freight and what quantity is handled on a periodic basis by customs and border agencies? Are border security forces appropriately trained and equipped with identification and detection tools? What percentage of shipments are subject to physical inspection, and what percentage of inspections lead to the detection of illicit material of all types?
- Is there evidence or intelligence to suggest that terrorists are exploiting the international freight or fast parcel and postal systems to acquire SALW, parts and components, and ammunition?
- Does the State employ measures that permit the tracking of freight and parcels into the country, or through the country if trans-shipment from a port is taking place, to facilitate traceability?
- To what extent has the State, in conjunction with international partners, been successful in curbing the ability of terrorists and terrorist groups to operate across international borders?

As noted by the World Customs Organization Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework), it is important to maintain good relations not only with other national government agencies and other countries, but also with business entities involved in legitimate international trade activities.<sup>108</sup> Commercial entities can provide useful information for risk profiling and assessment, especially if made aware of the penalties, sanctions, and reputational risk they can suffer if found to have facilitated or enabled a delivery of SALW and ammunition to terrorists. As noted in section 2.4, outreach to the wide range of entities involved in the international arms trade is critical for ensuring that such entities do not unwittingly, or purposefully, facilitate terrorist acquisition of SALW.

## Security and management of national stockpiles (2.6)

Access to and diversions from lawfully held stockpiles at the national level are recognized as a major source through which terrorists acquire SALW and ammunition. Broadly speaking, the national stockpile consists of the “state stockpile” (i.e., under the control of a state’s defence and security forces) and

---

108 See Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework), 2021 edition, pp. 23-28, <http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/safe-framework-of-standards.pdf?la=en>.

### Box 44. Categorization of items’ attractiveness to criminal and terrorist organizations

While all SALW, and ammunition, could be used by terrorist groups, they are most likely to seek ways to access and acquire items that would significantly increase their capability. Depending on the context and the assessed and analysed threat and risk levels, more stringent security measures must be applied to such items, categorized according to the items’ attractiveness to terrorist organizations. In further reducing security and other risks, items in surplus that are attractive to terrorist organizations should be identified, prioritized, and destroyed.

the “civilian stockpile” (i.e., small arms and ammunition acquired and held by licensed and authorized civilians and civilian entities). Section 2.6.1 addresses security measures, while measures to aid management are addressed in section 2.6.2. There is a large volume of existing international guidance and good practices for ensuring safe and secure national stockpiles of SALW and ammunition – for both security and management of state and civilian stockpiles - and States and other users of this submodule are encouraged to consult this material for more detailed guidance.

#### 1. Security considerations for national stockpiles (2.6.1)

Security considerations for national stockpiles includes all measures for the State to effectively secure and control its own stockpiles of SALW and ammunition and the elimination of all opportunities for

unlawful diversion. In reviewing, assessing, and strengthening national stockpile management systems and security measures, States must pay particular attention to items' attractiveness to criminal and terrorist organizations.<sup>109</sup>

Two additional considerations for the security and control of SALW and ammunition that can be attractive to terrorists relate to:

**Stockpiles located in remote and/or border areas, at temporary sites or at forward operating bases.** Battlefield capture is a common way through which terrorists acquire SALW and ammunition in conflict-affected and operational settings.<sup>110</sup> Adequate attention should therefore be given to assessing and reducing risks through security measures and arrangements for the safe and secure transport to, from, and of smaller stockpiles located in such areas or sites.

---

109 See UN SaferGuard, International Ammunition Technical Guidelines, Security Principles and Systems, IATG 09.10 (in particular, p. 3), <http://data.unsafeguard.org/iatg/en/IATG-09.10-Security-principles-systems-IATG-V.3.pdf>; UN SaferGuard, Critical Path Guide to the International Ammunition Technical Guidelines, 2019 (in particular, pp. 63, 101, 110), <https://front.un-arm.org/wp-content/uploads/2019/03/Critical-Path-Guide-to-the-IATG-web.pdf>.

110 See, for example, Conflict Armament Research, "Typology of Diversion", Diversion Digest, Issue 1, 2018, p. 9, <https://www.conflictarm.com/publications>.

#### Box 45. Key issues for consideration on security considerations for national stockpiles

- Does the State conduct regular, systematic assessments of national state stockpiles, their locations, capacities, security systems, and measures in place? Are assessments conducted both at strategic and at operational or technical levels? Is the vulnerability of stockpiles to terrorist access and terrorist attacks included as an assessment criterion?
- Do the State and security forces have an established official categorization of items' attractiveness to terrorist organizations? Do the security forces have in place suitable security arrangements to store SALW, and to safeguard ammunition, according to categorizations of attractiveness to terrorist organizations?
- Is there any evidence or intelligence to suggest that terrorists target specific locations and stockpiles of State-owned SALW, and associated ammunition (e.g., in remote and/or border areas, at temporary sites and/or at forward operating bases), or transports to and from such locations or sites? If so, is the trend decreasing or increasing?
- Does the State have a vetting system and procedures in place for individuals responsible for and with access to stored, and transported, State-owned SALW and ammunition?
- Is there a suitably resourced entity within the State responsible for assuring compliance with legislation, regulations, and administrative procedures pertaining to the safe, secure, and accountable management of state stockpiles? If so, what is the frequency by which this entity inspects or reviews the procurement, storage, (final) use and final disposal?
- Does the State have robust risk assessment processes in place for regulating civilian access and possession of small arms and ammunition? Does the regulatory framework include provisions on safe and secure storage, handling, and transport of such items?

**Recovered SALW and ammunition.** The lack of capacity to safely and securely manage recovered SALW undergoing custody changes can significantly hinder their processing. The same applies for the treatment of recovered ammunition. This is relevant for changes of custody from defence and security forces, to (a) focal point(s) conducting tracing operations, to justice authorities for judicial processing. It is also relevant in low-capacity and conflict-affected settings, where frequent or larger quantities of recovered SALW need to be safely and securely processed, as well as for recovered ammunition that needs to be treated (see sections 3.1–3.3).

Small arms and ammunition held by licensed and authorized civilian entities and civilians also represent a source of supply for terrorists. Generally, a risk-based approach should be applied by States in regulating civilian access to and possession of SALW and ammunition.<sup>111</sup> Robust licensing processes and procedures must be established and implemented by the national licensing authority for regulating such access and possession, in addition to measures to ensure safe storage, handling, and transportation by civilians and civilian entities (e.g., to prevent theft). This also includes mechanisms to verify and inspect civilian holdings and compliance with such measures, in accordance with domestic law and regulations.

## 2. National accounting system (2.6.2)

An effective national accounting system can be described as a system that accounts for the entire State-owned stockpile of SALW and ammunition, as well as the licensed and authorized civilian held stocks at any point in time. One of the purposes of a national accounting system is to record and account for

---

111 See Modular Small-arms-control Implementation Compendium, National Regulation of Civilian Access to Small Arms and Light Weapons, MOSAIC 03.30, 2015, <https://www.un.org/disarmament/wp-content/uploads/2018/10/MOSAIC-03.30-2015EV1.0.pdf>.

### Box 44. Categorization of items' attractiveness to criminal and terrorist organizations

- Does the State ensure the marking of all SALW at the time of their manufacture or production (this applies to a State with an industrial manufacturing capacity)?
- To what extent are all regulated and authorised SALW in the national borders (i.e., all State-owned SALW for governmental use, and all licensed small arms or firearms in civilian possession) adequately and uniquely marked? For example, what percentage of State-owned SALW currently in the national stockpile are marked? To what extent does the State ensure that all newly imported weapons are adequately and uniquely marked?
- Is there an established national programme – including a prioritization and sequenced, measurable specific plan – to ensure that all newly imported SALW and all those SALW already in-country in governmental use are adequately and uniquely marked?
- To what extent are electronically readable unique identification weapon markings applied and corresponding electronic reading tools used by national authorities (e.g., to facilitate identification by non-expert personnel and enhance traceability)?

SALW and ammunition across their life cycle. Such systems can be manually or electronically operated and are composed of two subsystems: (i) a national marking system (see 2.6.2.1) and (ii) a national record-keeping system (see 2.6.2.2). An effective national accounting system is one of the prerequisites for, and an essential component of, an effective tracing system at the national level.

### **Weapons marking (2.6.2.1)**

States must ensure that SALW are adequately and uniquely marked at defined stages of their life cycle in line with relevant international instruments, at a minimum at the time of manufacture and import. Existing international guidance provides recommended minimum information to be included in marking on SALW at these stages to assist with national record-keeping and tracing requests. It is possible for the manufacturer to provide markings on newly produced items that contain information regarding not only the manufacturer but also the importing State - if the importing State's marking requirements are made available to the manufacturer.

It is important to provide for marking for different end users and for other stages in the life cycle of SALW, such as:

- When proofed by authorized entities and inspecting authorities;
- When distinguishing between government use (e.g., by defence and security forces) and civilian use (e.g., private security companies or hunting);
- When legally transferred from government to non-government use;
- When recovered and to be disposed of, including through destruction;

#### **Box 47. Key issues for consideration on record-keeping**

- What is the level of maturity of the State's broader national record-keeping system, capacities, practices, and procedures? What type of national recordkeeping methods are used (e.g., manual, or electronic)? What is the frequency by which records are updated?
- To what extent is the national record-keeping system for State-held SALW harmonized vertically (i.e., identical informational elements recorded within a "database" in a national authority that is a custodian of records from the top level to the lowest unit level)?
- To what extent is the national record-keeping system for State-held SALW harmonized horizontally (i.e., identical informational elements that are recorded and structured within a "database" in that is maintained across national authorities that are custodians of records)?
- Do the State and record-keeping authorities have systems, procedures, and measures in place to control and authorize access to records as well as to ensure security of recorded information and data (e.g., a backup system)?
- Does the State maintain a national registry of records of State-held SALW, and ammunition, for governmental use that have been lost, stolen, or captured in combat? If so, are these records shared and centralized within a central national authority? Are these records shared with the national lead entity or focal point coordinating and/or processing tracing operations?

#### Box 48. Key issues for consideration on information collection, including investigations, and analysis system

- To what extent does the State possess the fundamental core capabilities of forensic (including ballistic) evidence analysis and investigation of illicit SALW, and ammunition, parts, and components?
- What is the level of centralization or decentralization of the national tracing system? Has the State established a national tracing centre or similar entity?
- To what extent does the State have access to and use existing international tracing mechanisms and information exchange networks (e.g., to process international tracing requests and complement its threat picture of the weapon capabilities of terrorist groups)?
- Does the State have an automated ballistic identification system? To what extent does the State have access to and use existing international ballistic evidence exchange and comparison mechanisms and networks (e.g., INTERPOL's Ballistic Information Network)?
- Does the State have the means to securely receive, store and process (i) information contained in international tracing requests and (ii) information and intelligence related to terrorist weapon capabilities?
- To what extent is the State able to take the analytical products resulting from recovered and traced SALW, associated ammunition and related items, and integrate or fuse these products with other indicators or sources of information or intelligence?

- When government surpluses are deactivated; and
- When authorized civilian-owned holdings are deactivated.

It is possible that terrorists and criminal actors will make efforts to remove, alter, or obliterate markings on SALW and ammunition (crates and boxes). States, in cooperation with manufacturers of SALW and marking technology developers, are therefore encouraged to ensure that markings (i) are difficult to remove and/or alter and (ii) can be recovered if efforts have been made to remove such marking (i.e., retrieval of marked information) (see also 3.2).

#### Record-keeping (2.6.2.2)

States must have an effective, comprehensive national record-keeping system in place that ensures that complete and accurate records of all SALW at defined stages of their life cycle<sup>112</sup> are established and regularly updated and that these records are easily accessible in a timely manner and maintained over defined time periods. The keeping of records for indefinite time periods significantly enhances tracing, analytical, and investigative capabilities.<sup>113</sup>

---

112 This includes records of transfers (e.g., exports and/or imports, transit or trans-shipment, brokers, and end users and documentation); records of SALW, and ammunition, in the national stockpile; records of authorized civilian possession of SALW; records of lost and stolen State-held SALW and ammunition; records of disposals (e.g., destructions, sales or donations) and deactivations; as well as records of SALW, ammunition, and related material, recovered from the illegal or illicit sphere.

113 Relevant international instruments provide minimum time periods, while relevant international standards recommend keeping records indefinitely. National legislation and regulations can set time periods for which records are maintained.

Most effective national record-keeping systems rely on high degrees of vertical harmonization (within national authorities and record custodians) and horizontal harmonization (across national authorities and record custodians) of informational elements included in records, as well as inter-connectivity and interoperability of record-keeping systems at appropriate levels. The centralized storage of all such records, within key ministries or agencies or an authorized national lead authority, can greatly increase access and analysis of records.

Manual record-keeping systems, if structured and used appropriately, can be effective, while efficiency is improved through computer-based, networked communication systems. Access and information security measures are needed for both types of system.<sup>114</sup>

## Information collection, including investigations, and analysis system (2.7)

It is of critical importance that the authorized national lead entity or the focal point that oversees the information collection and analysis system, in particular the tracing system, at the national level and coordinates and/or processes domestic (see section 3.4) and international tracing operations (see section 3.5), is appropriately mandated, resourced, and knowledgeable. The capacities and the siting of such national tracing focal points, units or entities within governments' national security architectures vary. Such an entity will also likely lead or coordinate inputs for the assessment and analysis of SALW-related threats and risks to inform the national policy or strategy (see section 2.1.1). States may have a centralized (e.g., one focal point and database) or decentralized national tracing system (e.g., with several focal points and databases). A specific coordination including an information sharing mechanism and procedure is needed to conduct domestic, and if needed international, tracing operations (see 3.4 below). A centralized database,<sup>115</sup> where all information (data) from SALW, and ammunition, recovered from the illegal and/or illicit sphere is centrally collected and analysed (see sections 2.6.2.2 and 3.1–3.3) is another key requirement for an effective national tracing system and capability. Where several such databases exist, coordination is needed, and communication between them is required as a first step. At more advanced stages, registries should be inter-connected (through networked communication systems) and made interoperable with other national systems, and international systems.

Key investigative methods and techniques that can be applied to identify acquisition modes, actors, entities, and individuals involved in terrorist procurement networks are described in section 3.6. As noted, the effective application of such investigate methods and techniques requires coordination by the national focal point or lead entity and close cooperation between law enforcement, intelligence, and specialist military agencies, among others. Robust and reliable processes must therefore be established to allow the flow of information and intelligence between those entities.

---

114 Generally, these include access authorization and control measures, regular (independent) inspections, and a secured backup system to prevent information and data loss in the case of any unforeseen event (e.g., an attack).

115 This database is sometimes also referred to as the "national repository" or "national database".



Photo / Adobe Stock

## Countering terrorist acquisition of SALW and ammunition: downstream measures

### Incident scene exploitation, including registration and documentation (3.1)

Once a scene or site at which SALW acquired by or misused by terrorists has been secured and rendered safe, the systematic and proper registration and documentation of all recovered SALW, small calibre ammunition, and related material is an integral part of collecting information (including data) and evidence. Wherever possible, forensic (biometric) evidence (e.g., fingerprints and DNA) should be collected first (e.g., by law enforcement units). It is fundamental that registration and photographic documentation include at a minimum:

- The essential informational elements of each SALW,<sup>116</sup> and ammunition (i.e., of individual rounds or by lots or batches);
- Additional informational elements on or in a SALW;
- Attributing informational elements (e.g., confirmed, or suspected users); and
- Contextual informational elements (e.g., on the capture, seizure or confiscation, cache, and so on, as well as on victims, disaggregated by gender and age).

<sup>116</sup> The essential, unique identification of a small arms or light weapon registered shall include: a) make; b) model; c) caliber; d) complete serial number; e) country of manufacture; and f) country of most recent import (if the weapon bears an import mark). See Modular Small-Arms-Control Implementation Compendium, MOSAIC 05.31, Version 1.0, 2021-08-27.

#### Box 49. Key issues for consideration on incident scene exploitation, including registration and documentation

- Can an estimate be given of how many (quantity of) SALW and ammunition have been recovered from the illicit sphere over a specific timeframe by different defence and security forces and law enforcement (e.g., by year or month)? Can an estimate be given of how many of these (percentage of total quantity) could have been subsequently technically exploited?
- Does the State have a procedure in place for the processing of recovered SALW and the treatment of recovered ammunition, including their registration and photographic documentation? If so, is the procedure ad hoc or formalized (written)?
- What is the number of defence and security force as well as law enforcement units that have received training on scene exploitation, including SALW and ammunition registration and documentation? Is such registration and documentation included in defence and security force as well as law enforcement units training curricula (alongside the safe and secure handling of SALW and ammunition)?
- Does the State and its defence and security forces have specialized weapons-technical intelligence units?
- How mature are the broader State capabilities for the analysis of forensic evidence? For example, is the State able to recover and record fingerprints and compare them to fingerprints stored in a national or international database?
- Are there examples of where the State has used information acquired from incidents in the successful prosecution of those involved in terrorist SALW-related offences?

Registration, including photographic documentation of SALW, and ammunition, does not usually require specialist skills, techniques, and equipment. A standard operating procedure or protocol for dealing with such materiel should be developed and adopted at the national level to ensure awareness and consistency at different levels and to sustain this critical capability for subsequent downstream measures over time.<sup>117</sup> Such a procedure or protocol should cover at minimum the specific measures described in subsections 3.1 to 3.5 of this submodule.

Specialist skills and techniques are needed to collect forensic (biometric) evidence on site. At more advanced stages, specialized military<sup>118</sup> or law enforcement units are trained to collect such information and evidence (and prepare on-site technical and forensic reports).

---

117 INTERPOL and the United Nations Office on Drugs and Crime in the global law enforcement and criminal justice domain, and non-governmental expert organizations such as Conflict Armament Research and the Small Arms Survey, which are specialized in tracing conflict weapons, have developed guidance material including templates and capacity-building initiatives in this regard.

118 This includes explosive ordnance disposal or weapons-technical intelligence units. Weapons-technical intelligence refers to the processes and capabilities to collect, exploit and analyse SALW (and other weapons and systems), ammunition and related material. Such capabilities enable technical exploitation, tracing operations, the provision of support to judicial processes, and the identification and targeting of asymmetric threat networks.

Where on-site exploitation is not possible,<sup>119</sup> all recovered items must be safely and securely transported. The integrity of the chain of custody and material evidence needs to be maintained for subsequent technical exploitation (see section 3.2). For such cases, States should have dedicated sites and facilities where illicit items will be technically exploited.

### Technical exploitation (3.2)

The full and complete technical exploitation of recovered SALW and ammunition serves multiple purposes and is a critical enabler for the national focal point entity and relevant national authorities to implement several upstream and downstream measures and activities, including:

- Providing the necessary information for domestic tracing operations (see section 3.4) to help identify domestic sources of supply or points of diversion (e.g., the manufacturer in the case of “reactivated” or “converted” weapons);
- Providing the necessary information for international tracing operations (see section 3.5) to help identify sources of supply or points of diversion external to the State;
- Examining, to confirm or rule out, and exploit links between SALW and ammunition used in one case and those used in other cases of terrorist activities;
- Providing the necessary information (data) to inform threat and risk analysis (see, for example, section 2.1.1);
- Providing the necessary information (data) to inform transfer risk assessments and mitigation measures (see section 2.4); and
- Informing other types of countermeasures.

The ability of national authorities to technically exploit SALW and ammunition recovered from terrorist incidents or attacks, and to inform the above-mentioned measures and activities, will be dictated in the first place by their capacities to correctly, completely, and accurately identify SALW, parts and components, and ammunition.

---

<sup>119</sup> On-site exploitation, including registration and (photographic) documentation, may not be possible where larger quantities of SALW, and ammunition, are recovered or in low-capacity and/or high-risk environments, such as in military operational and/or conflict-affected settings. When responding to an incident or attack and/or during operations, wherever the situation and circumstances allow for it, efforts should be made to collect weapons—technical information and intelligence.

#### Box 50. Key issues for consideration on technical exploitation

- To what extent does the State possess the fundamental core capabilities of recovery, preservation, and analysis of (i) forensic ballistic evidence on illicit SALW (including for those with obliterated, altered or removed markings) and ammunition, and (ii) forensic biometric evidence on illicit SALW and ammunition?
- Does the State have a national reference guidance document that systematically identifies, documents, and catalogues all SALW, parts and components, and ammunition recovered in-country from the illicit sphere? If so, is this reference guide held manually or in a secured electronic format?

#### Box 51. Key issues for consideration on information management

- Does the State have a standardized format (in line with international standards and good practices) for the submission of reports of SALW, associated ammunition, and related material recovered from the illicit sphere, including from terrorists?
- Are such reports collated centrally by one national lead authority and entered into a central registry (or “repository”) database? Or are such reports collated into registries (or repositories) and databases kept by several authorities at the national level?
- How are informational and analytical products resulting from the analysis of recovered SALW, ammunition, and related items being used and acted on?
- Are forensic exhibits (e.g., fingerprints and DNA) and law enforcement interview reports collected from those arrested and subsequently prosecuted for SALW-related offences?
- Do the State employ information systems to help in the storage, processing, and analysis of all-source intelligence?
- Do the State’s information management (IM) processes permit the rapid and effective flow of information and intelligence on SALW-related threats and risks to those entities that need it?
- Do the State’s IM processes permit the rapid and effective flow of information and intelligence on illicit arms flows, trafficking, and threats to regional and/or international partners (under established cooperative frameworks)?

Where markings on recovered SALW have been removed, altered, or obliterated, forensic capabilities are required to retrieve markings and the information contained in them for exploitation and analysis (see section “Weapons marking”).

### Information management (3.3)

A robust and effective approach to information management (IM) underpins most successful approaches to prevent, mitigate, and counter terrorist acquisition and use of SALW and ammunition. IM should be understood as the process of collecting, organizing, storing, and providing information within a government or organization. An effective IM system and robust IM processes are mirrored in and crucially underpin several upstream (e.g., the information collection and analysis system) and downstream measures (e.g., tracing operations). It is essential that where automated data, information or intelligence systems are employed, analysts are provided with automated collation and analysis tools to process the ensuing large volumes of information. Effective IM processes are also a key requisite for the sharing and exchange of information and intelligence with relevant regional and international stakeholders and partners as part of international cooperative efforts.

#### Box 52. Key issues for consideration on domestic tracing operations

- Does the State have a mandated and authorized, sufficiently resourced and empowered national lead entity or focal point at an appropriate level within the government responsible for coordinating and/or processing domestic tracing operations (this entity or focal point may be identical to the lead entity or focal point responsible for coordinating and/or processing international tracing operations)?
- What is the level of centralization of the national tracing system? Does the State have centralized or decentralized national tracing system?
- Are focal points established at appropriate levels within all relevant national authorities (i.e., custodians of records of State-owned SALW, and ammunition; custodians of records of lost, stolen, or captured SALW, and ammunition) responsible for the processing of domestic tracing operations?
- Is there a domestic tracing coordination, including information-sharing, mechanism in place? Does the State have a procedure in place for the conduct of domestic tracing operations? If so, is the procedure ad hoc or formalized (e.g., written)?
- How effective is the State in undertaking domestic tracing operations? For example, what percentage of SALW, and ammunition, recovered from the illicit sphere are traced domestically? How many domestic tracing operations have been undertaken within a year? How many of them were successful?

### Domestic tracing operations (3.4)

Unless terrorist groups and individuals rely on sources external to the State in which they operate, they acquire SALW, and ammunition, primarily from domestic sources. An effective national system for domestic tracing operations is essential to determine if and how SALW, and associated ammunition became illicit and ended up in terrorist hands at the national level. The national system should enable authorities to identify the circumstances (e.g., the “what”, “when”, “where”, “how” and “with whose involvement”), establish the facts of criminal activities, and initiate judiciary actions.

Incrementally over time, the accumulated data and analysed results of domestic tracing operations allow the identification of different sources through which terrorists acquire SALW at the national level. Such tracing operations also enable the identification of risks and vulnerabilities in national stockpile security systems and measures (see section 2.6) and support investigative law enforcement as well as prosecutorial capabilities that inform the judicial process (see section 3.7). It is important that domestic tracing operations are conducted before proceeding with international tracing operations (see section 3.5).

### Box 53. Key issues for consideration on international tracing operations

- Does the State have a duly mandated, authorized, and sufficiently resourced national focal point or entity at an appropriate level within the government responsible for the coordination and/or the processing of international tracing operations for SALW (this entity or focal point may be identical to the lead entity or focal point responsible for coordinating and/or processing domestic tracing operations)?
- Is there a coordination, including information-sharing, mechanism in place for the processing of international tracing requests? Does the State have a procedure in place for the processing of international tracing operations? If so, is the procedure ad hoc or formalized (e.g., written)?
- To what extent does the State systematically conduct international tracing operations where domestic tracing operations have not yielded the required results (i.e., successfully established the point of diversion and the source domestically)?
- How effective is the State in processing (i.e., issuing and promptly responding to) international trace requests? For example, what percentage of those SALW, and ammunition, domestically traced and confirmed as not originating from domestic sources, are traced internationally? How many international trace requests are being processed (including being issued and responded to) within a year's time frame?
- How are analytical products resulting from international tracing operations used and acted on by relevant national authorities?

## International tracing operations (3.5)

Terrorist groups and individuals can source SALW and ammunition from sources beyond the borders of the State in which they operate. An effective system at the national level to process international tracing operations is essential to identify such sources, breaks in unsecured supply chains, and terrorist procurement networks. Therefore, effective cooperation with States and international partners is a prerequisite for tracing operations at the international level. Similarly, coordination at the national level by a national lead entity or focal point is required to execute and process international tracing operations (e.g., issuance of and responses to trace requests) under existing international cooperative frameworks, instruments, and mechanisms (see section 2.2).<sup>120</sup>

The effective execution of international tracing operations, and their sustainability over time, requires

---

120 Several instruments and cooperative frameworks exist that can be used by States to engage in international tracing. States shall cooperate with United Nations Security Council mandated sanctions monitoring teams (i.e., the 1267 Sanctions Monitoring Team) and entities such as groups and panels, and other entities mandated to monitor the implementation of relevant United Nations arms embargo regimes, which undertake or can facilitate international tracing requests. For SALW recovered in crime, INTERPOL Member States should make full use of the existing INTERPOL tools and resources, including to properly identify illicit firearms and process international trace requests. A number of subregional or regional arms control and law enforcement instruments and organizations also provide cooperative frameworks and include provisions for tracing operations and information exchanges. Non-governmental expert organizations, such as Conflict Armament Research through the iTrace platform, also support such efforts. In some contexts, bilateral or multilateral security commissions can also provide frameworks that allow cooperation in this regard. In other contexts, specific national and subregional or regional systems exist (e.g., the US system for facilitating the tracing of US-sourced firearms through the eTrace tool).

**Box 54. Key issues for consideration on identifying acquisition modes, involved actors, entities, individuals, and perpetrators**

- What type of investigative methods and techniques does the State and relevant national authorities employ? Does the State exchange information and good practices with international partners?
- Does the State effectively integrate the various sources of information and intelligence open to it to identify perpetrators?

the development and adoption of an administrative standard operating procedure or protocol at the national level. This should define, inter alia, the roles and responsibilities of the lead entity or focal point, as well as of other relevant and competent national authorities, and appropriate information exchange mechanisms.

### **Identifying acquisition modes, involved actors, entities, individuals, and perpetrators (3.6)**

The ability of the State to identify the modes of terrorist acquisition of SALW is fundamental to any effective preventative, mitigation, and response strategy or policy (see section 2.1.1), including for the development of corresponding countermeasures and capabilities. The identification of actors, entities,

**Box 55. Key issues for consideration on criminal justice process**

- To what extent does the national legislative and regulatory framework include mandatory and additional enforcement and criminalization provisions, in line with the applicable international law, including international arms control and counter-terrorism instruments?
- Does the State conduct regular reviews of its legislative and regulatory regimes to ensure their effectiveness in responding to emerging trends in terrorist SALW acquisition?
- Is there a track record, and are there examples, of successful prosecutions of persons involved in the trafficking in and use of SALW for terrorist purposes?
- Are appropriate security measures in place to protect those involved in the administration and delivery of justice?
- Has the State concluded effective bilateral or multilateral arrangements and channels for the following: (i) to cooperate with authorities (e.g., law enforcement, prosecutorial and judicial) of other States; (ii) to coordinate cross-border investigations and prosecution; and (iii) to prevent and combat trafficking in SALW and ammunition?
- Are actors of the criminal justice system aware of relevant international obligations and commitments regarding the prevention of terrorist acquisition of SALW and ammunition as well as the ways and means through which terrorists acquire such items?

and individuals involved in terrorist procurement networks may be achieved through a combination of different methods and techniques:

The analysis and use of biometric evidence (e.g., DNA and fingerprints)<sup>121</sup> from a weapon used in a suspected or confirmed terrorist incident can lead to or support the identification of the perpetrator, as well as links to other terrorists and incidents.

Profiling of recovered SALW, and ammunition, enables the generation and establishment of comparable baseline information and factual profiles of holdings, types, and origins of illicit SALW, and ammunition, proliferating and circulating in-country and in specific terrorist groups, to assist further investigation.

Systematic, targeted tracing of SALW, and (to the furthest extent possible) ammunition, helps identify the points in space and time when SALW, and ammunition, became illicit and were acquired by terrorist groups and individuals, as well as the circumstances of their acquisition and those involved in their supply.

The application of document extraction methods and techniques applied to documentation related to or encountered with recovered SALW, ammunition, and related materiel helps build a comprehensive threat picture and identify actors, entities and individuals involved in procurement networks.<sup>122</sup>

The development, adoption, and deployment of profiling mechanisms, methodologies and indicators by national arms transfer control authorities, law enforcement, intelligence, border, and customs agencies increase detection rates by providing filtering mechanisms that concentrate “concentrate investigative efforts and resources on those cases aspects of which may signal a potential clandestine shipment”.<sup>123</sup>

A nationally coordinated “layering approach” (or multi-layered approach) is considered one effective way to identify actors, entities, and individuals involved in terrorist procurement networks, and the links between the illicit trafficking of SALW, ammunition, and other illicit goods. Such an approach integrates or fuses “material” indicators (e.g., analysed tracing results) with financial and other indicators.<sup>124</sup>

Depending on the context, this may include intelligence derived from information collected and provided by human sources, as well as from imagery sources. The exploitation of other types of intelligence, such as signals intelligence, may provide real-time information on where and how terrorists are acquiring and using SALW and ammunition. Open-source intelligence, for example derived from social media

---

121 See United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, CTED and UNOCT, in association with the Biometrics Institute, 2018.

122 See UN SaferGuard, International Ammunition Technical Guidelines, Security Principles and Systems, IATG 09.10, p. 13; see also H. Griffiths and A. Wilkinson. *Guns, Planes and Ships: Identification and Disruption of Clandestine Arms Deliveries*, SEESAC, 2007.

123 UN SaferGuard, International Ammunition Technical Guidelines, Security Principles and Systems, IATG 09.10, p. 13.

124 UN SaferGuard, International Ammunition Technical Guidelines, Security Principles and Systems, IATG 09.10, p. 13. Other types of indicators may include air, maritime, land, end user, broker/freight forwarder indicators.

accounts, can also yield considerable contextual or complementary information, which may also be useful to support in the above efforts.<sup>125</sup>

All methods and techniques described in this section are to be applied in due cognizance of, and in full compliance with, international law, including international human rights law and, if applicable, international humanitarian law, as well as rule of law principles.

### **Criminal justice process (3.7)**

States should evaluate the effectiveness of their national criminal justice measures and processes related to preventing terrorist acquisition of SALW and determine whether their national legislation and regulations include appropriate enforcement and criminalization provisions for addressing terrorist acquisition of SALW and related ammunition (see section 2.1.3). Legal review processes should also consider existing or emerging threats and risks related to terrorist acquisition of SALW and ammunition (see section 2.1.3). The establishment of mandatory criminal offences to enforce existing SALW control regimes is essential for effective justice responses, as it provides the necessary basis for investigation, prosecution, and adjudication. Other activities associated with terrorist acquisition of SALW, and ammunition, can also be criminalized by States for deterrence purposes.

International cooperation (see section 2.2), in particular international law enforcement and judicial cooperation, is vital to counter terrorist acquisition and use of SALW and ammunition. States should consider entering into regional and international cooperation agreements for detection, interception, and subsequent investigation and prosecution of SALW-related criminal offences that are connected with terrorism.

Investigations regarding terrorist acquisition of SALW should not only focus on the primary offence of illicit acquisition or possession, but also examine the sources and origins of the weapons and transactions (see sections 2.7 and 3.6) to enable the prosecution of entities and individuals involved in illicit activities along the supply chain.

It may also be helpful to work with members of the judiciary to raise their awareness and increase their understanding of the different ways and means through which terrorists acquire SALW, parts and components, and ammunition, both domestically and internationally. Criminal justice actors should be familiar with international SALW control and counter-terrorism instruments and provisions. More broadly, States should consider building the capacity of criminal justice authorities in the investigation, prosecution, and adjudication of cases, including complex cases involving terrorist acquisition of SALW.

---

<sup>125</sup> While this type of information and intelligence may be useful, its verification can pose significant challenges (e.g., where essential informational elements are needed to uniquely identify SALW and ammunition).

#### Box 56. Key issues for consideration on development of countermeasures

- To what extent does the State monitor the use of SALW, parts and components, and ammunition, by terrorist groups (and organized criminal groups, to the extent there is a linkage)? To what extent can the State respond expeditiously and effectively to changes in terrorist group tactics, techniques, and procedures related to their acquisition of SALW and ammunition?
- How regularly does the State comprehensively assess and analyse the nature and dynamics of SALW-related terrorist threats, risks, and impacts across its territory? How is this assessment and analysis used to inform relevant national policies and strategies? To what extent can the State implement a feedback loop and through generated results of the effective implementation of downstream measures inform the strengthening of relevant upstream measures? How does the State adjust or further develop corresponding countermeasures and capabilities?
- How quickly is the State able to respond to changes in the use of SALW, parts and components, and ammunition by terrorists and terrorist groups and develop corresponding upstream and/ downstream countermeasures and capabilities?

### Development of countermeasures (3.8)

Any effective strategy and corresponding counter-capabilities need to be able to adapt and respond to changes in the ways through which terrorists acquire and use SALW in a specific national and subregional context. It is essential that national resources are available to closely monitor and conduct regular assessments of SALW-related terrorist threats, risks, and impacts. The results of such efforts inform changes in the broader national policy, regulatory framework, and upstream and downstream measures described in this submodule.

Generally, upstream, and downstream measures must be implemented in concert; on their own, these measures will be insufficient to prevent, prepare against, and mitigate terrorist acquisition and use of SALW and ammunition. A State needs sufficient capacity to be able to effectively implement the capability maturity model feedback loop – effectively implementing downstream measures and feeding back lessons learned into upstream measures – to learn and adapt countermeasures and capabilities accordingly and consistently over time. The key elements of the capability maturity model include the extent to which the State can respond to either predicted or actual changes in sources, ways, and means through which terrorists and terrorist groups acquire SALW and ammunition, and how the State is then able to further refine, develop, and adopt effective upstream and downstream countermeasures.









[www.un.org/counterterrorism/cct](http://www.un.org/counterterrorism/cct)

