ADDENDUM TO THE HAGUE GOOD PRACTICES ON THE NEXUS BETWEEN TRANSNATIONAL ORGANIZED CRIME AND TERRORISM:
FOCUS ON CRIMINAL JUSTICE
The nexus between transnational organized crime and terrorism comes in many forms and manifestations. Terrorist organizations and transnational criminal networks have exploited and benefitted from many factors, including conflicts, instability, lack of rule of law, porous borders, high levels of corruption and weak democratic institutions and law enforcement. In such situations, terrorism and transnational organized crime can flourish and fuel each other. When terrorism, the financing of terrorism and transnational organized crime intersect, this can further contribute to escalation of violence, may intensify conflicts in affected regions, and have an impact on security.

The international community has increasingly reiterated concerns that where linkages exist between transnational organized crime and terrorism, responding effectively becomes more challenging due to the complex and dynamic nature of the crimes. Understanding this linkage is moreover difficult, as it is context and region specific. Terrorist groups and transnational criminal networks may interact with each other for financing or operational purposes, such as through the exchange of networks, knowledge, or skills. Sometimes a structural cooperation exists, which could be witting or unwitting, opportunistic or more organized, whereby terrorist groups and transnational criminal organizations integrate or transform from a criminal group to a terrorist organization or vice versa.

Terrorist organizations and transnational criminal networks may intersect when it comes to illicit trafficking in goods such as cultural property, drugs, firearms, wildlife, gold or other precious metals, and stones or in commodities such as oil, charcoal, or sugar. Terrorists can be involved directly or indirectly in such illicit trafficking. When terrorists are indirectly involved in trafficking, they may control trade routes and provide security, transport, or safe passage to criminals involved in trafficking in exchange for advantage, control, goods, or cash. Sometimes terrorist organizations can be directly involved in trafficking and become themselves traffickers, which allows them to fund or expand their organization. There are thus specific circumstances where terrorist organizations and transnational criminal networks might benefit one another, and in which both terrorist-related and transnational organized crime-related offences occur.

The United Nations Security Council (UNSC) has adopted various resolutions on this issue. UNSC Resolutions 2195 (2014), 2322 (2016) and 2347 (2016) underline the importance of enhancing international and regional cooperation, when terrorism and transnational organized crime converge. More recently, UNSC Resolutions 2462 (2019) and 2482 (2019) recognize that terrorist organizations can benefit from transnational organized crime as a source of financing and encourage UN Member States to strengthen their responses in recognizing and addressing the linkages between terrorism and transnational organized crime that pose a threat to international peace and security.

The Criminal Justice and Rule of Law Working Group (CJ-ROL WG) of the GCTF has taken the initiative to explore linkages between terrorism, financing of terrorism, and various forms of illicit trafficking of goods from a criminal justice perspective as part of its Work Plan for 2019-2021. A first expert meeting was held in London, United Kingdom, on 29-30 October 2019. It explored criminal justice responses to the linkages between terrorism, financing of terrorism, corruption, and other financial crimes.¹

A second expert meeting was held in Malta on 11-13 February 2020 and focused on linkages between terrorism, financing of terrorism, and illicit trafficking in firearms, drugs, natural resources, cultural property, as well as on maritime crimes and piracy. This initiative builds on earlier documents developed by the GCTF, such as the GCTF *The Hague Good Practices on the Nexus between Transnational Organized Crime and Terrorism*, which encourage a criminal justice approach to that nexus (Good Practices 1, 2, and 23), the *Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector*, and the *Abuja Recommendations on the Collection, Use and Sharing of Evidence for Purposes of Criminal Prosecution of Terrorist Suspects*.

The Addendum is intended to complement and support the implementation of the United Nations Convention against Transnational Organized Crime (UNTOC) and its supplementary Protocols on Trafficking in Persons, Smuggling of Migrants, and Trafficking in Firearms Protocols, the United Nations Convention against Corruption (UNCAC), as well as universal international counterterrorism conventions and protocols.

Terrorism and transnational organized crime are generally criminalized by different laws and may require different criminal justice responses. When terrorism and transnational organized crime do not intersect, the linkage should not be overstated. When terrorism and transnational organized crime do intersect, a thorough understanding of the nature of the linkages between terrorism and transnational organized crimes is important in order to formulate an appropriate criminal justice response. At all times, such a response should be in accordance with applicable international law, such as applicable human rights law obligations, including with respect to derogations. To ensure that criminal justice is in compliance with applicable international law, including international human rights law, and within a rule of law framework, appropriate procedural safeguards should be adopted. Furthermore, there is a need to adopt a gender-sensitive approach in the criminal justice system and to take into account the complexities that women may face as victims, witnesses, or perpetrators. This includes providing guidance on gender-sensitive issues that may arise during arrest, questioning, prosecution, adjudication, or detention, and during rehabilitation and reintegration of women.

This Addendum aims to offer good practices and recommendations on how to strengthen the criminal justice approach and improve the capacity of law enforcement officials and prosecutors to successfully detect, investigate, and prosecute crimes that sit at the nexus between terrorism and transnational organized crime, in accordance with domestic law, while respecting international law, including in particular international human rights obligations.

**Good Practices**

**I. Prevention**

*Good Practice 1: Raising Awareness and Capacity among Criminal Justice Actors and Other Competent Authorities*

Considering the negative impact that both terrorism and transnational organized crime have on society, focusing on prevention of these crimes is paramount. It is essential to research the linkages
between these crimes and their specific characteristics and to share this knowledge through technical assistance, including capacity-building programs and case-based mentoring with the relevant authorities in order to support them to recognize these developments in the local context. Given the expert knowledge needed to understand the complexities of, for example, illicit trafficking dynamics of cultural property or wildlife and their convergence with terrorist networks, incorporating expert technical assistance, including lectures, or using actual case studies is a good practice. When prosecutors are posted abroad, they may engage in training activities, participate in workshops, and enhance their understanding of the linkage. Training should focus on how to conduct financial investigation and increase understanding of the role of informal banking (e.g. the use of Hawala) to enable detection and/or disruption of these crimes. Such training should also address human rights issues. States are recommended to support and engage in bilateral, regional, and multilateral capacity-building programs, particularly drawing upon the resources and expertise of the UN Office on Drugs and Crime (UNODC).

Having a good understanding of the nexus between terrorism and transnational organized crime is moreover important for making appropriate choices in allocating resources, as well as in determining which criminal justice responses should be applied.

States are therefore recommended to support multilateral capacity-building programs, especially those offered by the UNODC, to raise awareness, build capacity among relevant practitioners, and strengthen partnerships with civil society, in understanding and recognizing the potential linkage between terrorism and transnational organized crime. A multi-sectoral or multi-entity approach is needed and should include law enforcement and the prosecutor's office, as well as the judiciary, prison and probation services, intelligence agencies, financial intelligence units, border security (including customs), and other relevant governmental authorities involved in preventing and combating terrorism and transnational organized crime.

Given the high level of expertise needed for an effective law enforcement response to certain crimes, States are recommended to set up dedicated police units – where such units do not exist – with qualified staff to effectively prevent, detect, and prosecute, for example, illicit trafficking in cultural property or wildlife crimes with a possible link to terrorism.

Parliamentarians can play a role to ensure that international conventions the State is party to and binding UNSC Resolutions are duly implemented in domestic legislation within a rule of law framework and in accordance with international law.

Considering partnerships between criminal justice authorities and the education sector, including academia and think tanks, is also important. Primary and secondary educational institutions have successfully worked on preventing both violent extremism conducive to terrorism and recruitment by transnational organized criminal groups. Examples of successful practices include joint activities with teachers, teacher training centers, and policymakers, using varied resources such as dialogue, educational tools, and games. Evidence-based policymaking is crucial to identify possible linkages and develop effective countermeasures, and the role of academia in advancing and publishing relevant research in this regard is key.
Good Practice 2: Developing and Strengthening Public-Private Partnerships and the Role of the Private Sector in Prevention

Given the primary responsibility of the State in counter-terrorism related activities, Governments are recommended to develop close partnerships with the private sector, as these may be conducive to crime prevention. A particular recommendation for private sector organizations in this respect is to exercise due diligence in their actions. States should draw upon the expertise and, where possible, support the capacity-building efforts of multilateral organizations with experience in this area, such as the UNODC.

Museums, art dealers, auction houses, and other cultural institutions can assist, for example, by compiling up-to-date inventories of all cultural property in their possession, updating lists and directories of stolen art, and reporting stolen cultural property. Those buying and selling art and cultural property should refuse to buy or auction goods of dubious provenance and should subsequently and without undue delay notify law enforcement authorities, when they are offered these goods. In some countries, art dealers and auction houses are, under penalty of criminal sanctions, required by law to exercise due diligence. This obligation is consistent with principles of the UNESCO 1970 Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property, the UNIDROIT 1995 Convention on Stolen or Illegally Exported Cultural Objects, and, in the European regional context, the Council of Europe 2017 Convention on Offences relating to Cultural Property. Furthermore, unbiased experts from universities, museums, or cultural institutions can play a role in researching certificates of provenance and expert reports where appropriate in accordance with international standards. Law enforcement authorities and relevant experts may in turn assist museums, art dealers, collectors, auction houses, and other cultural institutions by providing them with lists of suspect regions under control of terrorist organizations, from which cultural property may be illegally excavated or stolen and then exported and transferred onto the art market. In addition, INTERPOL’s Works of Art Unit has formed an extensive network of contacts with museums and auction houses and maintains the Stolen Works of Art Database. The Unit is also active in conflict zones in order to collect information directly from the places of origin of items of cultural property.

Insurance companies can also play an important role in prevention, due to the precautionary requirements they set as conditions for insuring goods, events, or travel of ships in regions prone to piracy or maritime crimes. Vessels traveling through waters where the risk of maritime crime including but not limited to piracy is high may, for example as a condition for a lower insurance rate, be required to stick to the assigned sailing route, where marine naval vessels patrol.

The financial sector, in particular banks, is well positioned to help prevent the commission of (or attempts to commit) illegal activities by transnational organized crime networks or terrorist groups, such as financing of terrorism, corruption, and money laundering, by imposing strict controls in accordance with domestic law and regulations on transactions above a certain threshold or by preventing transactions in cases of suspected criminal activities. Factors that can be taken into account include the nature, scale, diversity, and complexity of their business; their target markets; the number of customers already identified as high risk; the jurisdictions to which the bank is subject to, either
through its own activities or the activities of customers, especially jurisdictions with relatively higher
levels of corruption or organized crime, and/or deficient anti-money laundering and countering the
financing of terrorism (AML/CFT) controls, as determined by the Financial Action Task Force (FATF). In
addition, financial institutions can monitor distribution channels, including whether the bank deals
directly with the customer or relies (or is allowed to rely) upon third parties to conduct customer due
diligence. Examples of monitoring the distribution channels include confirming the identity of the
account owner (the customer) and taking reasonable measures to verify the identity of the beneficiary
(the recipient of the transaction) by using reliable independent sources, as well as obtaining
information on the purpose and intended nature of the business relationship and performing ongoing
due diligence and scrutiny of the transaction. Furthermore, after considering the usual activity and
profile of their customers, financial institutions can assess internal audit and regulatory findings, as
well as the volume and size of transactions. These monitoring activities can deter criminal activity.
States should, however, be aware of the potential impact of onerous banking regulations on legitimate
civil society organizations. Laws and regulations should align with the best practices of FATF
Recommendation 8 on non-profit organizations and make use of a risk-based approach to protect
non-profit organizations from terrorist financing abuse. The FATF style regional bodies support
member states in the implementation of effective AML/CFT measures in a manner that respects
human rights. Multi-stakeholder dialogue processes, inclusive of civil society, should be established as
part of responsive and robust mechanisms for review and remedy.

Internet service providers (ISPs), including social media intermediaries, provide powerful tools, such
as end-to-end encrypted communication tools, geo-spatial imaging, and other open-source
information, which enable coordination among transnational organized crime networks and terrorist
groups for illegal purposes. ISPs are therefore well positioned to prevent such criminal activities on
their platforms and render timely assistance to law enforcement investigations related to
transnational organized crime with links to terrorist groups. They should comply with applicable data
retention regulations and could assist by setting up, consistent with their terms of service, automated
analysis tools to detect and remove from their platforms criminal activities related to terrorism and
transnational organized crime and by notifying, without undue delay, concerned law enforcement
agencies.

States are recommended to make it a legal obligation under domestic law that manufacturers and
importers of firearms mark the items appropriately at the time of manufacture or to consider similar
legal obligations for import by keeping respective records to allow tracing of illicitly trafficked firearms
to identify the point of diversion. Furthermore, companies involved in firearms transactions can play
a role in keeping records of transfers and the accompanying documentation to increase the
transparency of arms trade and in preventing firearms from falling into the hands of transnational
organized criminal networks or terrorist groups.

The private sector is also well positioned to share information with law enforcement authorities on
certain specialist knowledge, such as on financial transactions, or recognized illicit trafficking of natural
resources and wildlife and cultural property. Considering the important role the private sector can
play in prevention (as well as in detection and investigation by providing expert witness statements),
States are encouraged to establish strong public-private partnerships. In this respect, all relevant
stakeholders are recommended to take the UN Guiding Principles on Business and Human Rights into account.

**Good Practice 3: Improving Protection Measures to Prevent Illicit Trafficking of Goods**

An important aspect of effective prevention includes developing or strengthening protection measures against illicit trafficking of goods by terrorists or transnational criminal networks. Protection measures function as an extra lock on the door and can have a deterrent effect. For example, sufficiently staffed border checkpoints which are well-equipped with the necessary technology to inspect travel documents and identities of travelers, as well as the possibility to scan the content of cargo, may function as an important deterrent.

Another important tool can follow from regulatory control and tracing mechanisms such as those listed in the Protocol to the UNTOC against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition, the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects, and the International Tracing Instrument, which facilitate adherence to import and export controls related, for example, to trafficking in firearms. Such export controls include issuing and control of end-user certificates for SALW. Secure stockpiles of firearms can also prevent their loss, theft, and diversion in the first place.

Protection measures relevant to preventing illicit trafficking in cultural property can benefit from identification of cultural property, as well as from a harmonized description and codification system, for example by meeting the requirements of the INTERPOL Stolen Works of Art Database or by using technology such as the ID-Art app of the INTERPOL Works of Art Unit. Making use of such a codifying system can assist museums, art dealers, auction houses, and other cultural institutions in maintaining inventories of cultural property and in reporting stolen goods. These inventories can subsequently be consulted by museums, art dealers, auction houses, or other cultural institutions, when they are offered goods for purchase or sale, or by customs or law enforcement authorities to identify the provenance of the goods or check whether they are stolen. Meanwhile, States need to be aware that illegally excavated cultural property is generally not registered in databases of stolen objects, since it was removed without the knowledge of the state of origin.

Considering the deterrent effect of such protection measures, States are recommended to improve them to prevent trafficking of goods by terrorist groups or transnational criminal networks or by transnational criminal networks working closely with terrorist groups.

**Good Practice 4: Developing Solid Mechanisms to Prevent Corruption and Protect Whistleblowers**

Corruption undermines democracy, human rights, and the rule of law. Corruption thrives, where institutions are weak and ineffective. This further facilitates terrorism and transnational organized crime. Corruption can take different forms, such as bribery, embezzlement, abuse of authority, laundering of proceeds of crime, concealment, and obstruction of justice, and may occur in both the public and the private sector.
To facilitate their illicit activities, some terrorist and transnational criminal networks may resort to bribing public officials, such as customs or border control and law enforcement officials, to obtain documents and permits, circumvent security checks, bypass arms control, or evade prosecution. In case of significant risk of corruption, these “integrity gaps” may even hinder the proper development of risk assessments. Corruption in the private sector, which may include accountants, lawyers, and trust and company’s service providers, may be used to generate funds to finance terrorist groups. It is recommended to consider developing legislation or other mechanisms that provide for regular oversight, such as audits, into sectors vulnerable to abuse.

It is therefore important that law enforcement authorities, customs and border agencies, and other agencies authorized to issue official documents such as travel documents or export and import permits strengthen their awareness regarding this potential risk and take precautionary measures to increase resilience in their organizations, by training officials regularly to recognize the signs and resist corruption. Good practices in this respect also include scrutinizing new employees, dividing responsibilities, applying the principle of multiple control, transparency and accountability of financial management, public procurement, the development of a code of conduct, and establishing internal and/or external oversight mechanisms, such as an integrity commission or inspector. Developing and maintaining digitalized registries for seized and confiscated items can also help prevent their diversion by corrupt authorities.

Whistleblowers may be an important source of information, which allows law enforcement agencies to detect and investigate corruption that facilitates terrorism and transnational organized crime-related offences. Whistleblowers are individuals working in the public sector or at private organizations who disclose legal or regulatory violations committed at their workplace, including corruption, to the authorities or the media. By doing so, they may put themselves at risk in terms of their job security or career opportunities or may even endanger their own and their family’s physical security. To facilitate legitimate reports, various channels ensuring confidentiality can be established. Examples of such reporting channels include telephone hotlines, mobile phone apps, web-based solutions, or other interfaces allowing confidential or sometimes anonymous reporting, internally or to an external supervising authority. States are recommended to establish appropriate legal frameworks to establish and facilitate reporting corruption. In addition, States should ensure that sufficient means are available to provide whistleblowers with protection from potential retaliation or intimidation through appropriate mechanisms, for example by offering physical protection, if necessary by relocating them and by shielding their identity, and by developing evidentiary rules to permit them to give testimony or share information in a manner that protects their safety. Protection afforded to whistleblowers should, however, be consistent with fair trial guarantees for defendants, including the right to examine or have examined witnesses against them and to examine witnesses on their behalf under the same conditions.
II. Detection

Good Practice 5: Making Risk Assessments to Understand the Linkages between Transnational Organized Crime and Terrorism

Using research and risk assessments can help in identifying context-specific indicators, which can function as early-warning indicators and as such can assist in understanding, investigating, and prosecuting terrorism and transnational organized crime-related offences and in allocating resources to where they are needed most. Some of these specific dynamics and characteristics include the organizational structures of the groups, the regions in which they operate, or the use of communication channels and techniques. In some regions, for example, criminal networks, particularly those related to organized criminal groups pursuing financial or other material benefits, do not consider liaising with terrorist networks opportune, because that would likely lead law enforcement attention to pay more attention to their own criminal networks as well. In other regions this is not the case. In regions where terrorist organizations can operate fairly undetected, they might, on the other hand, even use the lack of government control to set up illegal taxation systems to fund their operations. Transnational criminal networks that traffic cultural property illegally may use social media to create a demand for the cultural property even prior to excavation. This specific characteristic shows the importance of monitoring publicly available social media postings to detect these individuals and networks, after which a full criminal investigation can start. It is therefore recommended that States invest in developing and using risk assessment tools to facilitate understanding of any linkage between terrorism and transnational organized crimes and develop indicators.

Good Practice 6: Strengthening Institutionalized Methods of Comparing and Analyzing Data, Patterns, and Trends

An important instrument in understanding patterns and trends and making context-specific risk assessments is the use of (inter-agency) databases, including those recording financial transactions. Sharing appropriate information between appropriate law enforcement agencies in accordance with domestic law, and, if appropriate, with FIUs, tax offices, custom and border control agencies, as well as between States, is therefore a crucial step toward setting up institutionalized methods to compare and analyze these databases. States are encouraged to strengthen the capacity of frontline officers to collect relevant data and make use of the available databases and improve, where applicable, the usability and interoperability of databases. Particularly when data are shared for the purpose of starting a criminal investigation, a proper legal basis needs to be provided. In all situations, States should comply with international law, including international human rights obligations and applicable domestic legislation on data protection.

Subsequently, agencies and frontline officers should have the authority, capabilities, and skills to use these databases effectively. States should therefore invest in improving the IT infrastructure and should provide training on relevant issues, including deep-web monitoring, tracing and seizing of virtual currencies, and big data analytics, as well as the appropriate use of emerging technologies consistent with applicable international law, including international human rights obligations, and
relevant domestic data protection laws and policy. Developments in new technologies, for example those developed by research institutes and universities (e.g., the datamining capacities of artificial intelligence) offer possibilities for analyzing big data. In addition, open-source intelligence provides a great resource for analyzing and detecting trends and the organizational structure of transnational criminal networks. For example, transnational criminal networks may use social media to find buyers for stolen cultural property.

Data collected by these agencies can moreover contribute to trend analysis and foresight studies. Trend analysis can facilitate understanding patterns of behavior of terrorist and transnational criminal networks, *modi operandi*, and trafficking routes, may thus provide crucial information for prevention, detection, and investigation, and should be shared with relevant governmental agencies and frontline officers. Since the environment in which terrorist and transnational criminal organizations operate is dynamic, and these organizations adapt to changing circumstances, foresight studies can moreover provide insight into how patterns of behavior of these organizations are likely to change in the future.

In collecting, analyzing, and sharing data, States are recommended to install quality assurance data reviews. States should moreover refrain from ethnic profiling in data analysis and abide by their relevant international obligations on privacy or data protection obligations, which may include conducting assessment of reasonableness or necessity and proportionality. States are furthermore recommended to install adequate safeguards against abuse, including independent and effective oversight covering all relevant activities and transparency of the database functioning and management, and formulating grounds and procedures for the data removal. States should be particularly prudent with regard to collecting, storing, and sharing data on children, with the best interest of the child as a primary consideration.

**Good Practice 7: Promoting Availability of Tracing and Surveillance Instruments**

There are tracing and surveillance instruments that are directly aimed at identifying individuals, instruments that indirectly identify these individuals, and instruments that detect illegal goods.

Basic instruments to verify the authenticity of travel documents and to check the identity of travelers against watchlists belong to the category of instruments that play a crucial role in detection and even play a role as deterrents. States should make available tracing and surveillance instruments and technical equipment to detect individuals who use a false identity or stolen or falsified travel documents. INTERPOL provides a useful tool in this respect with the Stolen and Lost Travel Documents Database. In addition, collecting, storing, and comparing biometric data of passengers, such as facial recognition, in a manner compliant with international and domestic law, provides a still more advanced instrument to detect travel by terrorists and persons involved in transnational organized crime. In this respect, the use of advance passenger information (API) and passenger name records (PNR) are also considered to be important tools for tracking and detecting air passengers. States should moreover refrain from using these tools in a manner that leads to ethnic profiling.

In vast areas where physical detection is difficult, the use of unmanned aerial vehicles or drones can fulfill an important function. Good practices developed to detect poachers make use of GPS trackers
on wild animals or thermal imaging to monitor their movements. The data these instruments transmit can help detect perpetrators indirectly and may also work as a deterrent.

To detect illicit trafficking of goods connected to terrorism or transnational organized crime, checking whether the import and export of certain goods is legal, and whether these goods are listed as looted or stolen is also important. For example, authorities can consult the International Council of Museums’ Red Lists to identify cultural property categories specifically targeted by illicit trafficking. States are moreover encouraged to promote the use of INTERPOL’s Database on Stolen Works of Art, which contain certified police information on stolen and missing art objects provided by authorized entities.

By adopting international best practices on marking and keeping records of firearms and through international cooperation and assistance on marking and tracing, States can trace seized weapons and identify potential arms traffickers more effectively.

Whilst increased use of surveillance techniques has assisted law enforcement in detecting terrorism-related and transnational organized crime-related offences, States should respect international human rights law, including the right to be free from arbitrary or unlawful interference with privacy, and uphold applicable domestic data protection laws, while utilizing these techniques.

Good Practice 8: Strengthening the Role of Customs and Border Control

Customs and border control play a key role in detecting cross-border movements of individuals related to terrorist groups and transnational criminal networks. Particularly long, porous borders and areas affected by violence and instability are a potential vulnerability in an effective law enforcement response.

Maritime border security also plays an important role in preventing, detecting, and countering abuse of the maritime domain for conducting potential attacks or illicit travel or trafficking.

With respect to detecting the movement of individuals related to terrorism and transnational organized crime, customs and border control agencies are recommended to encourage the use of INTERPOL’s Stolen and Lost Travel Documents Database, and are recommended to use API and PNR in accordance with UNSC resolution 2396 (2017), UNSC resolution 2482 (2019), and applicable privacy or domestic data protection law and policy. Instruments such as the Container Control Programme, established by UNODC in partnership with the World Customs Organization can play a role in intercepting illegal movements of drugs and other goods. States should raise awareness among border and customs officials, support the efforts of the UNODC and other international organizations with the mandate to provide technical assistance in this area in building practitioner capacity to detect terrorism and transnational organized crime-related offences and should provide the necessary equipment.

In addition, customs and border control agencies are well placed to collect relevant data on certain movements and feed them back into up-to-date risk assessments. They can, for example, gather information on how transport systems such as donkeys and small vessels are used to smuggle goods
in porous border and coastal areas. The World Customs Organization publishes illicit trade reports on trends in illicit trafficking in different kinds of goods annually.

Finally, customs and border control agencies are also well-positioned to detect and disrupt illicit financial flows, as they present at the border. This includes trade-based money laundering, recognized globally as an effective process for terrorist financing and resourcing and bulk cash smuggling. The role of customs and border control agencies can be strengthened through multinational operations such as the WCO/INTERPOL Operation Tentacle or development of an integrated border strategy and multilateral efforts such as the UNODC Container Control Programme.

**Good Practice 9: Building and Strengthening Public-Private Partnerships in Detection**

In some cases, the private sector has information that may be conducive to detecting terrorist and transnational organized crime-related offences. Given their primary responsibility in this matter, States should therefore invest in strengthening public-private partnerships in detection. Particularly private sector organizations, such as museums, art sellers, auction houses or other cultural institutions, and wildlife conservation foundations, are often the first to detect the illegal activities. Financial resources are largely transferred through regular bank accounts from those buying illegal goods to those trafficking them, from commanders in a terrorist organization to planners or executors of terrorist plots, from supporters of terrorist organizations to the network or individuals to finance their travel. Financial data can help detect the amounts transferred, the individuals, (shell) companies, or NGOs between which the transfer takes place, their relationship, and the trail of ATM money withdrawals, which can map individual travel. By building in red flag indicators to detect suspicious transactions, financial institutions can play a role in detecting patterns related to terrorism and transnational organized crime-related offences, which is of great value to law enforcement authorities. Public-private partnerships benefit the work of customs and border agencies significantly as well. Furthermore, in line with relevant UNSC resolutions, FATF recommendations and applicable domestic law, financial institutions should be required by law to inform the FIUs promptly about suspect transactions. Meanwhile, States need to be aware that terrorists often use the underground economy or informal trade channels and not necessarily the banking sector to finance their actions. The major difficulty for financial intermediaries lies in the low level of financial flows, which often cannot be detected by means of the thresholds recorded in transaction monitoring systems. Another difficulty is that often the source of funds used to finance terrorism is legal and goes unnoticed.

**III. Investigation**

**Good Practice 10: Strengthening Multidisciplinary and Multi-Agency Coordination and Analysis**

Facilitating effective coordination between the specialized counterterrorism bodies and those dealing with organized crime is important. Updating legislative and procedural frameworks may be necessary to ensure complementarity of the procedural laws covering the mandates of the different law enforcement units, the jurisdiction of the courts, and the rules governing information sharing and coordination.
In situations where linkages are suspected between terrorism and transnational organized crime, it is important to gather the relevant expertise within the police and investigative authorities and to ensure that relevant agencies with different mandates are able to join forces as appropriate, to strengthen the investigation capacity of the State as well as for the prosecution. In principle, investigations should be proactive and guided by criminal investigative information.

In some countries setting up ad hoc or permanent multidisciplinary teams, such as task forces, has proven useful to understand better the complexities of the linkages between terrorist and transnational criminal networks and to facilitate information sharing. States are therefore recommended to consider the establishment of such teams. In some cases, this means bringing together investigation experts from fields that have a stand-alone status, such as drugs and terrorism or weapons and terrorism, to reflect on the crosscutting nature of these forms of criminality. In other cases, it means integrating or making available experts specialized in e.g., illicit trafficking in wildlife, natural resources, or cultural property in counterterrorism units. As part of this broader perspective on the investigation of crimes that have linkages with both terrorism and transnational organized crime, States are recommended, when appropriate, to add expertise on investigation into corruption, money laundering and illicit financial flows, or obstruction of justice to that on terrorism and transnational organized crime.

Even in situations where multidisciplinary cooperation is less institutionalized, organizing technical meetings or sharing a physical workspace proves beneficial for exchanging knowledge and information. States are also recommended to establish effective lines of secure communication, such as through the introduction of an encrypted mobile app as a criminal information management system for the relevant agencies and between the different field offices to facilitate secure exchange of information. Multilateral organizations such as INTERPOL and UNODC have resources that may assist in these cases.

In some cases, facilitating multi-agency investigation or multi-agency coordination might be important. The relevant agencies might each have their own mandate and expertise that contributes significantly to crime investigation. In the case of maritime crimes and piracy with connections to terrorism and transnational organized crime, for example, an integrated investigative approach might utilize simultaneously the expertise of border and customs authorities, FIUs, as well as the coast guard and the military. To ensure effective multi-agency cooperation, investing in trust-building and mutual understanding of different corporate institutional identities and modi operandi among the different agencies in the partnership is important. This is especially relevant in cooperation with intelligence services. In all cases, including multi-agency investigations or coordination, respecting all applicable domestic substantive and procedural laws is important, as are fair trial guarantees with respect to the rights of the defendant, in conformity with applicable international human rights obligations.

**Good Practice 11: Encouraging Police-to-Police Cooperation and Mutual Legal Assistance**

Terrorism and transnational organized crime are often committed with a cross-border element. Trafficking illegal goods might take place between two or more countries, while the money flows to an additional country and ultimately finances a terrorist organization in yet another country. Potential
terrorist buyers of illegal SALW might be abroad, for example, as intermediaries or brokers of the illegal deal might be as well. Obtaining a proper understanding and gathering evidence of the crime and the underlying facilitating network may necessitate international police cooperation and mutual legal assistance during the investigation phase, including upon the basis of reciprocity. States should develop mechanisms and proper legal frameworks to enable, as appropriate and consistent with domestic law, police-to-police cooperation and mutual legal assistance between two or more countries to facilitate questioning of suspects and witnesses (via video/telephone conference when permitted by domestic law or in person), search and seizure of communication data, real-time interception of communications, or collection and transfer of evidence. In doing so, States should respect the individual’s right to be free from arbitrary or unlawful interference with privacy, including when data are exchanged. States should also respect obligations regarding fair trial guarantees for defendants and other applicable domestic law protection when questioning victims, witnesses, and suspects. Respecting human rights and fundamental freedoms is of utmost importance to both the sharing of information within a State between different intelligence, law enforcement or other relevant authorities, as well as between different States. States can rely on formal judicial and law enforcement or intelligence cooperation tools for the exchange of information or share information on the basis of reciprocity or on an ad hoc basis. In particular Article 15 of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, prohibits the use of any statement established to have been made as a result of torture as evidence in any proceedings, except against a person accused of torture as evidence that the statement was made. In case a State has genuine concerns as to how the information will be used in another country, States are recommended to share the information conditional on strict assurances that the information provided will not result in any human rights violations or abuses.

To facilitate cooperation between States, States should consider ratifying and implementing relevant conventions that provide a legal basis for law enforcement cooperation in criminal matters. This legal basis can be found in various counterterrorism conventions, as well as in the UNTOC, and the Protocols thereto, and in other relevant international conventions that provide a legal basis for mutual legal assistance or by concluding a bilateral agreement. In the absence of legislation specifically permitting MLAs or agreements addressing the same. States are encouraged to provide each other with assistance on any available legal basis, including, where permitted, notably on the basis of reciprocity. Moreover, the existing international conventions on MLA should not hinder States from using other expedited MLA procedures where appropriate. Furthermore, appointing police liaison officers in foreign jurisdictions may establish a relationship, which will facilitate formal police-to-police cooperation.

Furthermore, States are recommended to use platforms and strengthen their cooperation with regional and international institutions of which they are members. Through cooperation within such institutions, arrangements already exist regarding, for example, information exchange, provision of operational analysis in support of operations, appointment of liaison officers or focal points, or assistance through expertise and technical support.

Subject to national legislation, setting up joint investigation teams (JITs) concerned with specific investigation of a case with transboundary elements is a good practice during the investigation phase
in appropriate cases. JITs can be enabled by an international agreement, on a case-by-case basis, or follow pre-set models and arrangements to facilitate strategic and operational technical assistance in evidence gathering and analysis. They can be used to share information and coordinate between States and other actors, for example between source countries, countries from which operations are coordinated, transit countries, or destination countries. Considering the differences between legal obligations and frameworks of States involved in an investigation, deciding how to share evidence within the framework of a JIT, as well as how to develop an evidence grid to provide clarity on the different evidentiary thresholds for the crimes involved, might also be helpful.

**Good Practice 12: Enhancing the Use of Special Investigation Techniques**

Considering the often sophisticated levels of communication between members of terrorist and transnational criminal networks, special investigation techniques can play an important role in unraveling the networks and the complex infrastructure of the organization behind these terrorism and transnational organized crime-related offences. Special investigation techniques can include physical and electronic surveillance, use of Trojan software, undercover operations, use of informants and confidential sources, phone and computer analysis, and financial intelligence investigation. If resources for organizing physical surveillance or undercover operations are scarce, searches of phones and computers pursuant to a judicial warrant can already generate a lot of information on e.g., wildlife crime. As already highlighted in UNTOC, States are therefore encouraged to make appropriate use of special investigative techniques; at the same time, they need to ensure that these special investigative techniques are applied in accordance with domestic law and adequate oversight of its implementation. Moreover, the use of undercover agents, informants, or confidential sources may present challenges at the prosecution stage, including the need to protect the identities of such individuals. Fair-trial guarantees need to be observed when making use of testimonies from informants and sources. In addition, clear operational guidelines and training are needed when using special investigative techniques. Prosecution and remedial measures should take into account gender differences and gender dynamics where appropriate and consistent with equality before the law.

Another investigative technique, which is also addressed in the 1988 Drug Convention and the UNTOC, is the use of controlled delivery, where, subject to national legislation, investigative authorities consciously facilitate passage of the illicit goods under law enforcement supervision, within the transnational criminal network and from suppliers to potential buyers, with clear objectives, including discovering the network and individuals involved in these crimes and the trade routes used. Controlled deliveries are used to trace, for example, illicit trafficking in drugs, wildlife specimens, weapons, and cultural property. Given the potential risk of losing control of these goods, law enforcement needs to exercise great caution during controlled deliveries or should take measures to mitigate the risk involved, to the extent authorized by law.

The use of investigative measures should have a clear domestic legal basis and should be used strictly in accordance with applicable international law and should not be executed without appropriate oversight.
Good Practice 13: Strengthening the Use and Capacity in Financial Investigation

Terrorist and transnational criminal networks use multiple channels to move their finances, while trying to conceal the source or destination of the funds. This can be done by setting up shell companies or sham/ front charity organizations, abusing legitimate charity organizations without their knowledge, or using prepaid cards and mobile-payments, virtual assets, online money remitters, informal money value transfer systems, cash couriers, and other methods to transfer funds. In compliance with inter alia multiple UNSC resolutions, such as 1267 (1999) and 1373 (2001), it is important that States take action to cut networks from their financial resources to dismantle the criminal activity.

Financial investigation of terrorism and transnational organized crime-related offences are of great importance to provide insight into the infrastructure of the organizations behind the crimes and the money flows. In addition, in some cases, financial investigations can provide evidence linking terrorism-related offences to transnational organized crime-related offences. Financial investigation involves collection, collation, and analysis of all available information, with a view towards assisting in identification and/or prosecution of crime and in confiscation of the proceeds and instrumentalities of crime. Financial investigation is focused on finding the money trail that can help identify additional offenders and potentially locate evidence and instrumentalities used to commit the crimes. In investigations of terrorist financing, non-financial information (e.g., phone numbers or email addresses) contained in financial documents can provide vital intelligence for mapping networks of relevant individuals and entities. As FATF specifies in a report on operational issues in financial investigations, this type of intelligence can prove even more important than its initial evidentiary value. Meanwhile, States need to ensure that a legal basis is provided for the financial investigation, and that it is executed in full respect of human rights obligations and applicable domestic and international privacy protection.

In line with the UNSC resolutions, FATF recommendations and applicable domestic law, States should develop investigative expertise to pursue terrorism financing and money laundering crimes. Competent authorities, such as tax authorities or anti-corruption enforcement authorities, can also play an important role in financial investigations. Good practices include establishing a strategic coordinated approach to financial investigation, which can start with specialized training of investigators, analysts, and prosecutors, and strengthening cooperation agreements involving multiple agencies, including FIUs. Furthermore, States should reinforce access to the information and the capacity of their FIUs to analyze terrorism-financing by developing risk indicators with the competent authorities. States should ensure that their regulatory framework allows financial institutions to file suspicious activity reports (SARs) efficiently. This mechanism is vital for collecting, analyzing, and disseminating financial intelligence required for countering illicit financial activity by terrorist and transnational organized crime groups. The financial data processing mechanism should allow representatives from a variety of industries to send and receive secure messages and issue advisories and system updates to the user community. Record-keeping and reporting actions shall also be secured for investigation purposes.
In principle, FIUs, in accordance with their legal mandate, should not only share financial intelligence reports with law enforcement agencies upon request but should also pro-actively share suspicious transactions and activities with law enforcement agencies. States are recommended to facilitate cooperation involving their FIU and others, FIUs and law enforcement agencies, and FIUs, law enforcement agencies, and financial institutions. For example, States could establish a Countering the Financing of Terrorism Taskforce to implement the international standards of AML/CFT.

**Good Practice 14: Cooperation with Private Sector in Investigation**

Information obtained lawfully from the private sector can play a crucial role in providing insight into e.g., money transfers and financial flows within transnational criminal networks, which banks, accountants, and insurance companies can provide. These financial institutions furthermore have to play a role in freezing funds based on UNSC resolutions 1267 (1999), 1373 (2001) and subsequent resolutions or based on criminal confiscation orders. States are recommended to strengthen financial regulatory frameworks and these partnerships prior to the investigation, so that these regulatory frameworks can be useful during the investigation and prosecution phase.

Other modalities that are used to raise funds include crowdfunding, online fund-raising activities, use of virtual assets, and blockchain technologies. States should enhance direct cooperation with Internet Service Providers and request information pursuant to domestic legal processes to preserve electronic evidence but also to detect illegal activities on the web in accordance with applicable domestic law, including due process requirements and applicable privacy or data protection regulations, and international human rights obligations.

**IV. Prosecution**

**Good Practice 15: Enhancing the Legal Framework**

To combat terrorism and transnational organized crime successfully, States should have an adequate legal framework in place that allows for prosecution of terrorism and transnational organized crime-related offences. States should ratify and implement the relevant existing international instruments pertaining to terrorism and transnational organized crime to ensure that the international legal framework concerning such crimes is effective.

Furthermore, States should regularly conduct assessments on the implementation, submit periodic reports and actively participate in applicable review mechanisms, and seek and/or provide technical assistance in order to enhance and strengthen the legal framework (of other States). States could also as part of reviewing their counterterrorism and/or organized crime strategy assess whether there are any gaps in the implementation of the relevant conventions.

In addition to ratifying or acceding to UNTOC and the three supplementary Protocols thereto, as well as UNCAC, States could further strengthen the legal framework by adhering to relevant regional anti-money laundering conventions and other international standards concerning anti-money laundering and countering the financing of terrorism, including recommendations issued by the FATF. States
should also consider, as appropriate, ratifying specific conventions and protocols and adopting legislation that criminalizes forms of trafficking on which terrorist organizations tend to rely (e.g., illicit trafficking in drugs, firearms, natural resources, and cultural property), such as the 1988 Convention against Illicit Trafficking in Narcotic and Psychotropic Substance and the UNESCO 1970 Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property.

Furthermore, States should consider ratifying the main international human rights and international humanitarian law conventions and regional human rights conventions and ensure that relevant provisions are implemented domestically. This would enhance the domestic legal framework and could enable greater protection of human rights when addressing the linkage between terrorism and transnational organized crime.

Considering the impact of terrorism and transnational organized crime on society, States should not only criminalize the commission of the actual crimes themselves, but should also consider criminalizing all acts that knowingly or, if available under domestic law, recklessly facilitate transnational organized crime or the attempt to commit such crime. Criminalizing these acts allows for prosecution of the criminal system behind the crime, i.e., transporters, organizers and others that facilitate committing the crime, as well as lower-level criminals, such as poachers.

For example, UNTOC offers State parties two options for criminalizing participation in an organized criminal group. Some States criminalize the activities of an organized criminal group through the concept of conspiracy, prohibiting agreement to commit a specified crime. Other States criminalize such participation through the concept of criminal association, prohibiting intentional participation in the criminal group or its activities, be it through criminal or non-criminal acts. In addition, some States have criminalized the operation of businesses as part of an ongoing criminal enterprise, as well as crimes committed there, by introducing the offence of racketeering. When criminalizing and prosecuting these offenses, States should take care not to impose undue limitations on exercising the right to freedom of association.

Some countries impose a relatively short statute of limitations, for example for illicit trafficking in cultural property and natural resources. Where links exist between transnational criminal networks and terrorist groups, this additional complexity may present a challenge to prosecutors building a case and commencing prosecution in time. If applicable, States should consider extending or establishing longer limitations for bringing proceedings to allow successful prosecution of the crimes involved. Once it has been established that a transnational criminal group is linked to a terrorist organization, this could be pertinent for suspects that deliberately evade the administration of justice, especially for countries that do not allow for trials in absentia.

Transnational organized crime and terrorist groups can use corruption in both the public and the private sector to facilitate their criminal activities. States should, where appropriate, ensure effective implementation of UNCAC, including by enhancing their anti-corruption legislation, and ensuring that obstruction of justice is criminalized. For example, some States have criminalized intentionally and willfully providing false testimonies by officials and/or witnesses. Transnational criminal networks
have been known to obstruct justice by influencing or threatening witnesses as well as other actors involved in the judicial proceedings, such as law enforcement officials, prosecutors, and judges. In some States, protection is afforded not only to those involved in the judicial proceedings but also extended to journalists or public figures who may reveal criminal activities or other persons not directly related to the judicial proceedings. Depending on the local context, States could increase the penalties for committing and/or contributing to the offences of trafficking drug or arms, where such offences are committed for the purpose of terrorism.

Document fraud, such as theft of genuine documents, production of forged documents, or misuse of passports, also enables terrorism and transnational organized crime. States should consider criminalizing document fraud and identity theft, as well as all relevant forgery.

**Good Practice 16: Establishing Jurisdiction**

To be able to prosecute terrorism and transnational organized crime, States need to criminalize the relevant acts in their national legislation and establish jurisdiction. Jurisdiction can be established on the basis of various principles in accordance with relevant international law and domestic legislation. Especially maritime crimes and piracy committed on the high seas or in international waters can often trigger the involvement of multiple States claiming jurisdiction over crimes committed based on different principles. Where piracy is committed on the high seas, the universal jurisdiction principle can be applied, along with the flag state jurisdiction. Especially transnational activities of trafficking networks often touch the jurisdiction of several countries, for example when arms are shipped from one country to another by transiting countries in between. In these cases, States would have to consider whether there is a basis for jurisdiction as defined in their domestic systems.

When two or more States claim jurisdiction regarding the same offence, they are encouraged, when appropriate, to coordinate investigations and prosecutions.

**Good Practice 17: Developing a Comprehensive Prosecutorial Strategy**

When dealing with complex transnational criminal networks and terrorist groups, prosecutors are recommended to develop a prosecutorial strategy that yields the best possible result in the long run. This could mean identifying the critical nodes where the organization’s transactions are the most vulnerable or targeting the mastermind behind the criminal network. These individuals may be expected to bear the greatest responsibility for the crimes committed by the network. This may, however, prove more complicated than going after the “middlesmen,” such as transporters of illegal goods or those providing logistical support to arms traffickers, and secure a conviction for them. States should be encouraged to adopt measures through which the beneficial owners of assets can be identified. Prosecutors should in any case try to identify the different roles of perpetrators involved in trafficking crimes, for example poachers, transporters, intermediaries, and buyers, and should try to trace the trafficked items to their point of diversion or origin in order to investigate the network behind the individual offence.
States may consider to develop a separate strategy for children that have committed terrorist or transnational organized crime-related offences. When children are involved in these crimes, States should consider strategies that are in accordance with their applicable national and international legal obligations, including, as applicable, taking into account the best interests of the child as a primary consideration.

For those States that rely on prosecutorial discretion, prosecutors should take factors including the gravity and the nature of the crimes into consideration when exercising this discretion, in line with national norms concerning the functioning of domestic courts and judicial systems. Furthermore, prosecutors should exercise their discretion fairly, expeditiously, and impartially in the interest of justice. It is incumbent on the prosecutor to prove that a crime has been committed. Prosecutors may also want to make cumulative charges. For example, when illicit trafficking of cultural property is carried out with firearms, the accused could be charged with illegal possession of weapons, participation in an organized criminal group, and illicit trafficking of cultural property.

Each person in the chain may be charged with distinct offences. For example, some suspects may be prosecuted for isolated acts of looting or theft, whereas a transporter who knowingly facilitates illicit trafficking could additionally be charged with offences relating to involvement in the broader criminal aim. Depending on the approach taken by a State, whether it opts to criminalize participation in a criminal group through conspiracy (focusing on the wrongfulness of agreeing to commit a crime), criminal association (focusing on the wrongfulness of associating with those committing crimes), or racketeering (focusing on the wrongfulness of the ongoing criminal enterprise itself), different elements of the crimes need to be proven consistent with domestic legal requirements.

Considering the complexity and gravity of terrorism and transnational organized crime, prosecutors may want to request joinder of offences or defendants to prosecute the alleged crimes successfully. When terrorism and organized crimes have an international dimension, several suspects in different countries may be involved in the crime, and transferring the proceedings may be in the interest of justice and necessary to achieve successful prosecution on some occasions. States would need to adopt legislative measures to allow criminal proceedings to be transferred and could rely on the United Nations Model Treaty on the Transfer of Proceedings in Criminal Matters. In determining whether proceedings could be transferred, the competent authorities should consider the impact on victims, and that dual criminality is met and the principle of non-refoulement protected.

If appropriate, States should adopt incentives for the accused to cooperate with authorities in terrorist-related or transnational organized crime-related offences. If a person has voluntarily provided cooperation, prosecutors may, in accordance with domestic legislation, provide leniency or grant immunity from prosecution.

Finally, prosecution units specifically dedicated to transnational organized crime should not operate in silos and should avail themselves expertise from other prosecution units dedicated to terrorism or other relevant crimes. States are encouraged to facilitate coordination and establish channels of communication between different relevant governmental authorities within a country dealing with terrorism and transnational organized crime.
Good Practice 18: Strengthening Mutual Legal Assistance and Extradition (Judicial Cooperation)

Prosecution of suspects of terrorist and transnational organized crime-related offences can be strengthened, where applicable, by improving law enforcement, prosecutorial, and judicial cooperation. Where appropriate, this cooperation should also extend beyond criminal proceedings to a more strategic and tactical level. This is particularly important, since terrorism and transnational organized crime can be prepared in one country and managed from another in order to traffic goods from yet two further countries and perpetrated by nationals of numerous additional countries. Evidence and suspects in such cases are scattered in several countries. Cooperation can facilitate exchanging evidence, questioning witnesses, and making arrests, including those made pursuant to requests for extradition. Prosecutors are encouraged to reach out to each other through formal and, if permitted, informal channels to coordinate their efforts in practical terms, when several countries are involved in prosecuting the same crime or different members from the same terrorist organizations or criminal network to avoid gaps or competing requests for mutual legal assistance and potential double jeopardy issues, which in some contexts could be a ground for refusing extradition. Using informal channels could facilitate and expedite formal requests for mutual legal assistance and should respect the chain of custody. Communication between prosecutors should be encouraged, as it can help to facilitate the execution of mutual legal assistance requests.

States are encouraged to enhance cooperation on extradition and mutual legal assistance in accordance with domestic law and international counterterrorism conventions and other relevant conventions, such as the UNTOC and its Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition (2001), UNCAC, the 1988 Drugs Conventions, and the Second Protocol to the Convention for the Protection of Cultural Property in the Event of Armed Conflict, imposing the duty to submit the case to the relevant prosecutorial authorities for consideration, if an alleged offender is not extradited. The 1990 United Nations Model Treaty on Extradition may be an important tool for some countries in developing such international cooperation.

With respect to offences covered under the UNTOC, States have an obligation to provide each other with mutual legal assistance to the fullest extent possible. States are encouraged to ratify multilateral, regional, or bilateral conventions that provide a legal basis for mutual legal assistance and extradition if required and needed. Where permitted, States are also encouraged to provide mutual legal assistance on the basis of reciprocity. Additionally, law enforcement agencies are encouraged to exchange information through police-to-police cooperation.

In many jurisdictions mutual legal assistance and extradition are permitted, only if these offences are sufficiently criminalized by both States. Where necessary, States should establish appropriate offences and penalties, taking into account the gravity of the crimes.

When States receive a request for extradition of a person accused or convicted of a serious crime, the relevant authorities should consider, where appropriate, to extradite also when the crime has not been committed in the State requesting extradition, but the requesting State has valid jurisdiction ground under its national legislation and international law.
**Good Practice 19: Improving the Use of Different Types of Evidence**

Whilst transnational criminal networks and terrorist groups increasingly use the Internet to generate funds and finance their activities, prosecutors need to be able to handle electronic evidence in court. Prosecutors need to understand how to use digital forensics, how to evaluate electronic evidence, and how to preserve the validity, authenticity, and integrity of electronic evidence to ensure that it can be admissible in court. The right to be free from arbitrary or unlawful interference with privacy should be respected. As one example of potentially relevant considerations, prosecuting maritime crimes, whether it involves drug trafficking, illegal fishing, human smuggling, or piracy, normally requires that evidence should be collected at sea just after a ship has been lawfully boarded. Digital forensics can help extract relevant information from equipment on ships and assist in prosecution of maritime crimes.

States should also consider using forensic evidence, in particular relating to prosecution of certain offences that may be linked to terrorism and transnational organized crime, e.g., illicit trafficking in natural resources and wildlife. Forensic science can pinpoint where the animal or plant came from and how this relates to other shipments seized. This may help prosecutors identify the structure of the criminal networks behind the trade and prosecute the kingpin, in addition to a poacher caught red-handed.

Using expert witnesses is particularly important with respect to illicit trafficking in cultural property. To determine the authenticity and origin of cultural property, prosecutors could rely on expert witnesses. In some countries it is mandatory for the prosecutor to consult an expert when dealing with crimes relating to cultural property. Prosecutors may also consider using scientific methods to ascertain the provenance of cultural property.

Finally, intelligence is critical in the context of terrorism and transnational organized crime. Intelligence can provide useful insight into the structure of terrorist groups and transnational criminal networks. Subject to national legislation, States should establish mechanisms and procedures allowing the use of intelligence as evidence in criminal proceedings, while respecting international human rights obligations, in particular guarantees of a fair trial.

**Good Practice 20: Court Security and Witness Protection**

Prosecution of terrorism and transnational organized crime-related offences should be unhindered and free of interference. It is vital that all actors – victims, witnesses, informants, agents, juries, investigators, prosecutors, defense counsel, and judges – involved in prosecution of these crimes and in judicial proceedings are able to participate without fear of intimidation.

States should consider adopting measures that would enhance security in courthouses, when appropriate, while fully respecting for the rights of the accused. For example, trials may be held in courthouse facilities with extra security, security protection provided to judicial staff, and security threat assessments performed.
Witnesses play a crucial role in the investigation and prosecution of terrorism and transnational organized crime-related offences. Witnesses, informants, justice collaborators, and whistleblowers can be exposed to threats or intimidation or can be coerced to withdraw or falsify their statements. Some States have adopted measures that would provide physical protection to witnesses - both during and outside a criminal investigation - and establish appropriate procedural protection measures in court to enable witnesses to provide testimony. States are advised to establish sufficient witness protection programs to support and protect material witnesses in terrorism and transnational organized crime cases, as neither terrorist groups nor transnational organized networks will hesitate to harm or kill witnesses testifying against them. States should ensure that the right to a fair trial, in particular the right of the accused to examine the witnesses against him or her, are met in accordance with ICCPR Article 14 (3) (e).

Witnesses should be treated with respect and in a gender-sensitive, and non-discriminatory manner. When witnesses are also victims of crimes, they should have the right to seek an effective remedy from a competent judicial, administrative, or legislative authority. In accordance with international legal obligations and domestic laws, States should, where appropriate, provide for redress or reparations to victims of crimes, allow regular updates on the progress of the investigation and prosecution, and provide measures to protect their privacy and safety.

States should, while respecting international law and in accordance with domestic law, provide victims of crimes with support, protection, and access to compensation or restitution and, if permitted, enable victims to be heard during criminal proceedings. Some States have established a special victim support unit or liaison officer or have appointed a prosecutor to represent the victims. States could also provide assistance to victims and their families, including material, medical, psychological, and social support.

V. Sentencing, Rehabilitation, and Reintegration

Good Practice 21: Sentencing Considerations

The UN Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules) describe the main purpose of a sentence of imprisonment as protecting society against crime and reducing recidivism. States should ensure that conditions in detention respect the dignity of all prisoners. The severity of penalties available by law for those crimes linked to terrorism and transnational organized crime should reflect the gravity of these crimes. Parties to the UNTOC and to the 1988 Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances should comply with the treaty provisions in those instruments addressing punishment. In some jurisdictions, minimum sentences are prescribed for certain offences, such as drug trafficking. Several States allow for imposing cumulative charges on an accused for a number of different crimes for the same underlying acts.

In accordance with domestic law both aggravating and mitigating circumstances may merit consideration when deciding on a sentence. An aggravating circumstance might be the level of participation in a criminal group, illegal possession of a weapon, the impact of the crime on the economy or society, or a link between the crime and a terrorist organization, which could render the
punishment more severe. States could consider a connection with a terrorist offence involving organized crimes to be an aggravating circumstance in their criminal system. On the other hand, when a suspect has provided cooperation in the investigation and prosecution of a terrorist-related or transnational organized crime-related offence, this could be regarded as a mitigating circumstance, and may render the punishment less severe.

When determining a sentence, courts in some States may also consider other factors including means employed to execute the crime, level of cooperation in the investigation and prosecution, involvement in the offence and in the terrorist group or transnational criminal network, and, where appropriate, several individual circumstances, such as age, education, and social and economic condition of the convicted person. Furthermore, courts in some States may take into account prior convictions that are relevant to the current proceedings in their own country or in other states, while also taking into account that the person has already served a sentence for a prior conviction.

Good Practice 22: Strengthening the Use of Criminal Confiscation and Where Possible Non-Conviction-Based Confiscation

Conviction-based confiscation, also referred to as criminal confiscation or forfeiture, is the permanent deprivation of property or proceeds based on a court order following a criminal conviction. Criminal confiscation prevents terrorists and criminals from benefiting financially from illicit activities. Furthermore, confiscation can help undermine the source of funding of terrorist organizations and criminal networks.

Several international conventions encourage States to adopt measures to allow non-conviction-based confiscation (also referred to as non-conviction-based forfeiture). This might be relevant, for example, when conviction is not possible, because the accused person has died, when the accused is immune from prosecution, or when evidence to obtain a conviction is lacking. Generally, it enables lower standards of proof as well. Under certain circumstances, such as involvement in a criminal organization, some States provide a mechanism for reversing the burden of proof or allow enhanced or extended confiscation. This allows proceeds to be confiscated, even if they are not directly linked to the specific crime in which the offender has been convicted but clearly result from similar criminal activities. Note, however, that some States are precluded, on constitutional or other legal grounds, from instituting non-conviction-based forfeitures.

Other mechanisms include third-party confiscation, which allows the relevant authorities to confiscate property or proceeds belonging to a third party who knowingly acquired the property from a suspect with the intention of avoiding confiscation. Another very common and useful tool is freezing assets at an early stage on the basis of a court order or other competent order. The accused person does not lose the title over his property but may temporarily be prohibited from transferring, converting, disposing of, or moving the property. When firearms are seized or confiscated, States should trace them and take ballistic evidence in order to initiate investigations before destroying the confiscated items to prevent them from falling into the hands of unauthorized persons.
States could consider establishing dedicated units to oversee confiscations and develop procedures for identifying, freezing, and confiscating property and proceeds. These dedicated units could also assist with enforcing confiscation orders, managing confiscated property and proceeds, ensuring that third party rights are not violated, and facilitating effective cooperation with respect to property and proceeds located abroad.

Considering that organized crime and terrorism are frequently transnational, States may need to rely on mutual legal assistance to confiscate or freeze property located abroad. In some jurisdictions, a liaison officer, criminal justice advisor, or expert is seconded abroad to facilitate identifying, freezing, and recovering assets abroad.

Confiscation has an impact on property rights, which could also affect third parties. States should ensure that the right to a fair trial and all relevant due process guarantees under domestic law are respected.

Good Practice 23: Encouraging the Use of Risk Assessment in a Prison Context

A prison environment should provide security and safety to society, other prisoners, and the offender but should also provide a setting that supports rehabilitation and reintegration into society. However, due to the special environment, without responsible, effective and appropriate identification and monitoring of inmates who are susceptible to violent extremist ideologies conducive to terrorism, prisons can at times also be conducive to radicalization to violence and may be conducive to networking and skills transfer between terrorists and other criminals. These connections can help terrorists raise funds through illegal activities, ranging from petty crimes to trafficking in firearms or drugs. Furthermore, incarcerated criminals can be receptive to violent extremist views conducive to terrorism. A good example of detecting or preventing radicalization to violence conducive to terrorism amongst prisoners is setting up a hotline for prison staff or placing those suspected or convicted of terrorism-related offences in separate wings to prevent radicalization to violence of other prisoners.

Proper individual risk assessments are useful upon and during incarceration to determine the necessary security classification. Such risk assessments should be evidence-based and be conducted before or as early as possible during incarceration to demonstrate that restrictions placed on a prisoner are appropriate and should be reviewed by professional staff at regular intervals. Factors to be taken into account include criminal background, involvement in petty crime, membership of a criminal network or terrorist organization, relationships with others in and outside of prisons, and vulnerability to (further) radicalization to violence. They are particularly pertinent in preventing terrorists and other criminals from forging links within and outside the prison context and detecting them, when they occur. States are also encouraged to develop and use individual risk assessments that include any linkage between terrorism and transnational organized crime. The internal classification of a prisoner determines which prison regime will apply. When persons are convicted of transnational organized crimes with links to terrorism, they could, taking the individual circumstances into account, be placed in the same classification and prison regime as prisoners convicted of terrorism. States should also ensure that individualized risk assessments are performed, as described in the UN Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules).
**Good Practice 24: Improving the use of Prison Intelligence**

Prison intelligence can serve many different purposes related to managing internal security and safety within the prison, ranging from preventing escape, through detecting illegal activities within the prison, to maintaining safety and security for both prisoners and prison staff. Furthermore, prison intelligence can also help identify and prevent possible radicalization to violence in prison and determine whether any relationships are being established between terrorists and other criminals. Sharing prison intelligence with relevant governmental stakeholders outside the prison, such as law enforcement officials, prosecutors, and intelligence agencies, is moreover conducive to preventing prisoners (whether convicted terrorists or otherwise) from organizing crime-related activities directly or facilitating terrorist-related activities, such as providing access to forged documents, weapons, or money laundering networks.

Prison intelligence can be gathered both overtly through observation of convicted persons and voluntary interviews with prison staff and prisoners and covertly through the use of prison informants and listening devices, video surveillance, and interception of (e)mail. Considering the intrusive nature of covert surveillance, it should have a clear legal basis and sufficient safeguards in place to be consistent with the obligations of the State under its domestic laws and international human rights law, including respect for the right to freedom of opinion and expression, freedom of religion or belief, and freedom from arbitrary or unlawful interference with privacy.

To promote a consistent and systematic approach to prison intelligence, States should consider establishing a prison intelligence structure consistent with national legislation and appropriate best practices. States should develop a policy that is consistent with applicable international human rights law, to ensure that prison intelligence is collected, handled, used, and shared systematically. Prison staff, in particular prison intelligence officers, should be properly trained and have enough resources to be able to gather useful prison intelligence and establish mechanisms and protocols to ensure that all prison staff meet high standards of professional and personal conduct at all times.

**Good Practice 25: Developing Individual Rehabilitation and Reintegration Programs**

Safe and secure prison environments, adequately trained prison staff, and respect for domestic law and the human rights of prisoners are vital for rehabilitation programs to be successful. These programs should, where appropriate, take into account the specific needs of the individual, based on gender, age, and other relevant factors. Rehabilitation and reintegration programs for criminals convicted of terrorism or transnational organized crime may overlap but do not necessarily have to consist of the same measures. Whilst faith-based education and the use of influential persons, charismatic members of the community or other credible interlocutors may be useful for convicted terrorists, they may not be as effective for other convicted criminals. Rehabilitation programs should preferably start while serving a sentence and should respect freedom of religion or belief. In some countries, those who have been convicted of transnational organized crimes and are vulnerable to radicalization to violence conducive to terrorism are also able to join and benefit from rehabilitation programs specifically designed for convicted terrorists.
Some demobilization, disarmament, and reintegration (DDR) programs have been used to deal with transnational organized crime, in particular drug trafficking. In developing and setting up individual rehabilitation programs, prison staff should be cognizant of the linkage between terrorism and transnational organized crime and determine which elements are useful in the specific context.

States should also consider concluding multilateral or bilateral agreements that allow sentenced persons to be transferred in accordance with domestic law and international human rights law. One of the purposes of transferring a person to his or her home country is that this might contribute to successful rehabilitation and reintegration in society.