Abuja Recommendations on the Collection, Use and Sharing of Evidence for Purposes of Criminal Prosecution of Terrorist Suspects

Introduction

The Abuja Recommendations contained in this document were identified during an expert meeting held in The Hague and a review meeting held in Abuja, and are based on questionnaires and structured interviews with GCTF Members and content experts. With these Recommendations, the GCTF aims to support and complement existing work and initiatives by other international and regional organizations, namely the United Nations (UN) and other relevant stakeholders involved in this context.

The Abuja Recommendations build and elaborate on the GCTF *Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector (Rabat Memorandum)* as well as the GCTF *The Hague Memorandum on Good Practices for the Judiciary in Adjudicating Terrorism Offenses* and the GCTF *Recommendations for Using and Protecting Intelligence Information In Rule of Law-Based, Criminal Justice Sector-Led Investigations and Prosecutions*.

The aim is to offer recommendations to investigators and prosecutors of terrorism cases to help build a solid case based on strong and admissible evidence. The Abuja Recommendations are geared towards policy makers, law enforcement officials, and prosecutors.

Terrorists and terrorist networks are increasingly transnational in nature. Foreign Terrorist Fighters (FTFs) cross borders to join terrorist organizations in other countries, to relocate to new conflict zones or shelter places, or to return to their countries of residence. Furthermore, terrorist organizations often have members and cells in various countries, and use social media and the Internet to coordinate and communicate their actions, move financial resources and other assets across borders to support their activities, and use international criminal trafficking networks to raise funds and/or acquire weapons, skills, and explosives.

Due to the increasing complexity of terrorism cases, successful prosecution is both demanding and difficult. Overall, successful prosecution in terrorism cases requires intense coordination during the investigative phase related to the gathering of evidence and on the use of the general or specific investigative tools available.

Evidence in terrorism cases can sometimes be staggering in volume, encrypted or in a foreign language, classified or located in a conflict zone, or technically so complex that it requires forensic or technological experts. Other challenges that were identified during the first practitioners' seminar on 'Bringing Terrorists to Justice' organized by the United Nations Counter-Terrorism Executive Directorate (UNCTED) (s/2001/240) include investigation methods, international cooperation, protection of witnesses, and links between terrorism and other forms of criminality.

Frequently, due to the complexity of terrorist cases and the challenges of collecting admissible evidence, various prosecutorial strategies are followed, such as indicting terrorist suspects, including FTFs, for crimes including preparatory acts, terrorist crimes, and/or international crimes. In some

circumstances, ordinary crimes committed in a situation of an armed conflict can amount to war crimes.

In order to bring terrorists to justice it is important that admissible evidence should be used to the fullest extent possible. As sometimes terrorism charges – such as providing material support to a terrorist organization, – do not by themselves reflect the full extent of crimes that have been committed, prosecutors should therefore aim to try terrorist suspects, including FTFs, in a manner duly reflecting the seriousness of the crime. This will help to achieve justice, restore dignity, and bring closure to victims.

United Nations Security Council Resolution (UNSCR) 2242 (2015) urges Member States to research and gather gender-sensitive data on the drivers of radicalization for women, and the impacts of counterterrorism strategies on women's human rights. It is important to recognize the various roles both men and women can play in terrorism-related activities. Women as well as men can be perpetrators of terrorist attacks. There is, however, a need to adopt a more gender-sensitive perspective in a criminal justice approach to terrorism, taking into account the complexities that women may face as victims, witnesses or perpetrators. This includes providing guidance on gender-sensitive issues that can arise during arrest, questioning, prosecution, adjudication, or detention, as well as rehabilitation and reintegration of women. As stated in the GCTF *Neuchâtel Memorandum on Good Practices for Juvenile Justice in a Counterterrorism Context*, boys and girls caught up in terrorism have special needs and should be provided with adequate support throughout the criminal justice process.

The implementation of the Abuja Recommendations must be in conformity with relevant national and international law, in particular international human rights law, international refugee law, and international humanitarian law.

Recommendations

I. Recommendations on Law Enforcement and Judicial Cooperation

Considering the transnational and transregional threat of terrorism, strengthening law enforcement and judicial cooperation between States is crucial. The successful prosecution of terrorist suspects can be hindered if certain terrorism-related crimes have not been criminalized in national criminal codes, if a legal basis to facilitate extradition or mutual legal assistance (MLA) is missing, or if procedures for law enforcement or judicial cooperation are complicated and lengthy. States are encouraged, where applicable, to improve the effectiveness of law enforcement and judicial cooperation, invest in trust between stakeholders, and adapt to differences in legal cultures and language used. Adhering to obligations under international law – including international human rights law and international humanitarian law, particularly the right to a fair and public hearing – will enhance mutual trust and cooperation between States and strengthen the rule of law.

Recommendation 1: Streamlining law enforcement and judicial cooperation

The way in which criminal jurisdiction is established varies according to each country's national legislation, which takes into account the relevant international obligations of the particular State. Implementation of the international counterterrorism conventions and UN Security Council Resolutions contribute to the global criminalization of terrorist offences in national legislation and may help establish dual criminality to facilitate extradition and, when needed, MLA. The international counterterrorism conventions include an *aut dedere aut judicare* ("extradite or prosecute") obligation, requiring submission of a case to competent authorities for consideration of prosecution if an alleged offender is not extradited.

Depending on the (procedural) codes of different States, law enforcement and judicial cooperation can take different forms, and result in police-to-police cooperation as well as judiciary-to-judiciary cooperation, including between prosecutors and courts. This can occur through the issuance of a formal request or informally, including through a spontaneous exchange of information. Various forms of cooperation can include: questioning suspects and witnesses (via video/telephone conference when permitted by domestic law, or in person), delivery (in court) of testimony under oath, search and seizure of communication data, real time interception of communications, transfer of proceedings, or the collection and transfer of evidence. For the purpose of facilitating the cooperation between States in investigations and prosecutions of terrorism-related crimes, it is important that States lacking domestic authority to cooperate ratify conventions that provide a legal basis for MLA, as necessary and appropriate. In addition to ratifying the international counter-terrorism conventions, this can be done on a bilateral basis and by becoming a party to international or regional conventions on MLA, such as, but not limited to, the UN Convention Against Transnational Organized Crime or at the regional level the European Convention on Mutual Legal Assistance in Criminal Matters, the Scheme relating to Mutual Assistance in Criminal Matters within the Commonwealth, the ECOWAS Convention on Mutual Assistance in Criminal Matters, or the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters. In the absence of legislation specifically permitting MLA 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. Judicial cooperation bodies, such as Eurojust, could be used to facilitate cooperation and coordinate investigations and prosecutions in cross-border terrorism cases.

States are therefore recommended to criminalize terrorist offences through the implementation of international counterterrorism conventions, ratify existing MLA agreements and implement these in domestic laws to facilitate, where applicable, law enforcement and judicial cooperation, or, where appropriate, conclude bilateral agreements. Various model treaties have been drafted that can be instructive in this respect. An example is the United Nations Model Treaty on Mutual Assistance in Criminal Matters.

Recommendation 2: Strengthening central authorities for mutual legal assistance purposes

Designated central authorities furthermore fulfil an important function in expediting requests for MLA by the mere fact that they function as a focal point for foreign authorities to whom the request can be addressed. Central authorities can develop a global network, assisted by the United Nations Office on Drugs and Crime (UNODC). Central authorities can furthermore redirect the request for legal assistance to the right authorities, and can assist the requesting authority in drafting the request in accordance with the necessary requirements.

States are thus encouraged to designate an adequately staffed and trained central authority for MLA purposes to facilitate effective communication and cooperation between law enforcement officials, investigating judges, and prosecutors of different States.

Recommendation 3: Improving effective formal cooperation and information sharing

Not all actors operating in the criminal justice sector might be cognizant of applicable MLA procedures that guide international cooperation in criminal matters. Raising awareness among all actors operating in the criminal justice sector, as well as offering training to increase knowledge on how to use these procedures, is therefore recommended. These trainings should also pay attention to differences between legal systems.

Training should also address the need to share information with international and regional police cooperation organizations, such as INTERPOL, that have set up relevant databases, and with judicial cooperation organisations. Law enforcement officials and prosecutors furthermore need to become more cognizant of the human rights implications of using these databases, including obligations under international law, to refrain from interfering arbitrarily or unlawfully with privacy.

States are therefore recommended to invest in awareness raising and training on the benefits MLA can offer, the procedures of sharing data and the use of information available in the instruments and relevant databases set up by international and regional police and judicial cooperation organizations, including the international human rights obligations that apply, as well as the differences that exist between legal systems.

In order to expedite MLA, States are furthermore recommended to standardize request procedures, such as for those within regions, to the maximum extent possible. For example, templates could be developed for requesting legal assistance. Making use of electronic transfers of requests could further expedite procedures between central authorities or other criminal justice authorities. Some good examples of standardized templates have already been developed, for instance, by the European Union and the Council of Europe. Moreover, capacity-building programs have been developed *inter alia* by UNODC, also offering formats with different task descriptions tailored to both common and civil law systems.

Authorities submitting a request for legal assistance are advised to consult their counterparts in the requested State, including by sharing a first draft before submitting the formal request, to focus the request on the elements that are needed for the case, to use plain and simple language, and to provide the request in the language of the requested State. It is important to include in an MLA request what is strictly needed only in order to ensure assistance can be provided in a timely fashion.

Finally, and in order to effectively combat terrorism with legal measures, States are encouraged to contribute to information sharing systems and are recommended to offer each other to the greatest extent possible support through MLA in their investigations and prosecutions.

Recommendation 4: Investing in trust and (informal) networks

The information processed during criminal investigations and prosecutions of terrorist suspects can contain sensitive information also connected to national security. The investigation and prosecution of terrorist suspects should be conducted within a rule of law framework and in full conformity with international law, including international human rights law and international humanitarian law, such as the right to a fair trial. Information that is shared should nevertheless be handled with the required respect for the chain of custody and the sources should be appropriately protected. The same applies for information and evidence obtained through MLA. Considering the increasing number of terrorism-related cases with a transboundary or transregional element, sharing information and cooperating with foreign criminal justice actors becomes a crucial aspect of successful criminal justice responses. In light of these challenges, States are therefore recommended to invest in trust building between foreign criminal judicial actors.

The first aspect of building trust is becoming better acquainted with one's direct counterpart. Establishing (informal) networks between law enforcement officials or prosecutors can be helpful. Regional networks have already been established, such as the European Judicial Network. Informal networks are often very useful for sharing information and experience. Particularly when liaising with a direct counterpart prior to an official request for MLA, it will be worthwhile to submit an unofficial request, and focus on who it should be addressed to, what requirements should be fulfilled, or simply

to announce that the official request is coming to expedite the procedure. The informal sharing of information might also be instrumental during the preliminary stage of an investigation and for instance to establish probable cause in some jurisdictions for issuing an arrest warrant, even though the information might not be used as evidence during the trial later on in the procedure. States are therefore recommended to take a proactive attitude towards the sharing of information and the use of (informal) networks. The International Association of Prosecutors has developed a good practice in this respect. It should be noted, though, that making use of informal networks can never replace the official request and the guarantees regarding chain of custody and respect for fair trial that are integrated in the official trajectory. Within these networks, workshops can be organized to exchange experiences, challenges and good practices.

Another option to expedite procedures for MLA, or bilateral or multilateral law enforcement and judicial cooperation in general, is to appoint national liaison officers that are either posted in another State, or to an international police or judicial cooperation organization.

Recommendation 5: Promoting effective coordination of criminal investigations

Since terrorists often travel and operate within terrorist organizations and networks, investigations into the alleged terrorism-related crimes they have committed can seldom be limited to the jurisdiction of one State. Preparations for a terrorist attack might be made in one country, explosives and weapons smuggled from another country, instructions received from a third country, and the actual (planned) attack taking place in yet another country. At the minimum, it could be necessary for the law enforcement and judicial officials to contact and/or seek assistance from their counterparts in other countries, and request expedited assistance on an informal law enforcement to law enforcement basis in the investigation of criminal acts committed within their territory. This cooperation can later lead to requests for MLA if evidence is found that can be used in the prosecution of terrorism-related crimes.

International or regional police and judicial cooperation organizations, such as INTERPOL, Europol and Eurojust, moreover, have set up mechanisms for real time investigations with a transboundary or transregional element. This is particularly helpful in expediting the sharing of information, and for helping connect the dots in oftentimes very complicated networks of terrorist organizations.

A good practice, in some circumstances, of an even closer form of cooperation is formed by the Joint Investigation Teams (JITs) that can be set up for a specific purpose and a limited timeframe for the purpose of criminal investigation in one or more of the participating countries. JITs consist of competent national authorities of multiple States involved in complex cross-border criminal investigations that require coordination. The JIT Network, together with Eurojust, Europol and the European Anti-Fraud Office (OLAF), have developed a Practical Guide to provide information, guidance and advice to practitioners on the setting up and running of a JIT. Similar guides have been also developed by some other States. A model JIT agreement has been developed (available in all EU languages) to facilitate the setting up of JITs and represents a common non-binding baseline that practitioners can tailor to the needs of the case. However, since rules of disclosure as well as rules regarding admissibility of evidence might differ between States, clear arrangements should be included in the JIT agreement.

States are therefore recommended to offer full assistance, in accordance with domestic and international law, to other States conducting investigations into terrorism-related crimes with a transboundary or transregional element, and are furthermore encouraged to conduct coordination with national investigative agencies in other countries during their investigations. States are also advised to make use of the coordinating organizations available within the framework of international

or regional police and judicial cooperation mechanisms in case of complex investigations of terrorism-related crimes. Finally, States may wish to consider setting up JITs in criminal investigations with a high complexity and with a clear linkage to two or more specific States, which merits a close coordination of the investigation.

II: Recommendations on the Collection, Use and Sharing of Forensic Evidence

Forensic evidence – evidence collected through the use of scientifically accepted modern forensic sciences, consistent with applicable domestic and international law, including international human rights law – can be a valuable tool in the investigation and prosecution of terrorism-related crimes as stated in Good Practice 10 of the *Rabat Memorandum.*

Forensic science can help to prove that a crime has been committed (offence level), to identify victims and perpetrators (source level), or to describe the manner in which the crime has been committed (activity level). Forensic science can be used in the investigation and prosecution of terrorism-related crimes and can in some cases also be used in the prevention of terrorist incidents.

Forensic data can be retrieved from the crime scene, during the aftermath of a terrorist attack and/or on the battlefield, or from other relevant areas. The type of evidence recovered could range from fingerprints from unexploded improvised explosive devices (IEDs) to chemical characteristics of a bomb or data retrieved from electronic devices such as computers, mobile phones, flash drives or digital cameras. The forensic data can further be analyzed and documented at the crime scene itself – with the help of mobile equipment – or in laboratories.

Forensic science consists of many different methodologies such as ballistic and firearms examinations, fiber analysis, forensic chemistry or the use of biometric technology. In particular, biometrics – through a semi-automated recognition of individuals based on specific traits such as face, fingerprints, iris, voice, DNA or teeth – are frequently used. Forensic technology, especially with regard to biometrics and DNA analysis, is advancing very fast. Those States that have the technical and financial means could invest in forensic research, develop more sophisticated and reliable techniques that can be used in terrorism-related crimes and assist in building forensic capabilities in other countries.

The collection, analyzing, storing, using and sharing of forensic data can have implications for privacy rights, but can also affect the right to a fair trial. Privacy – although not absolute – is a human right recognized in article 17 of the International Covenant on Civil and Political Rights (ICCPR).

According to UNSCR 2396 (2017) all States shall develop and implement systems that collect biometric data in order to responsibly identify terrorists including FTFs in a manner that complies with States' domestic law and international human rights law. In order to further develop the use of forensic science in terrorism-related crimes these legal requirements including privacy rights should be addressed. States need to invest in developing their forensic capabilities, which includes investing in scientific research, technology, facilities, expertise and training staff but also ensuring that the current system is capable of adapting to new scientific developments such as forensic intelligence. Through developing new applications, using internationally accepted or scientifically proven standards for storing, analyzing and sharing forensic data, and furthering forensic cooperation between different stakeholders, forensic science can play a vital role in preventing and countering terrorism.

Recommendation 6: Promoting the use of internationally accepted or scientifically proven standards relevant to retrieving, analyzing and documenting forensic data

Part of a crime scene investigation consists of retrieving relevant forensic data that will be further processed and analyzed in (mobile) laboratories. If the methods of collecting, analyzing and storing are done in accordance with internationally accepted or scientifically proven standards and are well documented, forensic data can provide crucial information that can serve as evidence in court. Furthermore, the collection of forensic data in the context of sexual crimes with terrorist intent should be done in a gender-sensitive manner. The increased use and exchange of forensic data underlines the importance of developing and adhering to national and international standards. This includes accreditation of forensic laboratories, the use of standards with respect to scientifically established methods of analyzing forensic data within different forensic disciplines and the certification of forensic scientists and examiners. This would contribute to a more fair, efficient and reliable use of forensic evidence in terrorism-related cases.

Forensic laboratories can be established as an independent public body, a private organization, or as an entity linked to a law enforcement agency. Accreditation helps to build trust in forensic laboratories by offering assurance that laboratory activities are performed in accordance with relevant standards. With regard to the accreditation of forensic laboratories, the updated ISO/IEC 17025:2017 General Requirements for the Competence of Testing and Calibration Laboratories provide useful guidance on how to implement a quality system that is based on scientific methodology. In addition, the International Laboratory Accreditation Cooperation have issued ILAC G-19:08/2014 on Modules in a Forensic Science Process, which provides more detailed guidance on the forensic science process from crime scene to court. States are thus recommended to accredit their forensic laboratories according to internationally accepted or scientifically proven standards. Furthermore, to ensure quality, States are advised to regularly conduct proficiency tests. States should at the same time be cognizant to allow for the development of new techniques that may contribute to advancing a given investigation technique.

Several national and international organizations have developed scientifically tested standards in a range of forensic methodologies such as finger print analysis, ballistic analysis, digital evidence and DNA sampling. At the regional level, notably within the EU, efforts are made to ensure the collection, analysis, and use of forensic data will be based on minimum forensic science standards. States are therefore recommended to develop national standards and adhere to international and regional standards, which could contribute to the reliability of forensic evidence in court and promote public confidence in forensic science.

Finally, States should ensure that a proper certification of forensic scientists is established to ensure reliability and quality of the persons that are analyzing forensic data.

Recommendation 7: Collecting and storing forensic data

Forensic data can play a vital role in the prevention, investigation and prosecution of terrorism-related crimes. The technology to analyze DNA has improved significantly and national DNA databases have been created by some States. Many other States are in the process of establishing a national database for purposes such as identification, health, immigration, or criminal investigations. States can establish different types of DNA databases for criminal investigations purposes: for convicted persons, for missing persons, or an elimination database to exclude laboratory staff and law enforcement officials who have been in contact with forensic data as part of their work. Whether a State decides to establish a centralized or a decentralized database could impact the interoperability and security of the

databases. Centralized databases, while more vulnerable, can facilitate database interoperability, whereas more secure decentralized databases may not enable compatible data sharing with other databases. States or international organizations, such as INTERPOL, with experience in setting up and maintaining a DNA database for criminal investigation purposes are encouraged to share their experiences with other countries. States should establish biometric databases that are able to distinguish amongst those biometrics associated with known/suspected threat actors (e.g. terrorists, criminals) and those that are not.

Further, the collection and storage of biometric data can affect the right to privacy. To protect personal data, States should ensure databases have a robust and secure infrastructure. In order to prevent privacy rights from being significantly eroded by the improper collection and retention of biometric data, States are recommended to collect and store biometric data for specific, explicit and legitimate purposes. States need to formulate legal requirements under which conditions DNA can be collected without consent, procedures for taking DNA samples (for example by obtaining a warrant), the period for which the data can be stored and how biometric data can be accessed and appealed by the accused or be removed from the databases. States are therefore recommended to adopt adequate safeguards. UN General Assembly Resolution 45/95 Guidelines for the Regulation of Computerized Personal Data Files (1990) contains useful guidance and principles that could be applied with respect to the storing of biometric data.

In order to protect the rights of a child, States are advised to establish specific provisions regarding collecting, using, and storing the forensic data of minors. This could include consent from parents, limiting the duration of storing biometric data even more or permanently deleting data when it concerns minor crimes. In addition, to ensure that applicable international human rights obligations are observed, States are recommended to consider establishing adequate oversight mechanisms.

Recommendation 8: Sharing of forensic data and evidence: the need for intra-state and international cooperation

International forensic cooperation between stakeholders can take many forms. There is a need for a better understanding of and knowledge among criminal justice actors on what forensic science entails and how it can contribute to the prosecution of terrorism-related crimes. Closer cooperation between forensic laboratories and with criminal justice actors within a country should be encouraged through establishing a platform to exchange views. States are recommended to raise awareness of forensic science – including its limitations and opportunities – among criminal justice actors but also to enhance understanding of the evidentiary value of forensic evidence among the forensic community.

Through cooperation among forensic laboratories in different countries, countries can for example assist each other in collecting or analyzing forensic data in the aftermath of a terrorist attack, provide training, and exchange methodologies to improve forensic capabilities. As a best practice, States could consider carrying out forensic tests *pro bono* for countries that do not have any forensic capabilities. Considering the different technological and financial capabilities of countries, States are therefore recommended to promote forensic institutions to participate in international and regional networks of forensic institutions to enhance the exchange of forensic expertise, strengthen technical capabilities and developing common standards.

Law enforcement officials and prosecutors from different countries can share forensic expert opinions through MLA, or in certain circumstances via police-to-police cooperation, to support the investigation and prosecution of terrorist offences in accordance with human rights obligations. Some of the challenges – relating to sharing of information – are also relevant to sharing forensic data and

evidence. Law enforcement officials and prosecutors should be cognizant of the different standards of admissibility of forensic evidence that may apply in different countries.

Finally, the exchange of forensic data contained in different national databases between countries or with international or regional organizations is a form of international forensic cooperation. A good example is the Prüm Convention that allows EU Members States to share and match DNA profiles in an automated way. States are, in accordance with their domestic laws, also encouraged to share DNA profiles with the DNA database of INTERPOL. This database uses international standards that are compatible with the Prüm Convention. States who share DNA profiles with INTERPOL retain ownership of the DNA profiles and determine what type of information will be shared with which countries. Furthermore, INTERPOL has established a data protection office to ensure data protection, transparency, and accountability to facilitate and ensure trust among States to share forensic data with INTERPOL.

Recommendation 9: Strengthening the use of forensic evidence in court

The evaluation and interpretation of forensic findings, also referred to as expert opinions, can be used as forensic evidence in court. To be able to use forensic evidence in court it is vital that the methods of how and where the forensic data has been found, which methods have been used to retrieve and analyze the forensic data, and the number of persons that have handled the forensic data are carefully documented. Prosecutors need to ensure the authenticity and integrity of forensic evidence. Law enforcement officials and prosecutors are therefore recommended to carefully document how forensic data is retrieved and analyzed to facilitate its use as evidence in court.

Furthermore, the presentation of forensic evidence in court should be done by qualified forensic experts. To ensure that the interpretation and evaluation of forensic findings are conducted systematically and professionally, the Technical Committee 272 on Forensic Sciences of ISO is currently developing a standard on dealing with the detection, collection, analysis, interpretation and reporting of forensic evidence, which can be useful in improving the standards and procedures. States are recommended to invest in (the training of) qualified forensic experts, setting up a roster of registered forensic experts, using standard terminology and developing model reports regarding the interpretation and reporting of forensic findings for investigation and prosecution purposes.

To guarantee fair trial and the principle of equality of arms, the defense counsel should be able to question the validity of forensic evidence that is presented against the accused. This means that forensic evidence should be disclosed – in so far as the investigation permits this – in a timely manner to allow the defense counsel to examine the forensic data or consult a forensic expert to analyze the forensic data or interpret the forensic findings. Considering the costs involved in reviewing forensic evidence, States are advised to make forensic science available to the defense by integrating it in a legal aid scheme.

III: Recommendations on the Collection, Use, and Sharing of Electronic Evidence

Whilst the progress of information and communication technologies provides numerous benefits, terrorists and terrorist organizations also use the Internet for terrorist purposes such as recruiting, financing, training, planning, and the carrying out of terrorist attacks including cyber-attacks. The fact that terrorists rely heavily on the Internet also means they leave digital traces that provide opportunities for criminal investigations and prosecutions. The increasing use of electronic evidence in terrorism-related cases, however, brings along additional challenges as well.

Information obtained from the Internet could be categorized as Basic Subscriber Information, Traffic Data and Content Data, all of which can constitute electronic evidence. For the purpose of securing data as electronic evidence, there are various manners in which law enforcement officials and prosecutors can obtain this data. "Data preservation" must be distinguished from "data retention". To preserve data means to keep data, which already exists (longer) in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. Data preservation is the activity that keeps that stored data secure and safe whereas data retention is the process of storing data. Data retention refers to an automated retention period of stored data relating to traffic information, location and basic subscriber data. Law enforcement officials and prosecutors can in addition to stored information also request real-time information, which consists of either traffic or content data.

Electronic evidence is volatile, easily altered, damaged or destroyed, time sensitive, and not bound by territorial jurisdictions. The rapid developments in communication technology, the use of encryption, anonymizers and cloud computing, require States to adapt their technological capabilities accordingly. General investigative tools may not be adequate in gathering and obtaining electronic evidence and would require more 'cyber-specific' tools as has been underlined in Good Practice 4 of the *Rabat Memorandum.*

Cooperation with service providers is vital in preserving and obtaining electronic evidence. The fact that data can be permanently in migration or can be stored in multiple or in foreign jurisdictions, poses a challenge for those law enforcement officials and prosecutors seeking to submit an MLA request and needing to know to which country to issue the request. The gathering of electronic evidence and data retention rules can have implications on privacy and other human rights. In accordance with UNSCR 1373 (2001) paragraph 2, which has been reaffirmed by UNSCRs 2178 (2014), 2322 (2016) and 2396 (2017), States are required to give one another assistance as much as possible in the prosecution of terrorist suspects.

Recommendation 10: Improving the use of general and cyber-specific tools to obtain electronic evidence

The use of electronic evidence is becoming increasingly important in the prosecution of terrorist suspects. Law enforcement officials can use traditional or special investigative techniques to obtain electronic evidence or rely on more cyber-specific tools.

When appropriate, it is recommended that law enforcement officials or prosecutors try to get consent from the user or next of kin to obtain data. The term user is defined by the service providers and often refers to the creator of an account and is sometimes used interchangeably with subscriber, referring to the person who is registered to use an online service. This could in particular be useful when encrypted technology has been used. Other tools such as open source investigations – referring to publicly available data - can be useful to either locate a user or service provider or to determine whether any criminal activity took place. Law enforcement officials could use open source tools to obtain relevant electronic data. Defining the term 'open source' narrowly, to prevent potential violations of human rights such as the right to freedom of expression, must be taken into consideration. Law enforcement officials and prosecutors are furthermore advised to document where the information came from to ensure that it can later on be used as evidence in court.

In situations where the traditional investigative powers prove to be insufficient to obtain electronic evidence in terrorism-related crimes, States are recommended to consider adopting cyber-specific legislation for example to ensure the preservation of computer data and/or adhere to multilateral or regional cyber-specific conventions. Furthermore, States are recommended to invest in improving the

capabilities of law enforcement officials by providing training and using best practice manuals – such as the guides of the UNODC or Council of Europe - on how to obtain electronic evidence.

States should assess whether the current legislation takes into account new technologies and is suitable to preserve and obtain electronic evidence such as prescribing service providers to retain data or allowing law enforcement officials to obtain real-time data or search computer hardware.

Recommendation 11: Locating and preserving electronic evidence

Terrorists and terrorist networks are frequently using software tools and other techniques to hide their identity and location and to store their information. Once the location of the data is determined, or once the service provider holding the data is identified, law enforcement officials or prosecutors should try to preserve the data as soon as possible to prevent it from being altered or deleted. Law enforcement officials or prosecutors can, in some jurisdictions, submit a data preservation request directly to a service provider, use informal cooperation – such as police-to-police cooperation – or send an MLA request to preserve the data. Law enforcement officials and prosecutors should make a preservation request through 24/7 networks, where available.

Cloud computing is making it increasingly difficult to determine where data is stored, as data can sometimes be stored in foreign, multiple or unknown jurisdictions leading to a 'loss of location'. Furthermore, cloud computing raises specific challenges relating to applicable law and jurisdiction. States apply different criteria for different purposes to establish jurisdiction. Depending on whether data are needed for data protection, tax, intellectual property or prosecution purposes, different connecting factors are used to determine jurisdiction and applicable law. States are recommended to explore whether legislative measures may be needed to ensure that data are not lost and can be used to investigate and prosecute terrorism-related crimes.

Recommendation 12: Encouraging effective cooperation with service providers

A service provider transfers information electronically and refers to telecommunications companies (landline and wireless), data carriers, cable operators, network providers, satellite companies, and internet providers. Service providers are regulated by a range of national laws and have often also developed their own internal policies and regulations. Storing data is expensive and whether the service providers retain data depends on the national law where the service providers are based. In some countries, there is no obligation to retain data, whereas other countries require service providers to retain data for a limited time.

Requests to service providers to take down content must be made in a manner consistent with international human rights law and need to be balanced against the fact that the content might be of interest to law enforcement officials and prosecutors. The GCTF *Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online* offer useful guidance on this topic.

Service providers can, depending on the jurisdiction, preserve data, disclose data and respond to emergency requests on a voluntary basis, based on their own law enforcement guidelines, and depending on the national law of the country where they are based. The law enforcement guidelines describe the procedure for making a preservation or disclosure request, what type of data can be requested, how such a request can be submitted, the possibility of extending a preservation order and whether the user will be notified. Several of the major service providers disclose data in case of an emergency.

This plethora of legal and company regulations creates a complex environment, which requires law enforcement officials and prosecutors to familiarize themselves with the law enforcement guidelines of the providers and the different data retention rules of the countries where the service providers are located.

In case a service provider does not have any procedures in place, law enforcement officials are recommended to reach out to international or regional law enforcement organizations or use police-to-police cooperation with the law enforcement officials of the country where the service provider is located to seek assistance in obtaining electronic evidence. However, the current procedures for cooperation between judicial authorities to obtain electronic evidence in cross-border situations are slow compared to the speed at which electronic data can be changed or deleted. Informal cooperation will facilitate the process of obtaining electronic evidence directly from service providers but also assist in speeding up a formal request to disclose data. Setting up informal networks between law enforcement officials, prosecutors, services providers and other stakeholders may also help foster better understanding and build trust.

States should encourage service providers to develop more consistency and standardization in the process of preserving, obtaining and transferring data, including answering to emergency requests, and by designating legal representatives at country level to facilitate the receipt and processing of requests to gather electronic evidence.

Recommendation 13: Obtaining electronic evidence located abroad

Electronic evidence is often located in a jurisdiction other than where the criminal proceedings take place. Although MLA requests can be time consuming and complex, States still tend to rely on traditional and formal forms of international judicial cooperation. Countries can use multilateral conventions, such as the United Nations Convention against Transnational Organized Crime, and regional or bilateral MLA treaties as well as their domestic law as a legal basis to obtain electronic evidence located abroad, or relevant provisions of some of the international or regional counter-terrorism conventions. Furthermore, States can rely on international cyber-specific conventions, such as the Budapest Convention of the Council of Europe, to obtain electronic evidence located abroad. To facilitate and expedite the MLA process law enforcement officials and prosecutors are encouraged to clearly specify what kind of data is required, ensure any dual criminality requirement is met, and consider using international or national templates for MLA requests, or using the UNODC MLA Request Writer Tool. Officials may also benefit from reaching out informally to the requested States prior to sending out the formal request. Another best practice is to share the draft MLA request informally, before submitting it through the formal channels. Different forms of informal cooperation such as police-to-police cooperation or the 24/7 National Central Bureau networks of INTERPOL can be used. Other informal cooperation networks such as the 24/7 network under the Council of Europe Cybercrime Convention or the G8 Subgroup on High-Tech Crime can also be used ahead of sending an MLA request or in support of an MLA request.

The use of informal cooperation is often faster and therefore very useful in the context of gathering electronic evidence, particularly when the information is being gathered for intelligence purposes. A possible follow up with formal requests can be made in case the information should be used as evidence. Law enforcement officials, prosecutors and other relevant authorities could also consult the Practical Guide for Requesting Electronic Evidence Across Borders developed by UN CTED, UNDOC, and the International Association of Prosecutors (IAP).

Considering that evidence obtained through informal cooperation or directly from the service providers may not be admissible in court, formal cooperation remains crucial to obtain electronic

evidence located abroad. States are recommended to utilize the existing legal frameworks to allow for MLA in obtaining electronic evidence from abroad, to alternatively use informal cooperation mechanisms prior to or in addition to formal cooperation, and to rely on domestic law or on reciprocity as a legal basis to afford each other MLA in terrorism-related cases.

Recommendation 14: Respecting human rights in the context of electronic evidence

The use of general or cyber-specific tools and data retention rules can have an impact on the right to privacy – pursuant to article 17 of the ICCPR - and the protection of personal data. The protection of personal data is closely linked to the right to privacy, but not all legal systems differentiate between these two. The protection of personal data is not as firmly anchored in binding international instruments, but a considerable number of countries are adopting national laws on data protection.

Lawful surveillance and retention of data for the purpose of combatting terrorism is a legitimate aim but in some jurisdictions needs to be necessary and proportionate in order to avoid being arbitrary. Although most States have privacy protections, the way in which privacy is regulated differs substantially: in some countries privacy is constitutionally regulated, whereas in other countries specific privacy acts have been adopted. Privacy can also be protected through self-regulation; service providers have adopted privacy policies and sometimes have jointly adopted privacy principles. Common safeguards include restrictions to the type of data (subscriber data, traffic data or content data), time limitations to the use of investigative tools, effective guarantees against abuse, and independent oversight mechanisms. States are recommended to assess whether their national privacy laws and data protection laws sufficiently take into account the need for law enforcement authorities investigating and prosecuting terrorism-related crimes to use investigative tools while respecting the right to privacy and human rights in light of the on-going technological developments.

Recommendation 15: Strengthening the use of electronic evidence in court

Electronic evidence can easily be altered or modified and may pose challenges when it is being introduced in court. Prosecutors need to ensure the authenticity and integrity of electronic evidence presented in court. The use of digital forensics – a process of collecting, analyzing and reporting on digital data retrieved from computers, smart-phones or other similar devices – is vital to present electronic evidence in court. When electronic evidence is obtained directly from service providers, law enforcement officials or prosecutors could request a service provider to provide a supporting document to establish the chain of custody or a statement indicating that the electronic evidence is self-authenticating. States are recommended to invest in expanding their capacity in digital forensics, which includes equipment but also the training of staff on issues of decryption and assessing reliability of electronic evidence.

The use of different file formats, operating systems and software by criminal justice actors and service providers within a country and between countries makes it difficult to use electronic evidence in terrorism-related cases. States are therefore recommended to develop international standards to improve the interoperability of electronic data in different legal systems and improve the use of electronic evidence in terrorism-related investigations and prosecutions.

Electronic evidence is in most countries admissible in court. Electronic evidence can be presented in different ways in court, making use of testimonies or expert reports but also electronic equipment. Electronic evidence can sometimes be so technically complex that an expert witness on digital forensics might be required in court to explain the relevance of the electronic evidence in a particular case. States are recommended to improve the technical capabilities of prosecutors by providing IT

training on a regular basis on the different aspects of retrieving, storing and using electronic evidence in court.

IV. Recommendations on the Collection, Use and Sharing of Intelligence for Criminal Investigations and Prosecutions

The intelligence services – both civilian and military - have relevant insights into terrorist networks and terrorists, on and off the battlefield. Especially if regular channels of law enforcement and judicial cooperation between criminal justice sector actors are no longer functioning, for instance because of a conflict situation, the intelligence services can play a crucial role in gathering intelligence for criminal investigations and prosecutions. This is also the case in the context of FTFs who have left for conflict areas and are returning home or travelling to a third country. To optimize the possible use of intelligence as evidence in court, effective coordination, cooperation and communication between the intelligence and law enforcement services in a country and between countries are vital. Another challenge is related to the actual use of intelligence as evidence in court, which hence goes beyond using such information as a mere lead to start an investigation, and to ensuring that procedures in place make it possible for information to be released to a court in compliance with the right to a fair trial, while protecting sources and methods.

In particular, States should have mechanisms and procedures that allow intelligence information relevant to terrorism threats to be shared, where appropriate, with authorized law enforcement personnel. These procedures should be established by taking into account both the national security concerns of a government and the right to a fair trial of the accused. In order to safeguard the lives of victims and informants, protect sources and methods, and maintain the usefulness of sensitive investigative techniques, governments must be able to protect certain types of information and techniques from public disclosure, even in the course of public criminal justice proceedings.

The following recommendations complement and build on United Nations Security Council Resolution 2396 (2017) and on a number of already-existing GCTF Good Practices and Recommendations, in particular Good Practices 6 and 9 of the GCTF *Rabat Memorandum*, *Good Practice 6 of the GCTF The Hague Memorandum on Good Practices for the Judiciary in Adjudicating Terrorism Offenses* and Recommendations 1, 2, 3, 4, 5 and 6 of the *GCTF Recommendations for Using and Protecting Intelligence Information In Rule of Law-Based, Criminal Justice Sector-Led Investigations and Prosecutions.*

Recommendation 16: Promoting effective coordination, cooperation and communication

More coordination and cooperation, for instance through fusion centers (but also via more informal cooperation mechanisms), will lead to a better understanding of the different roles and needs of both communities. The relevant information is often there, but it must be made available to those who need it as far as this is possible in accordance with domestic laws; it must first reach the relevant actors. For example, intelligence officers may have information at their disposal that is not relevant to their own work, but which may be crucial for a prosecutor trying to find the final piece of the puzzle that would allow for a successful prosecution of terrorist suspect. When a certain piece of information was in fact key in securing a conviction of a terrorist, communicating this back to the initial information provider, which may also include a foreign intelligence service, can help foster a positive feedback loop.

States are therefore recommended to keep investing in coordination and cooperation mechanisms between the intelligence services, law enforcement community and the judiciary within their country. As already recommended in the GCTF *Recommendations for Using and Protecting Intelligence*

Information In Rule of Law-Based, Criminal Justice Sector-Led Investigations and Prosecutions, States should consider establishing mechanisms or procedures by which intelligence agencies may be made aware of the standard rules of evidence used in judicial proceedings in the relevant country.

Recommendation 17: Improving the sharing of intelligence for criminal investigations and prosecutions internationally

States can share intelligence for criminal investigations and prosecutions both bilaterally and multilaterally, for example via INTERPOL or Europol. Sharing of intelligence benefits from human rights compliance in both the data collection phase and the phase of processing and use of the intelligence in the criminal procedures. States may be more willing to share intelligence if assurances on human rights compliance in the context of data collection and sharing have been provided.

It is understandable that States will especially share intelligence with only those countries whose services they trust – for instance because of the other State's trustworthy (human rights-compliant) legal system. Some States require in their national legislation and regulations that they will only share intelligence with foreign services if these comply with certain human rights requirements. 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.

States are furthermore encouraged to increase intelligence sharing for criminal investigations and prosecution through international organizations. Terrorism, especially related to the FTF phenomenon, has a transboundary or transregional element and thus requires a truly international response. Similar to the domestic level, it is also vital at the international level that the relevant information ends up with the actors who need it. Organizations like INTERPOL and Europol can play a central role in this context. In each situation, whether bilaterally or multilaterally, States are advised to provide organizations such as INTERPOL and Europol information for criminal investigations and prosecutions obtained in full conformity with human rights.

This will increase the chance that the information will be found admissible in case it will be used as evidence in court.

Recommendation 18: Strengthening the use of intelligence as evidence in court

Intelligence services may be wary to disclose the sources and methods in which their information has been obtained. Yet, in order to ensure admissibility of the information as evidence in court, it is important, according to relevant domestic law, that the origin and hence the reliability of the information can be established by both the prosecutor and the judge. In general, and to avoid as much as possible the need to follow declassification procedures, States are recommended not to overclassify their intelligence data.

Furthermore, in some countries a third party, with both a foot in the intelligence community and the law enforcement community, such as an independent commission or a special intelligence prosecutor, may review the intelligence and decide whether or not certain information can be declassified and turned over. In yet other countries, including many common law countries, law enforcement officials will work with the intelligence officers to identify which information is relevant for the case. Subsequently, the prosecutor will work with these entities to agree on the appropriate format in which the information will be disclosed to the court and/or the defense. States are recommended to consider establishing such mechanisms that can turn intelligence into useable evidence, taking into account the specifics of the legal system.

Recommendation 19: Respecting international law and human rights

Human rights law prescribes that the accused is entitled to challenge the evidence against him. At the same time, some flexibility may be needed to take into account the valid security concerns that come with using classified or sensitive intelligence information, at least if it is determined that this information is intended to be used as evidence in criminal proceedings. Some of the out of the box thinking and non-traditional methods may be required. For example, by protecting the identities of witnesses by having them testify using a pseudonym or behind a screen or in light disguise (with the court's permission).

As regards the question of what to do in case of pre-trial violations of international law: in most legal systems, judges have discretion in deciding which remedies should be attached to which violations, but the extent to which judges are trained on standards of international law (versus domestic law) and the extent to which international law standards are incorporated into a particular State's domestic law may vary. While stressing the autonomy and independence of the judiciary, and in accordance with the applicable and relevant practices and legal frameworks, States could formulate guidelines that judges can take into account when assessing certain (pre-) trial violations of human rights and/or international law. Suppression of unlawfully obtained evidence or suppression of the fruits of such evidence are the more serious remedies. Some violations are indeed considered so serious – for example the use of torture to extract intelligence information – that in all such cases, irrespective of the actor responsible, evidence should be declared inadmissible in a court of law, to avoid undermining the integrity of the court's process. In such cases, officials should also consider whether such 'tainted' information should be shared – bilaterally or multilaterally. For some less serious violations, other remedies can be considered, such as a reduction of the sentence, financial compensation or – for mere procedural violations not substantively impacting the rights of the suspect – a statement that certain rules were not followed.

V. Recommendations on the Collection, Use and Sharing of Evidence by the Military

Investigating and prosecuting terrorist-related crimes is seldom limited to acts committed within the territory of one State. Terrorists and terrorist organizations often operate abroad and have a transboundary or transregional character. To collect information and evidence on terrorism-related crimes, it is oftentimes necessary to cooperate with other States through MLA. However, during (post-) conflict situations such cooperation is not always effective or at all possible. This is caused by the often chaotic and insecure situation where the information is located making the use of existing MLA agreements very difficult, or because such MLA agreements do not exist and judicial cooperation based on reciprocity is not possible with the country where the evidence is located. In these situations, the risk of impunity arises because the actual terrorism-related crimes committed in these (post-) conflict situations may not be prosecuted for lack of evidence. In such a scenario, prosecutors in some countries have used an alternative prosecutorial approach, which focuses on prosecuting perpetrators for attempting to travel, conspiracy to commit terrorist crimes, or membership of a terrorist organization. In these situations, the risk of impunity as well as the right to justice to the victims arises, which is worth considering.

In addition, a chaotic situation, for instance caused by an armed conflict situation, may also occur on the territory of the State that is prosecuting the suspect itself. Also in this situation, it may be very difficult for the prosecution to prove terrorism crimes, including related crimes, such as acts of sexual violence committed by members of terrorist organizations.

The challenge law enforcement officials and prosecutors encounter in collecting the relevant evidence is especially acute in relation to the growing threat posed by FTFs and returnees, and the ambition of prosecutors to prosecute their own nationals or residents. A lot of information can be retrieved in (post-) conflict situations that could be relevant for criminal prosecutions. Examples are intelligence information, forensic information such as fingerprints on IEDs retrieved on the battlefield, information and evidence gathered at sites such as mass graves, and information on membership of individuals to terrorist organizations and the scope of the networks they operate in. This kind of information and evidence can provide crucial pieces in a jigsaw puzzle on how terrorist networks operate and who has committed what kinds of terrorism-related crimes.

In most cases, collection of information that can be used as evidence is not the main goal of military operations. However, because of their presence on the battlefield, the military personnel may be able to contribute to the collection of relevant information that can be used as evidence in court. Such activities must be conducted consistent with international law.

In appropriate circumstances, and in coordination with the military forces, International Commissions of Inquiry or other mechanisms authorized by the Security Council to do so may also retrieve relevant information from the battlefield that can be used in the prosecution of terrorism-related crimes. Clearly, the scenario in which the military is facilitating in the collection of information and evidence should be considered to form an exceptional situation.

A particular challenge, however, for law enforcement officials and prosecutors is how to ensure that the information retrieved by the military and other acknowledged actors in (post-) conflict situations meets the legal thresholds to be allowed as evidence in criminal proceedings, according to the legal system in different States. The strict legal criteria that are laid down in the national criminal codes, which include the admissibility of evidence, preservation of the chain of custody and evidence, and respect for fair trial principles, need to be met.

This challenge has been acknowledged in the Madrid Guiding Principles (S/2015/939, 23 December 2015), and mentioned in UNSCR 2396 (2017). Also, the Sixth Report of the Secretary-General on the threat posed by ISIL (Da'esh) (S/2018/80 of 31 January 2018) highlighted that only a few States are able to collect evidence in conflict zones, and that the efforts to collect evidence in conflict zones need to be strengthened.

Several international initiatives are currently being developed to support the role of the military, provide guidance and clarify the mandate that would be needed, as well as the modalities that can be used. In a UN context the 'UN guidelines to facilitate the use and the admissibility as evidence of information preserved, collected and shared by the military' will be able to provide such guidance.

Recommendation 20: Strengthening the use of information collected by the military as evidence in court

Considering the fact that in exceptional situations such as during a conflict or a high-risk situation, law enforcement officials may not be able to perform their tasks of investigating terrorism-related crimes, States are recommended to ensure that information collected by the military can be used as evidence in terrorist cases in accordance with their criminal law, and if needed amend their legislation in order to make this possible, or provide instructions on how this can be done. States are furthermore recommended to ensure that fair trial principles, absence of torture and inhuman and degrading treatment, observance of the adversarial principle, and fair admission of evidence are being respected when allowing the use of this information collected by the military.

In some situations, law enforcement officials and prosecutors could even take a more proactive role and explicitly communicate their evidentiary needs in specific cases to military actors, for instance in the preparatory phase of a military mission.

Some States have gained experience in collecting information from the battlefield and using it as evidence in criminal proceedings, while balancing between the notions of securing the chain of custody in oftentimes chaotic and insecure circumstances, and the right to a fair trial including but not limited to absence of torture and inhuman and degrading treatment, observance of the adversarial principle and fair admission of evidence. States are therefore recommended to exchange these experiences in order to develop a compendium of good practices.

Recommendation 21: Preserving the chain of custody and respecting the integrity of the criminal proceedings

A key requirement for submitting any form of information as evidence in criminal proceedings is that the chain of custody has been observed and preserved. Respecting the chain of custody when information is collected on the battlefield and is used in a criminal proceeding, irrespective of the form of evidence (physical evidence, electronic evidence or forensic evidence), may be difficult. This is because the procedure of 'bagging and tagging' evidence in an otherwise sealed crime scene cannot always be observed in chaotic and highly insecure situations on the battlefield. However, military actors or other authorized actors retrieving information from the battlefield could, whenever possible once they find themselves in a more secure environment, ensure traceability on who retrieved the information, where, when and under what circumstances it was retrieved, and keep a ledger of who handled the evidence and to whom it has been transferred to. Missing links in the chain of custody should not, however, preclude admissibility automatically. Notwithstanding these challenges and the possibilities that nevertheless exist, it is recommended that States raise awareness among criminal justice actors about the limits and possibilities of collecting information and evidence in battlefield circumstances, taking into account imperatives of operational effectiveness.

During the trial, a number of challenges can occur that can impact the admissibility of the information as evidence in court. These include the (cross-) examination of a witness or military who collected the information, and the level of knowledge and skills on how to perform the 'bagging and tagging'.

The defense should be able to verify the reliability and credibility of the evidence submitted. For reasons of national security the identity of the individual (whether military or another actor) that handled the information or evidence on the battlefield could need to remain hidden. In order to nevertheless facilitate a testimony on how this information or evidence has been collected, while at the same time ensuring to the greatest extent possible that the fair trial principles are observed, some creative or non-conventional solutions should be found to accommodate the rights of the defense for cross examination. Examples might be through video-links or submitting an affidavit, subject to domestic rules of evidence.

There are furthermore differences in the level of knowledge and skills between the various actors operating on the battlefield on how to handle information or evidence that needs to be submitted in a criminal case as evidence. One can expect, for instance, that, where such units exist, military police or embedded investigators (for instance seconded by the Ministry of Justice to the military command) will be trained to handle evidence. Depending on the level of knowledge and skills of the relevant military actors, the value of the evidence presented can overcome irregularities in the chain of custody in case they occured. Eventually, it will be the court that decides whether the evidence will be admitted.

States are therefore recommended to consider the development of guiding principles in accordance with their domestic criminal procedural rules and international human rights obligations that assist relevant criminal justice actors in assessing the balance that needs to be found between the circumstances under which information or evidence has been collected and the observance of the chain of custody, as well as the integrity of the criminal proceedings, including ensuring full respect to the rights of the defense.

Recommendation 22: Promoting effective cooperation, coordination, mutual legal assistance, and communication with relevant actors

Law enforcement officials and prosecutors who need to make use of evidence collected on the battlefield in their terrorism cases are encouraged to do everything in their power to establish working relationships with the criminal justice authorities of the State in which the evidence is collected, in order to facilitate MLA. However, in those situations where this seems to be impossible, law enforcement officials and prosecutors are recommended to establish as early in the process as possible working relationships and lines of communications with the relevant actors on the battlefield that can assist in collecting information that can be submitted as evidence.

Recommendation 23: Strengthening multipurpose use of information gathered by military and declassification of military intelligence

On many occasions, and as part of the regular activities of military during an operation, intelligence will be gathered for operational purposes. Such intelligence might contain important information on terrorism-related crimes committed, terrorist networks, and individuals involved. Clearly, this information might be of interest for criminal investigations and prosecutions. In general, it is advised that information be only classified if necessary. In those situations that intelligence has been classified, and can be declassified later on if relevant for the investigation of a case or a criminal prosecution, the question remains whether the intelligence information can be admissible in court.

In some situations, the information collected by the military can be processed through a dual track and with a dual purpose. In addition to the processing through the intelligence and confidential track, the information could at the same time be processed with a prosecutorial purpose in mind, ensuring that the chain of custody is observed and fair trial guarantees respected. When appropriate, law enforcement officials and prosecutors are therefore advised to communicate the prosecutorial needs in an investigation to the relevant actors in order to ensure opportunities are not missed to process information.

There are good practices on how the need for confidentiality of sources can be balanced with the need of transparency in criminal proceedings, while respecting fair trial guarantees. States are therefore advised to take into consideration the Recommendations and Good Practices already developed in the GCTF *Rabat Memorandum*, the GCTF *The Hague Memorandum on Good Practices for the Judiciary in Adjudicating Terrorism Offenses and the Recommendations for Using and Protecting Intelligence Information In Rule of Law-Based, Criminal Justice Sector-Led Investigations and Prosecutions*, and the GCTF R*ecommendations for Using and Protecting Intelligence Information In Rule of Law-Based, Criminal Justice Sector-Led Investigations and Prosecutions*.

VI. Recommendations on the Hearing of Witnesses and the Use of Testimony

Witness testimonies have been and remain of critical value in investigating and prosecuting crimes, including terrorism-related crimes. There are various sorts of witnesses that can testify, such as victims, expert witnesses, informants and justice collaborators/*pentiti*.

Because of the crucial role of witnesses in investigations and prosecutions of serious crimes, many of them may be intimidated or threatened, something which is particularly notable in terrorism-related cases. In the context of FTFs, family members may testify against the FTF, but then withdraw or change the testimony because they may be intimidated. This raises issues of both vulnerability and credibility. Therefore, it is of utmost importance to protect witnesses – in and outside the court – and at the same time ensure fair trial guarantees for the defendant in accordance with article 14 of the ICCPR.

One can expect an increase in the use of such witnesses in terrorism-related prosecutions, especially expert witnesses. This is because terrorism cases are becoming increasingly complex, taking into account the technical or sometimes scientific nature of the evidence, such as electronic evidence or forensic evidence. As a result, the nature and relevance of such evidence will need to be clarified to prosecutors, defense counsel and judges by expert witnesses.

The following Recommendations will complement and further build on already-existing GCTF good practices and recommendations, in particular: Good Practice 4 of the GCTF *The Hague Memorandum on Good Practices for the Judiciary in Adjudicating Terrorism Offenses*, Good Practice 1 of the *Rabat Memorandum* and Recommendations 1, 5 and 7 of the GCTF *Recommendations for Using and Protecting Intelligence Information In Rule of Law-Based, Criminal Justice Sector-Led Investigations and Prosecutions*. In addition, the UNODC manual Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime (the UNODC Manual) is highly relevant for the context of terrorism cases as well and should be considered.

Recommendation 24: Enabling the use of procedural protective measures

To ensure that witnesses, to the greatest extent possible, can testify without feeling intimidated or threatened, a variety of protective procedural measures in court can be considered. These include: the use of pretrial statements (either written or recorded audio or audio-visual statements) as an alternative to in-court testimony; redaction of the witness' name and address from written statements; testimony via closed-circuit television or audio-visual links, such as videoconferencing, shielding the identity of the witness, by using a pseudonym, light disguise, voice alteration, or having them sit behind a veil or screen; or the removal of the public from the courtroom (*in camera* session). States are recommended to look into the variety of procedural measures that other States, as well as tribunals, use to protect witnesses in court, and where appropriate adopt such measures that conform to their international obligations and domestic legal frameworks and systems. This includes an assessment of whether current legislation permits such procedural protective measures and whether the measures are technologically feasible.

These measures may impact the rights of the defendant "to examine, or have examined, the witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him" pursuant to article 14, paragraph 3 (e) of the ICCPR. The rights of the defendant and the public perception of the legitimacy of the judicial institutions are best served with a limited use of classified information or closed proceedings. Therefore, a conviction should not solely be based on classified or secret testimony nor on evidence that has been redacted or summarized.

Recommendation 25: Adopting a tailored, flexible, and comprehensive approach to questioning, assisting, and protecting witnesses

It is important to adopt a tailored, flexible and, comprehensive approach when questioning, assisting, and protecting witnesses in order to obtain accurate and reliable information about what has occurred. When interviewing witnesses, all relevant elements should be taken into account, such as age, gender, and mental capacity. Certain circumstances require that special attention be paid to certain individuals or groups, such as women, the elderly, or children. Moreover, to avoid additional trauma and re-victimization, special attention needs to be paid to victims of terrorism acts, including women who have suffered from sexual crimes committed by terrorist organizations. For those vulnerable witnesses, the above-mentioned procedural protective measures, including the use of video-technology or in-court psychological assistance, may be more pertinent than for other witnesses. Recognized, assessed and approved NGOs that have experience with dealing with vulnerable people can be of assistance in the context of witness assistance, which is to be differentiated from witness protection. In those circumstances when evidence is collected by the military, military personnel should be aware that the persons they interview may be intimidated by them, which could impact the reliability of the witness statement. Hence, institutional/cultural sensitivities, or simply how one will get across, must be taken into account. Finally, witness protection should be understood in a broad and comprehensive manner; measures should be implemented as early as possible, and not only physical/security-related threats, but also the well-being and dignity of persons should be taken into consideration, including the emotional stress that testifying in court can engender. States are thus recommended to develop a tailored, flexible, and comprehensive approach to questioning, assisting, and protecting witnesses.

Recommendation 26: Assisting persons possessing sensitive or classified information to testify

Persons possessing sensitive or classified information – for example intelligence officers – may be reluctant to testify in court, but the specific protective measures as presented in Recommendation 24, where appropriate, may facilitate such testimony nonetheless. However, it has been noted that when they do, judges have sometimes found the statements of such persons, including of intelligence officers from foreign services, not credible, and not because of the (lack of) information such persons possess, but because of the way it was presented. To avoid crucial information from not being taken into account by the judge for such reasons, States are recommended to invest more in assisting persons who may not be familiar with providing a testimony in a (foreign) court, including intelligence officers and other persons whose information may be key to the case. If States invest in familiarizing the individuals with effective delivery of their statements/explain what it is like to testify in court and how one should behave and interact with the judge, their witness statements may be found more credible, which, in turn, may lead more quickly to a successful conclusion of the case.

Recommendation 27: Establishing witness protection programs

Next to procedural protective measures in court, a State may decide to establish a witness protection program based on an analysis taking into account, among other things, the available resources, the will to prosecute terrorism-related crimes based on witness statements, and the frequency of violence against witnesses. Sometimes, witness protection programs allow for relocation in other countries, including for immediate family members. Programs can be located within or outside the police force, and there are also models where programs are implemented by a multidisciplinary body. Whatever the approach, States are recommended to ensure that there is separation from the investigation, confidentiality of procedure and operations, and organizational autonomy from the regular police. Dedicated resources and close coordination between relevant national actors are absolutely vital in this context. States are also recommended to continuously provide multidisciplinary training that will

enhance the confidence of other States in their capacity to protect witnesses and thus strengthen international cooperation on witness relocation.

Recommendation 28: Strengthening the use of expert witnesses in court

In view of the increasing use of very technical forms of evidence, such as electronic evidence or forensic evidence, courts are likely to make more and more use of expert witnesses. Considering the technicalities involved, it may be difficult to assess what is actually being said (the substance of the statement) and the expert-level of the witness in question. In all cases where witnesses are heard in court, it will boil down to the question of how reliable and convincing the judge finds the statement of the witness in question, which may be contested by another (expert) witness brought forward by the defendant in the criminal proceedings. To be able to make that assessment, a judge must understand the statement and furthermore, must be confident that the expert witness is in fact an expert. Experts are well advised to speak clear and plain language and to answer the questions asked to them in a comprehensible way. To avoid unnecessary and cumbersome litigation about the alleged expertise of an expert witness, States are recommended to develop mechanisms that can assist in streamlining the process of using expert witnesses in court. While challenging, an example could be the creation of an (inter)national list of accredited and qualified expert witnesses on a specific area. Besides accreditation and certification of experts, standardization of how certain evidence should be interpreted could be helpful. States are recommended to cooperate with the ISO to consider where standardization of other forms of very technical evidence such as forensic evidence would be possible. Another best practice is that in complex cases, the defense and prosecution experts exchange reports before the trial commences. Any areas of disagreement are addressed and discussed and only afterwards presented to the court. When experts meet and are able to discuss areas of disagreement, they usually become very minimal and may even disappear completely.