Criminal Justice Sector and Rule of Law Working Group

Recommendations for Using and Protecting Intelligence Information In Rule of Law-Based, Criminal Justice Sector-Led Investigations and Prosecutions

Introduction and Guiding Principles

In implementing effective counterterrorism (CT) strategies, many States have recognized the benefits of a collaborative and cooperative relationship between law enforcement and intelligence agencies. Underscoring the critical role that intelligence and sensitive law enforcement information can play in the prevention of terrorism, Good Practice 6 of the *GCTF Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector (Rabat Memorandum)* encourages States to enact rule of law-based measures to protect the sources and collection methods of such information in terrorism cases. Once developed, these legal safeguards may allow investigators and prosecutors to use intelligence and sensitive law enforcement information as evidence, as appropriate, in a manner that both protects the sources and collection methods and maintains the accused person's right to fair trial as recognized under national and international law, including human rights law.

Although a number of States have made substantive progress in achieving the goals of Good Practice 6, numerous challenges remain for sharing intelligence and law enforcement information for the purposes of investigations and prosecutions. At various multilateral meetings, CT practitioners have highlighted these challenges and advocated for targeted training and other capacity-building assistance to support the development of appropriate legal mechanisms and technical capabilities that might address concerns about more open and consistent information sharing.[1]

In response, the GCTF convened two expert-level meetings to examine how to effectively implement Good Practice 6 of the *Rabat Memorandum* across different legal systems and the issues that can arise in the course of such implementation. The first meeting was held in January 2014 in Frankfurt, Germany, and the second in July 2014 in Vienna, Austria, held in conjunction with the Terrorism Prevention Branch of the United Nations Office on Drugs and Crime. Some of the critical issues that the experts considered included the following:

1. What coordination mechanisms, along with appropriate legal and administrative frameworks, should a State have in place to support the appropriate, effective, and timely sharing of both intelligence and sensitive law enforcement information within its system of government?

[1] For example, UN Counter-Terrorism Executive Directorate (CTED) organized a prosecutors' seminar in June 2012 in Ankara. For the full report, see http://www.un.org/en/sc/ctc/docs/2011/2011-12-16_ankara_prosecutorseminar.pdf.

2. What is the appropriate role/relationship between prosecutors, investigators and intelligence agencies at the investigation phase of a case?[2]

3. What types of legal safeguards should be enacted to govern the use of intelligence information in criminal proceedings that will effectively protect the sources and collection methods of the information while ensuring the right of the accused person to a fair trial?

At the meetings, the experts agreed that it would be useful to develop a set of non-binding recommendations to assist interested States in the application of Rabat Good Practice 6. The experts recognized that sensitive law enforcement sources and information are generally protected from disclosure during the course of investigations and judicial proceedings by the laws and regulations of most States, and the topic is well addressed by other Rabat Good Practices and international instruments. Therefore, the experts agreed that the below recommendations should focus on the use and protection of intelligence information in rule of law based investigations and prosecutions.

Experts also emphasized that, like all other measures taken to counter terrorism, the use and protection of intelligence in criminal proceedings should be in conformity with domestic law and policy and international law, including international human rights law.[3]

The experts also agreed that to ensure States and their intelligence agencies are accountable to their citizens for their actions, there should be specific and comprehensive legislative frameworks in place that define the mandate of intelligence agencies and their respective legal authorities under domestic law. The collection of intelligence, pursuant to a rule-of-law framework, is necessary to facilitate the appropriate use of intelligence information as evidence in criminal investigations and proceedings.

The proposed recommendations below are intended to assist interested States to effectively implement Rabat Good Practice 6. States are encouraged to incorporate as many of the recommendations as appropriate to their circumstances and consistent with their domestic laws and policies.[4]

---

[2] In some States, the role the prosecutor should play includes: (a) ensuring that investigations comply with applicable domestic and international law; (b) providing input, as appropriate, to choices being made by law enforcement and intelligence agencies and the tools being employed by such agencies to collect information at early but critical phases of a case; and (c) obtaining court authorization, where appropriate, for use of special investigative techniques.

[3] It was especially noted that effective oversight is necessary to ensure that cooperation between law enforcement, investigative officials and intelligence services is not used as excuse to "outsource" investigative requirements to intelligence services to avoid specific restrictions imposed on law enforcement agencies.

[4] States are also encouraged to refer to the report of the UN special rapporteur on the topics of fair trial and oversight of intelligence services in the CT context. The reports are available at: http://www.ohchr.org/EN/Issues/Terrorism/Pages/Issues.aspx

Recommendation 1: Respect for rule of law and human rights.

States should make sure that the use of intelligence in criminal investigations and prosecutions is done in a manner that respects the rule of law under both domestic and international law, in particular international human rights law. States should implement effective processes and procedures to ensure that, in compliance with due process and the right to a fair trial, intelligence can be effectively and appropriately used in criminal investigations and prosecutions. To ensure that the principle of legality is upheld and that the right of the accused to a fair trial is preserved, State practice should:

- Incorporate the procedures for cooperation between intelligence agencies, law enforcement, and, as appropriate, judicial officials in the legal and regulatory framework governing those agencies.
- Effective oversight, mechanisms and systems governing the cooperation between intelligence agencies and law enforcement to ensure that investigations are not being "outsourced" to intelligence agencies to avoid specific legal restrictions imposed on law enforcement.
- Include laws and policies which fully describe the purpose, procedures, means, and methods for protecting intelligence information, sources, methods, and witnesses in criminal investigations and trials that are designed to ensure the right to a fair trial of the accused, including:
    - the implementation of protective measures should be done in a manner that ensures the essence of the case is disclosed to the accused allowing for an effective defense;
    - that the same protective measures are, where appropriate, available to the defense when it needs to use intelligence information; and
    - that the imposition of protective measures for witnesses or information does not affect the ability to conduct a fair and impartial investigation and adjudication of reported violations of human rights related to the witness or information.
- Avoid basing a conviction solely on the testimony of an anonymous or "secret" witness nor on evidence that has been redacted or summarized.[5]
- Include laws and policies that address the use of "tainted" intelligence information, that is, information that may have been obtained by means that may violate international human rights law, in particular the prohibition of torture.

[5] States should recognize that the misuse or overuse of "secret" evidence or witnesses may pose a risk to the public perception of the legitimacy of the judicial institutions.

I. Relationship between Law Enforcement and Intelligence Agencies

Recommendation 2: States should have mechanisms and procedures that allow intelligence information relevant to terrorism threats to be shared, where appropriate, with authorized law enforcement personnel.

Intelligence can exonerate as well as inculpate suspects, and States should establish procedures to allow properly-authorized investigators and prosecutors to receive intelligence information, where appropriate, that is relevant to a particular criminal investigation. Such procedures help to ensure investigators and prosecutors are in a position to make the best informed investigative and prosecutorial decisions in terrorism cases, which, in turn, can enhance the protection of human rights and promotion of the rule of law.

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. Those States that already have well-developed legal frameworks and procedures to address this issue generally take one of two recognized approaches, which can, more or less, be viewed as the "common law" approach and the "civil law" approach. The primary difference between the two approaches is the purposes for which the intelligence information can be used and the point in the case at which that decision is made. Both approaches have a common starting position, and that is to determine if the information can be declassified without harm to the sources, methods, witnesses, or national security, so that it may be included with all other evidence or information in the case. If the information cannot simply be declassified, that is where the two approaches diverge.

Most states that follow the civil law approach cannot include intelligence information in the case file as evidence. Rather, intelligence is provided to prosecutors, police, or magistrates/ investigating judges for lead purposes so that a law enforcement investigation may be directed towards collecting the necessary evidence. Under the civil law approach, all issues related to the use and protection of intelligence information are generally addressed in the investigative phase of the case. In those States that follow the "common law" approach, intelligence information can generally be used to both support an investigation and in trial as evidence. The investigators, and sometimes prosecutors, work with the relevant intelligence agencies to identify what classified or otherwise sensitive national security information is relevant to the case. The prosecutor then addresses the issue of what the intelligence information can be used for and in what form it will be disclosed with the trial court through motions in the pre-trial phase of the case.

In a third blended system, States maintain a separation between law enforcement and intelligence based on legal precedent or evidentiary rules that hold that too much interaction will result in a conclusion that the intelligence agencies are aligned with the prosecution and/or because such interaction could result in the disclosure of sensitive intelligence information in judicial proceedings. Where such a separation currently exists under domestic law or policy, States should establish procedures, as noted above, to allow for the limited referral of pertinent intelligence information to law enforcement personnel to support criminal investigations and judicial proceedings where appropriate.

It should be noted that in most States, even when intelligence information is shared with law enforcement personnel, the information remains under the control of the relevant intelligence service or agency from which the information originated. In such situations, the actual use of information, once disseminated, remains under the control of the originator. For example, even if specific intelligence information might be useful in obtaining a search warrant or in requesting authority to engage in electronic intercepts, that information may only be used for such purposes if the originating intelligence service or agency consents to such use and the manner in which it is to be used.

Where it appears that classified intelligence or other sensitive national security information is relevant to a criminal matter and needs to be provided to law enforcement or judicial personnel, States should ensure that their procedures allow for the sufficient oversight and independent review of the information to ensure that the appropriate balance between national security and the right to a fair trial of the accused are considered. States that have well developed systems have created different models to achieve this. For example, one State uses an independent commission to review the relevant intelligence and decide if it should be declassified and turned over. Another State uses a national level terrorism prosecutor – who is not involved in the case – to review all relevant intelligence and decide what should be turned over. Another model used by several States is the "fusion" center concept whereby the relevant law enforcement, prosecutors, and intelligence services of the State meet regularly, perhaps daily to share and discuss relevant information. One way of developing an effective fusion center is for the various personnel to share a location for the operational phase of an investigation, allowing intelligence to be discussed daily and facilitating joint decisions on whether and how intelligence can be used in the case.[6] Financial intelligence units may also consider having their own internal law enforcement unit that can play such a role.

Recommendation 3: Where appropriate, intelligence agencies should be informed on how intelligence information gathered and material captured might impact a criminal investigation or prosecution, especially when such information is intended to be used in proceedings. For example, in accordance with the defendant's right to due process, such information may be disclosed to the defendant or the information might be useful to the government as evidence in criminal proceedings.

To facilitate instances where intelligence information may be appropriately used to support law enforcement activities, 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. Such mechanisms or procedures may, if and where appropriate, allow intelligence agencies to consider how specific intelligence products might be crafted for use by relevant law enforcement consumers. Having law enforcement personnel work side-by-side with relevant intelligence counterparts may help to optimize the appropriate use of relevant intelligence information to support law enforcement investigations and judicial proceedings. By the same token, having prosecutors involved early in particular

[6] States which do not yet have effective cooperation and information sharing regimes may want to consider the following framework as a method to develop their regime: (a) establish mutual understanding through consistent engagement; (b) conduct interagency assessments of possible terrorist activity and coordinate plans of action; (c) promote intelligence sharing based on a mutually-agreed standard format; (d) acknowledge the need for real time information sharing; and (e) promote a culture of responsible information sharing and integrate and maximize information sharing capabilities.

investigations, whether undertaken by intelligence or law enforcement officials, can aid in preserving prospective judicial options.

For States that recognize a direct relationship between investigative personnel or prosecutors and intelligence agencies, some aspects of the role the investigative officials or prosecutors should play include: (a) evaluating whether the investigations comply with applicable domestic and international law, including international human rights law; (b) providing input, as appropriate, to choices being made by law enforcement and/or intelligence agencies and the tools being employed by such agencies to collect information at early but critical phases of a criminal case; (c) advising, as appropriate, how intelligence can be collected in a manner that will make it more likely to be admitted in Court when criminal charges are foreseen and will ensure that sources and methods will not be exposed during the criminal proceedings; and (d) in applicable legal systems, obtaining court authorization for use of special investigative techniques.[7]

II. Transforming Information Gathered in Clandestine Investigations into Evidence

Recommendation 4: Upon receipt of intelligence information, law enforcement personnel should evaluate the authenticity or reliability of the information and determine how it may best be used under their legal system, if at all, to support an investigation or as evidence in a prosecution.

After appropriately receiving intelligence information relevant to a criminal investigation, law enforcement personnel, prosecutors, and/or judicial personnel should evaluate, subject to the State's relevant law and procedures and together with relevant intelligence services or agencies where appropriate, the authenticity or reliability of the information and determine whether and how the intelligence may appropriately be used, if at all, to facilitate a law enforcement investigation or support a prospective prosecution. For example, in the different legal systems, such use might include: leading law enforcement personnel to new lines of inquiry; using intelligence to support applications for judicial approval for special investigative techniques; as expert evidence or testimony; and, as background information to understand the activities, capabilities, and intentions of a terrorist network under investigation.

In determining the authenticity or reliability of the intelligence information and whether it can or should be used to support an investigation or prosecution, consideration may be given to, *inter alia*, the legal authorities under which the intelligence was collected, the means or techniques by which the intelligence was collected, and the reliability of the source of the information. Such considerations may inform whether the use of the intelligence in a criminal proceeding is appropriate or, in certain instances, potentially prohibited under domestic or international law, including international human rights law.

[7] Officials involved in these situations should remain mindful that while intelligence agencies and law enforcement may use similar investigative techniques, they operate under very different legal authorities and for different purposes.

III. Protection of Witnesses and Intelligence Information at Trial (Rabat Good Practices 1 & 6)

Recommendation 5: States should have mechanisms and procedures for guaranteeing that relevant sources and methods that underlie intelligence information provided to law enforcement or judicial officials – the disclosure of which would jeopardize national security, as well as any witnesses who are linked to or give evidence related to that intelligence – are sufficiently protected.

Intelligence information appropriately shared with law enforcement or judicial officials may be useful as potential evidence in supporting a criminal proceeding, but such sharing may create an obligation to disclose the information to the defendant or publicly pursuant to the defendant's right to a fair trial. States should have procedures and mechanisms for dealing with such obligations.

As discussed in Good Practice 1, the right to a fair trial should be maintained in prosecutions that involve intelligence information used as evidence. At the same time, national security concerns may require States to seek to protect the sources and methods of the intelligence information, as well as any witnesses who may testify regarding such information, whose name or identifying information appears in records disclosed to judicial authorities or the accused or who otherwise require protection while testifying in a criminal proceeding based on their association with intelligence activities.

To achieve the balance between the accused's right to a fair trial and the protection of national security and witnesses, States have created various legal regimes, including: (1) using intelligence information solely for lead purposes for law enforcement, which must then develop evidence through law enforcement techniques; (2) using an independent commission to review the relevant intelligence and decide if it should be declassified and turned over; (3) using a national-level terrorism prosecutor – who is not involved in the case – to review all relevant intelligence and decide what should be turned over; (4) appointing a "special advocate" for the defense who will have the ability to review the intelligence information, to assist the defense; (5) having a separate judicial process to review the information, conduct the necessary assessment, determine whether the information should be disclosed and in what form; and (6) having the trial court determine how best to handle the disclosure of intelligence information in criminal proceedings.[8] In some of the States that use the latter regime, the role of the prosecution is to propose to the court the form and manner in which the information should be presented to the fact finder so that such presentation is consistent with the position of the originating intelligence agency and the requirements of national security. The court then considers the proposal to determine if the right to a fair trial is guaranteed.[9]

No matter which legal regime a State currently implements, some additional practices which States may want to consider that strengthen the protection of national security concerns while at the same time further protecting the right to a fair trial of the accused, include: (1) providing security clearances to defense counsel to enable the government, where

[8] In all such instances the Court needs to determine that the summaries of the information, stipulations of fact and/or redacted versions are sufficient to meet the right to a fair trial.

[9] States that use this type of regime generally allow the evidentiary hearings to be held *ex parte* and *in camera*.

appropriate, to discuss, and provide such counsel with, relevant intelligence information; (2) mechanisms that ensure the review of all evidence and resolution of any issues related to that evidence occur and are resolved before double jeopardy attaches to the proceeding; (3) where applicable, rules of procedure that ensure all evidentiary rulings involving the handling of intelligence information in criminal proceedings are immediately appealable to a higher court without the need first to proceed to trial; and (4) rules of procedure which make it clear that a prosecution cannot be ordered by any judicial official or court to proceed to trial where such a proceeding will require an unacceptable risk of disclosure of intelligence or other national security information. Implementation of procedures such as those above may help to ensure both the right to a fair trial and the protection of national security.

Regardless of the legal regime used to protect the intelligence information, most States provide similar protection to witnesses who are associated with or whose testimony addresses intelligence information.[10] As a general rule, the level of protection provided to a witness should be based upon the seriousness of the threat to the personal safety of the witness and his or her family or the level of the threat to national security based on the risk of disclosure of sensitive intelligence sources and methods or other national security information. Some of the protections that are available in some States include: (1) orders limiting the witnesses' testimony to only what is directly relevant to the proceedings; (2) orders that prohibit the defense from pursuing certain lines of inquiry or limit the questions to only specific topics without impacting the accused's right to a fair trial; and (3) allowing a witness to testify using one or more of the following measures to prevent his or her true identity from being known to the defense or the public – a pseudonym, light disguise, voice alteration, sitting behind a veil or screen. Many of these remedies already exist in the criminal law of many States in instances where law enforcement needs to rely on sensitive law enforcement assets for proof or evidence. For example, in affidavits in support of search warrants, some systems allow for sensitive human sources to be sometimes described in very general ways, rather than by name. States should consider the prospective usefulness of similar tools to secure information from intelligence service representatives, whether at trial or other judicial proceedings.

[10] The term "witness" as used here includes fact witnesses, "expert" witnesses, foundation witnesses, informants and victims.

IV. Protection of Intelligence Information Shared Between States

Recommendation 6: To facilitate international intelligence-sharing with regard to countering terrorism, States should develop processes and mechanisms to permit the sharing of relevant intelligence where appropriate, while ensuring the source State maintains control over how that intelligence is used by the receiving State.

Because terrorism is a threat to international peace and security, successful CT efforts require effective international cooperation. At the same time, a State must be able to retain control over the use of intelligence information it collects and/or develops even when that information is shared with other States. This is sometimes referred to as "originator controlled" sharing.

Under this principle, intelligence that has been provided to the receiving State should not be used for any purpose other than that for which it was specifically provided. For example, intelligence that was shared with another State for prevention of an act of terrorism could not be used by law enforcement for any other purpose or in any judicial proceeding without the express consent of the source State. The source State's discretion not to permit its use in the receiving State's domestic proceedings should remain unfettered.

States should have rules of procedure and evidence in place that would prevent the admission intelligence collected by another State in a manner that violates fundamental human rights, such as information obtained through torture. Given that it can be difficult to guarantee that the intelligence gathered by the requested State was collected in a manner that did not violate fundamental human rights, all States should undertake to implement practices that, if fully implemented, would provide the assurances necessary to overcome challenges to its intelligence collection methods.

Other measures that can facilitate greater sharing of intelligence information between States include:

- Promotion of respect for human rights by intelligence agencies by all States;
- Providing assurances to States as to how their sensitive information will be handled and protected with regards to mutual legal assistance requests;
- Working closely with other States and foreign prosecutors to ensure disclosure requirements can be met;
- Written agreements on the collection and use of information between intelligence agencies;
- Cooperation and coordination in covert investigations to allow for the product of those investigations to be used in several different jurisdictions;
- The use of regional agreements to foster cooperation; and
- Use and enlarge existing networks and improve existing best practices concerning international information exchange.

Recommendation 7*: *Training and Capacity Building

Intelligence collection and law enforcement are both traditional functions intended to support safety and security in all States. Yet they operate under different legal authorities and policies and, usually, for different purposes. As a result, historically intelligence and law enforcement agencies have had little interaction and rarely shared information. The global nature of terrorism mandates effective cooperation and information sharing between intelligence agencies and law enforcement at the national, regional and international levels. To achieve the necessary cooperation and information sharing States should consider implementing effective training and capacity building programs for all of the relevant CT actors, including intelligence officials, law enforcement officials, prosecutors, judges and other judicial officials, and parliamentarians. The training must be both targeted, so that each actor can understand the roles, responsibilities, requirements, and legal authorities of the other actors, and joint, so that all of the actors can learn how to effectively cooperate, collaborate and share information – all within a rule of law framework with full respect for human rights.