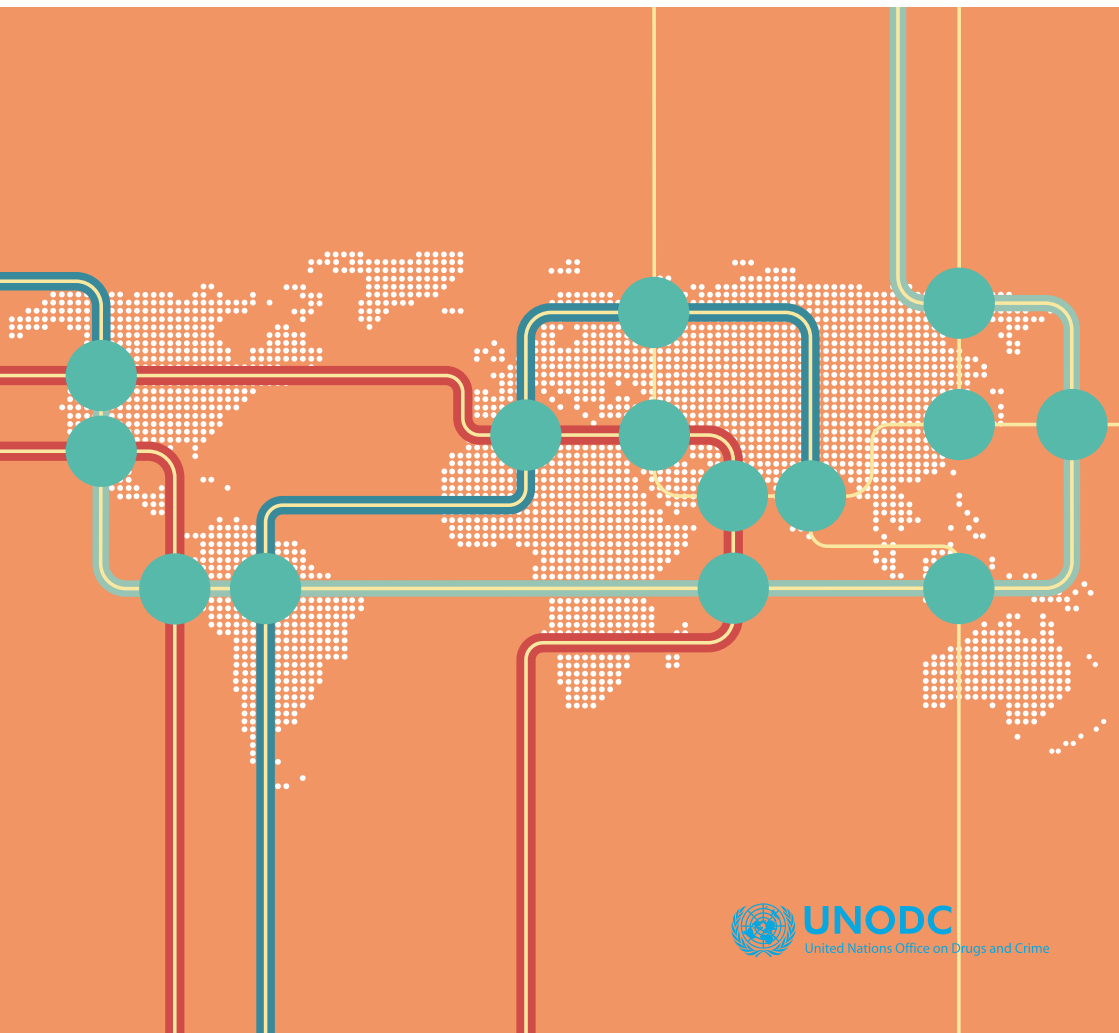


# Countering Terrorism and Foreign Terrorist Fighters: A field guide for frontline officers



Copyright © United Nations Office on Drugs and Crime, 2018. This field guide was produced by the United Nations Office on Drugs and Crime, Regional Office for Southeast Asia and the Pacific, in Bangkok, Thailand.

This is not an official document of the United Nations. The designations employed and the presentation of the material in this document do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations Office on Drugs and Crime concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitations of its frontiers and boundaries.

UNODC would like to recognize the contribution of the Government of Australia, the Government of Canada and the Government of the United States of America.

To view this publication from a mobile device or to access other UNODC publications, please scan the QR code.



This content is updated regularly with new information. For the latest version of content and to access other materials and tools please visit the QR code.

# Countering Terrorism and Foreign Terrorist Fighters: A field guide for frontline officers

This publication contributes to Sustainable Development Goal 16 that seeks to: “Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels”



The Sustainable Development Goals are the blueprint to achieve a better and more sustainable future for all. They address the global challenges we face, including those related to poverty, inequality, climate, environmental degradation, prosperity, and peace and justice. The Goals interconnect and in order to leave no one behind, it is important that we achieve each Goal and target by 2030.

# INTRODUCTION

Terrorism is not a phenomenon that is unique to the late 20th and early 21st centuries nor is it restricted to Islamic fundamentalists. Terrorist activities have been used throughout the centuries as a means of challenging a central government or military power. As far back as the Roman Empire local populations used terrorist activities as a means of challenging the Roman occupation of their lands. The term terrorism actually derives from the regime de la terreur that prevailed during the French revolution in 1793-94.

What has emerged in recent times is the engagement of states in funding and supporting terrorist activities, and from that we now have the term State Sponsored Terrorism. The assassination of an Austrian Archduke by a Bosnian nationalist trained and equipped by Serbia was the flashpoint that led to the start of World War I.

Even now state sponsored terror is used to fund terrorist groups and activities in neighbouring countries to destabilise and sow discord. Who can forget the falling of the Twin Towers in New York that led to the current war on terror. The emergence of al Qaeda and its affiliates and offshoots and the spread of Islamic fundamentalism to South East Asia.

As a frontline law enforcement officer, you may encounter suspects who are foreign terrorist fighters who are moving through your country to travel to conflict zones, or who are returning to their country from these same zones or who intend to use your country as a base of operations. This field guide will help you to understand how to develop strategies to identify these individuals and how to collect intelligence and evidence of their criminal activities.

You should carry this field guide with you while you are on duty. It contains quick-reference tools to address situations you are likely to experience in the course of your duty.

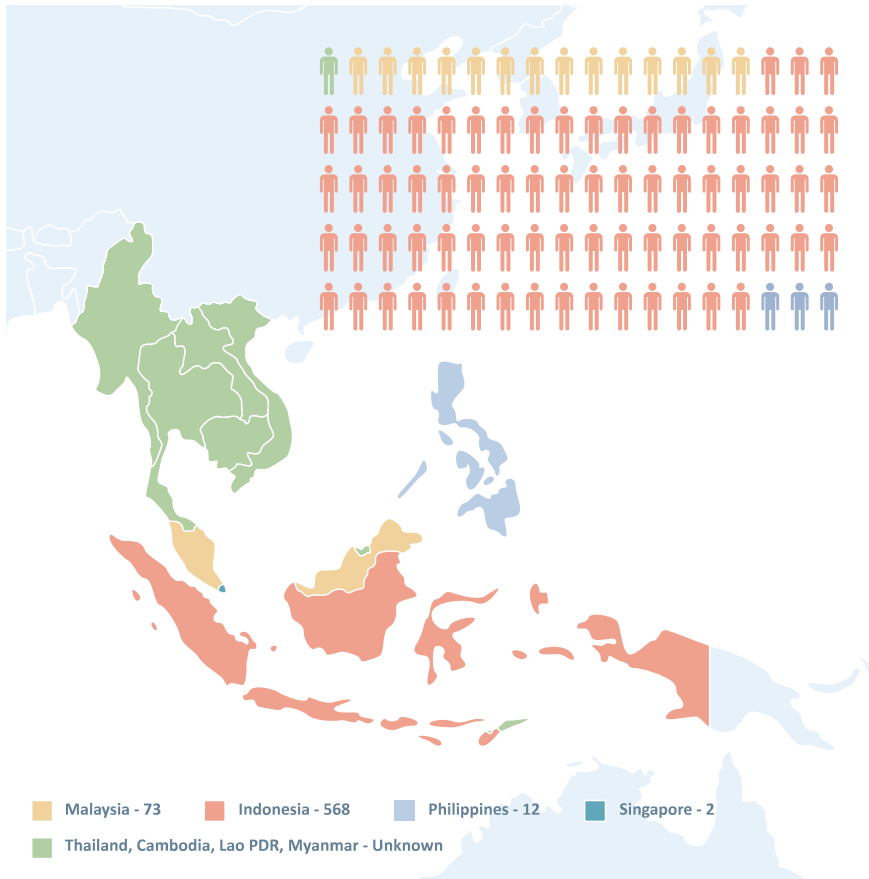
## Table of Contents

1. Terrorism and Foreign Terrorist Fighters	6	7. Sources of Information on Terrorist Groups	14
2. International Legal Frameworks to Combat Terrorism	7	8. The Internet and Terrorism	16
3. National Legislation	8	9. Risk Profiling Foreign Terrorist Fighters	19
4. Investigating Terrorism and Foreign Terrorist Fighters	9	10. Interviewing Suspects	21
5. Terrorist Groups Active in Multiple Regions	11	11. Securing the evidence	24
6. Terrorist Targeting and Methods	12	12. Chain of Custody	26
		13. Financial Investigations	27
		14. Sharing Intelligence	29

# 1. TERRORISM AND FOREIGN TERRORIST FIGHTERS

There are many different definitions of terrorism, some relate to country specific legislative requirements while others are more general in nature. The United Nations resolution 49/60 seeks to criminalise several armed activities that are considered ‘terrorist’ in nature. The resolution defines terrorism as:

“Acts intended or calculated to provoke a state of terror in the general public. A group of persons for political purposes are in any circumstances unjustifiable, whatever the consideration of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them.”



## 1. TERRORISM AND FOREIGN TERRORIST FIGHTERS

A “foreign fighter” has been defined as “an individual who leaves his or her country of origin or habitual residence to join a non-State armed group in an armed conflict abroad and who is primarily motivated by ideology, religion, and/or kinship.”

The term “foreign terrorist fighters” (FTF) is to be found in United Nations Security Council resolution 2178, which defines them as “individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict”

FTF can be differentiated from mercenaries and employees of private (military or security) companies in that the latter are usually recruited by States/governments and they join the warfare out of lucrative motives (though payment of salaries by ISIL (Da’esh) has been reported to be a financial incentive for some FTF).

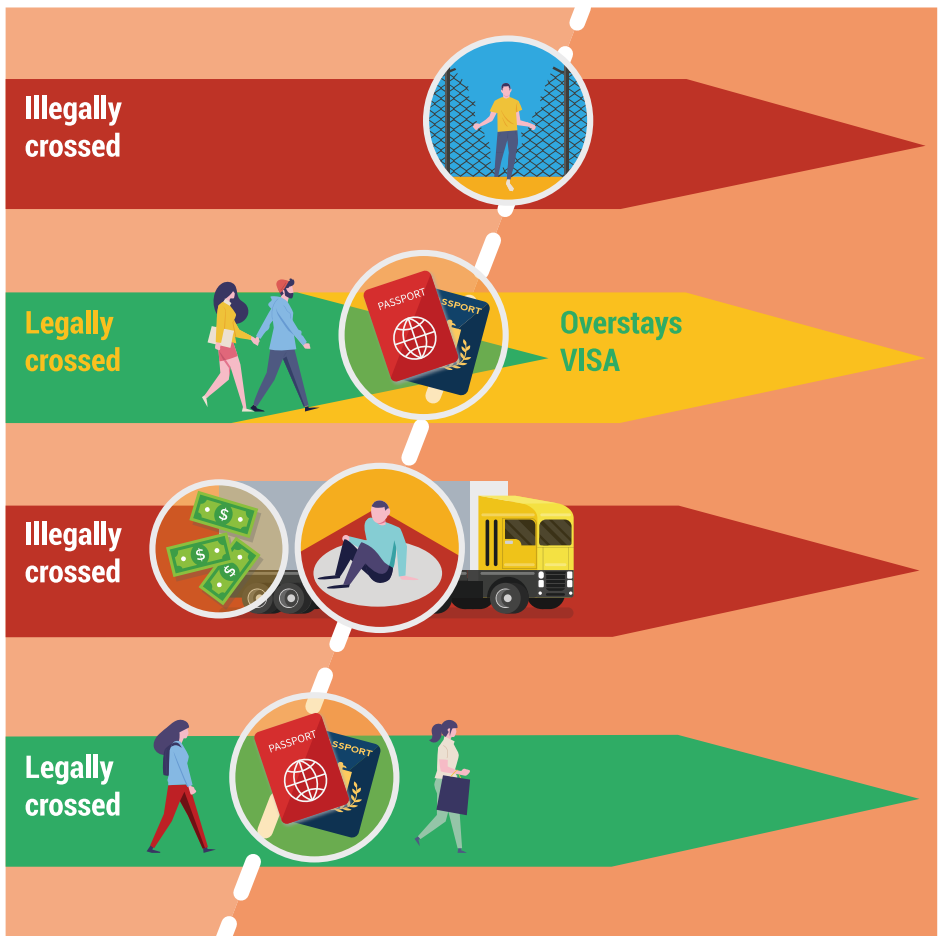
There are several types of individuals that become FTF’s. These include:

1. The Revenge Seeker, frustrated and angry and seeking an outlet to discharge that frustration and anger towards some person, group or entity whom he may see as being at fault
2. The Status Seeker, seeking recognition and esteem from others
3. The Identity Seeker, primarily driven by a need to belong and to be a part of something meaningful and seeking to define their identities or sense of self through their group affiliations
4. The Thrill Seeker, attracted to the group because of the prospects for excitement, adventure, and glory.

## 2. INTERNATIONAL LEGAL FRAMEWORKS TO COMBAT TERRORISM

Terrorism continues to pose a major threat to international peace and security. In addition to the devastating human cost of terrorism, its core aims are to destabilise governments and undermine economic and social development.

In response to the terrorist threat the international community has developed a common universal legal framework against terrorism. This framework is comprised of the 19 universal legal instruments against terrorism along with United Nations Security Council Resolutions. The



## 2. INTERNATIONAL LEGAL FRAMEWORKS TO COMBAT TERRORISM

implementation of these conventions, protocols and resolutions is informed by the guidance provided by the UN Global Counter-Terrorism Strategy along with the United Nations General Assembly Resolutions.

The United Nations Security Council, acting under Chapter VII of the United Nations Charter, adopted resolution 2178 on 24 September 2014. This resolution requires States to, inter alia, ensure that they have in place laws that permit the prosecution of: a) FTF, b) those who willfully fund or receive funds to finance the travel of FTF and c) those who wilfully facilitate the travel of FTF.

It further calls upon States to enhance international, regional and sub-regional cooperation to prevent and suppress the phenomenon of FTF, including to prevent the travel of FTF from or through their territories.

Several UNODC reports may assist you in gaining a greater understanding of the international legal frameworks in relation to terrorism and FTF's. These reports can be found here:

[https://www.unodc.org/unodc/en/terrorism/technical-assistance-tools.html#Practical\\_guides](https://www.unodc.org/unodc/en/terrorism/technical-assistance-tools.html#Practical_guides)



You should make yourself aware of the relevant pieces of legislation within your country that address terrorism, FTF's and related offences. Often this will be your penal code, but there may also be other legislation that will address specific issues such as anti-money laundering, financing of terrorist activities, immigration offences and FTF's.

During the investigation of terrorism or FTF's, several different agencies may play a role. The illegal movement of people may fall under the jurisdiction of the Immigration or Customs Departments assisted by the Police whereas being an FTF or money laundering may be a police matter. It is important to know what other agencies can assist you or who have jurisdiction in a terror related or FTF investigation.

It is also important that you advise your intelligence services of your investigation and seek their advice. These agencies frequently share information with their international counterparts and it is important that you do not inadvertently compromise one of their operations.

Several UNODC reports may assist you in gaining a greater understanding of your national legal frameworks in relation to terrorism and FTF's. These reports can be found here:

[https://www.unodc.org/unodc/en/terrorism/technical-assistance-tools.html#Practical\\_guides](https://www.unodc.org/unodc/en/terrorism/technical-assistance-tools.html#Practical_guides)



## 4. INVESTIGATING TERRORISM AND FOREIGN TERRORIST FIGHTERS

Terrorism is often targeted at the state, or sponsored by the state, so national intelligence services (NIS) will often figure prominently in combating terrorism or the investigation of terrorism related offences or activities. You should ensure that you communicate your intelligence and evidence to your national Counter Terrorism Unit (CT) or to the NIS and keep them apprised of developments.

Similarly, the monitoring of communications and individuals is often crucial for deterring or preventing acts of terror and it is often this surveillance that provides intelligence and evidence of planned criminal activities. These investigations will generally be carried out by the NIS or CT units or and not at the local level. However, it is often intelligence derived from local sources that is the catalyst for identifying a terrorist cell or FTF.

Before you commence any investigation into a terrorist network or FTF ask yourself these questions:

- Have I identified a possible terrorist or FTF??
- Do I have a legal basis for my investigation?
- Have I identified the offences that have been/suspect of being committed?
- Do I have sufficient resources to undertake the investigation?
- What are my department's procedures?
- Have I shared this information with my NIS or CT Units?
- Am I the right person to be conducting this investigation?

## 4. INVESTIGATING TERRORISM AND FOREIGN TERRORIST FIGHTERS

Once you have satisfied yourself that you have addressed these questions then you will need to plan your investigation. You should prepare an investigation plan addressing your objects, milestones and strategies. At a minimum it should include:

- Relevant legislation and offence(s) committed?
- Suspect (if identified)?
- Resources you will need, human, financial and material?
- Does this case have a transnational component?
- Other agencies that may assist you.
- Terrorist organisation subject to investigation and its affiliates.
- Identify relevant investigative methods.
- Surveillance – physical and electronic.
- Undercover.
- Technical – phone interception.
- Controlled delivery.
- Informants.
- Crime scene.
- Analytical support.

You should utilise the full range of tools at your disposal to investigate terrorism related activities and the movement of FTF.



## 5. TERRORIST GROUPS ACTIVE IN MULTIPLE REGIONS

Terrorism is not restricted to one religious cause. While the last forty years has seen the rise of Islamic Fundamentalism, they are by no means the only cause pursued by terrorist organisations operating in the world. Terrorist organisations can emerge, adapt, change, expand or become irrelevant. You should make yourself aware of the terrorist groups that are operating within your country and the region.

Understanding the cause of the terrorist group(s) operating in your area will assist you in identifying investigative strategies and starting points. It will also help with your risk profiling of suspected terrorists or FTF.

According to studies undertaken globally and in specific countries, following is a list of terrorist organisations:

- **Abu Sayyaf Group**
  - Philippines – Asia
- **Al Qaeda**
  - Worldwide
- **New People’s Army**
  - Philippines
- **Jemaah Islamiya**
  - Indonesia – Asia
- **Islamic State of Iraq and the Levant (ISIL)**
  - Worldwide
- **Hakat-ul-Jihad-al-Islami**
  - Bangladesh
- **Indian Mujahideep**
  - India
- **Jamaah Ansharut Tauhid**
  - Indonesia, Thailand, Malaysia.
- **Lashkar e-Taiba**
  - Pakistan
- **Turkistan Islamic Party**
  - China



This list is not exhaustive, and you should consult your legislation and intelligence alerts to identify terrorists’ groups active in your country.

Terrorists have shown themselves to be adaptable, cunning and ruthless in the way they seek to bring about their political agenda. They are continuously seeking ways to develop new and innovative methods to defeat NIS and law enforcement efforts to disrupt, dismantle and degrade their capabilities. In some instances, they even revert to open warfare to achieve their goals, as we have seen in the Middle East and Africa,

As a frontline law enforcement officer, you need to be aware of the targeting rationale of terrorist organisations and the methods they use to achieve their desired goals. Remember, these may change as terrorist organisations react to new NIS and law enforcement strategies or identify ways to defeat current security systems. These lists are not exhaustive, and you should keep yourself up to date with any security alerts.

### **Targeting:**

- Government buildings, Embassy's, Police Stations
- Checkpoints
- Monuments/Landmarks
- Places of Worship
- Markets
- Areas where large numbers of people congregate such as bars, theatres, hotels and sporting venues, shopping centres
- Critical infrastructure, water, gas, oil, transport networks

## 6. TERRORIST TARGETING AND METHODS

### **Methods Used and examples (not exhaustive):**

- **Vessels**
  - USS Cole
- **Vehicles**
  - Thailand, Kenya, Indonesia, Philippines, France, Australia, United States
- **Aircraft**
  - United States
- **Suicide bombers**
  - Indonesia, Iraq, Syria, Philippines, Afghanistan, India, Sri Lanka, Thailand
- **Improvised Explosive Devices (IED)**
  - Iraq, Syria, Thailand, Philippines, Indonesia, Afghanistan, Belgium, Iraq
- **Mortars**
  - Iraq, Syria, Afghanistan, Israel.
- **Missiles**
  - Israel, Iraq, Syria
- **Firearms**
  - Thailand, Indonesia, Philippines, Afghanistan, Iraq, Syria, Nigeria, Kenya
- **Knives**
  - United Kingdom, Australia, France, Thailand, Indonesia, China
- **Kidnapping**
  - Mexico, Afghanistan, Iraq, Syria, Nigeria, Afghanistan

## 7. SOURCES OF INFORMATION ON TERRORIST GROUPS

The best source of information on terrorist groups and the movement of FTF's are often the foreign terrorist fighters themselves. They may be able to provide information on the methodology used by the terrorist groups to recruit, transport and equip the FTF's. This may include the identity of recruiters, relevant phone numbers and social media accounts, the number of smugglers involved, routes taken, vessels or vehicles used and locations of safe houses. Additional information can be gathered from a variety of different sources. These can be divided into 5 categories:

### Workers

- Fishermen
- Construction workers
- Street vendors
- Sex workers



### Service Providers

- Taxi drivers
- Bus operators
- Social workers
- Shipping agents NGOs



### Open Source

- TV/Radio
- Print media
- Internet



### Official Sources

- Officers from your agency
- Other government agencies
- International agencies
- Neighboring Border Liaison Offices



### Criminal Sources

- Informants
- FTF
- Terrorists
- Financiers
- Safe House Operators
- Transporters
- Document Suppliers

## 8. THE INTERNET AND TERRORISM

The internet has revolutionised the way we live. As technology has developed so too has the ability for terrorists to use this technology to facilitate their subversive and criminal activities. The advent of web-based encrypted communication applications, the dark web, social media and the increased sophistication of mobile telephones have provided terrorists with greater flexibility, anonymity and reach for their message. The use of the internet by terrorist groups to facilitate their goal is often called cyberterrorism.

Cyberterrorism is a major issue for law enforcement and intelligence agencies. Cyberterrorism and radicalisation occur on both the open web and the dark web. The promotion of extremist views, media releases, videos and images and crimes perpetrated to support terrorism all take place on the internet. Terrorist groups have even developed a number of applications to avoid electronic surveillance by intelligence and law enforcement agencies.

The dark web is a collection of websites operating on an encrypted network with hidden IP addresses - all of which give users strong anonymity protection. Because they are not indexed by traditional search engines, you can only access them with special anonymity browser, such as I2P, Freenet, and the most common, The Onion Router (TOR) bundle.

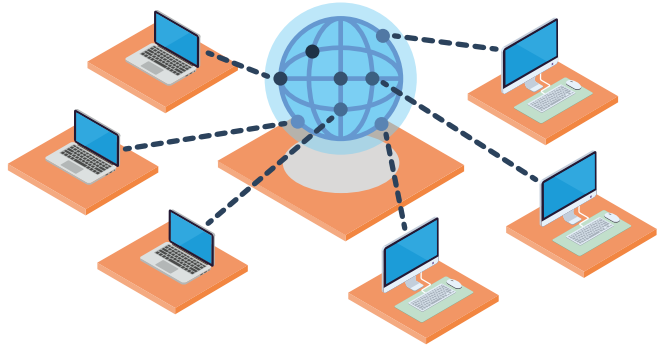
Several law enforcement and intelligence agencies have run successful major undercover operations targeting dark web users. If you believe that your terrorism case involves criminal activity on the dark web then you should consult with the speciality unit within your department that addresses cybercrime, if one exists. These types of operations require specialist training and equipment.

One area where you will find potentially valuable evidence and intelligence on terrorist related activities is through the analysis of suspects social media accounts. Social media offers law enforcement agencies the opportunity to gather intelligence on terrorist groups and individuals susceptible to radicalisation. The ability to map their network of



friends, images of their assets and notifications of where they are eating at restaurants, travelling on holidays, or meeting with friends may provide intelligence or investigative opportunities. Examples of social media sites include:

- Facebook
- Snapchat
- YouTube
- Twitter
- Instagram
- WeChat
- Zalo



Terrorists have been known to post photographs of themselves with firearms or from terrorist camps, wearing clothing linked to terrorist groups and promoting terrorist agendas. In some instances, the murder of opposing forces or innocents is recorded and posted on social media. In some jurisdictions you may be able to approach the operators of Social Media platforms seeking user information, you should check what options are available to you in your country.

While these platforms make it easier for terrorists to promote their agenda, they also present opportunities for investigators. You can use them as possible entry points for undercover investigators and for collecting intelligence and potentially evidence. Never use your own account to communicate with suspected terrorists on any of these sites. You should create or utilise covert accounts for your communications.

Should you communicate with suspects on these sites with a view to collecting evidence remember to:

- Ensure that your actions are legal within your jurisdiction
- Ensure that you have sought the permission from your supervisor
- Ensure that you notify your CT unit.
- Always use a covert account

## 8. THE INTERNET AND TERRORISM

- Screenshot the suspects profile – this can be changed by them at a later date
- Screenshot any messages between you and the suspects
- Record any videos or messages they send to you
- If possible do not share your photograph with a suspect
- If possible do not post your photograph on your covert profile
- Refrain from talking via video with the suspect
- Ensure chain of custody of any evidence you collect (see chapter 12)

Another area where you may collect valuable intelligence or evidence are web-based communication applications. These systems offer end to end encryption between users which makes interception difficult. Examples of these types of platforms include:

- WhatsApp
- Viber
- Line
- WeChat
- Telegram
- Wire
- Signal

The easiest way to collect evidence of a suspect's criminality using these platforms (prior to arrest) is to connect and communicate directly with them in an undercover capacity. If you have the suspects phone in your possession than you can collect the digital evidence through the use of a cell phone analytical tool such as Cellbrite, or the physical recording of messages, photos, videos, call records or audio conversations.

You should also be aware of applications on a suspect's telephone that may indicate links to terrorist networks. These include:

- **Tashfeer al-Jawwal** – encryption platform for mobile phones
- **Asrar al-Ghurabaa** – encryption platform developed by ISIL
- **Amn al-Mujahid** – encryption software
- **Amaq** – Used to disseminate information and allow user to change URL

## 9. RISK PROFILING FOREIGN TERRORIST FIGHTERS

Millions of young innocent men and women travel the world in search of adventure each year. Hidden amongst these young tourists are FTF's travelling to or from combat zones such as the Philippines, Iraq, Syria or Africa. The defeat of ISIS in Iraq and Syria has meant that many FTF's serving in these countries are making their way back to the country of origin or to other conflict areas.

These FTF's may be male, or female so it is important that you are aware of risk indicators that may assist you in identifying FTF's or potential FTF's. Suspect profiles are NOT designed to screen for any particular race, religion or political class.

There are a number of risk indicators that may help you identify FTF's. If you detect two or more of these risk indicators you should consider whether you need to stop and speak to the individual:

- Males 20-40 years old
- Females 18-30 years old
- Travel History, particularly to or from high risk countries such as Pakistan, Afghanistan, Iraq, Libya, Turkey, Syria and Somalia
- Indirect or broken travel patterns
- Use of fraudulent travel documents
- Appearing to be in disguise
- Separation of groups at border checkpoints
- Avoidance of law enforcement officers, canines or cameras
- Nervous behaviour
- Glancing eye movements
- Avoiding eye contact
- Staring gaze
- Exaggerated actions, yawning, laughing



## 9. RISK PROFILING FOREIGN TERRORIST FIGHTERS

- Pacing
- Sweating
- Clock watching
- Trembling or fidgeting
- Repeated face touching
- Tunnel vision
- Evasive or vague responses to questions
- Non-matching clothes and accessories
- Social media affiliation with extremist groups
- Flags, photos of extremist leaders, and other items suggesting extremist inclinations
- Extremist verbal or written comments

The sharing of intelligence between international intelligence and law enforcement agencies has also identified numerous people who have confirmed or suspected affiliations with terrorist organisations. These Terrorist Watch Lists are an excellent source of intelligence and any person you stop who is on such a list should be subject to search and screening.



You may need to interview individuals who you suspect are members of a terrorist organisation or are an FTF. When you interview a suspect, you need to abide by the rules of interviewing as expressed by your policies, procedures and laws in your country. You should only interview a suspect when you are legally entitled to do so and if you are required to warn the suspects of his rights you should do so. Failing to do this may render your evidence inadmissible.

These initial interviews may take at a point of entry/exit as a result of risk profiling or person/baggage search or during a patrol. You may also speak to an individual that is asking for asylum or is a refugee. After this preliminary interview, if you suspect that a person is a member of a terrorist organisation or is an FTF then you will require a more comprehensive secondary interview.

### **If possible;**

- Have two officers present
- One officer should take notes
- Record the interview by audio/video
- Consider the legal rights and welfare of the suspect
- Consider the need for an interpreter
- If the suspect is a juvenile, consider the need for a social worker or other authorised support person

If any incriminating evidence is located, you should consider moving straight to a more comprehensive secondary interview. If this is not the case, then some preliminary questions that should be asked of suspected terrorists or FTF's include:

- Full name, date of birth, address, email account, social media profiles and telephone number?
- What is your occupation?
- How much do you earn?
- Where did you obtain your passport?
- When did you obtain your passport?
- Where are you travelling?

## 10. INTERVIEWING SUSPECTS

- Who arranged your travel?
- What is the purpose of your travel?
- If the purpose of the trip is education;
- Where will you be studying?
- What course will you be studying?
- What is your education level?
- Where will you reside during your studies?
- How did you pay for your studies?
- What documentation do you possess to verify your claims?
- Who is the contact person from the institution?
- What is their phone number?
- If the purpose of the trip is tourism;
- Where do you intend to go for your holiday?
- What tourist attractions do you wish to visit?
- Where will you be staying?
- How long will you be staying in each location?
- Who is your contact person for your trip?
- How did you book your trip?
- Who paid for your trip?
- Who are you travelling with?
- Where did you obtain your visa?
- How much money do you have?
- Where have you travelled previously?
- Have you/are you seeking asylum?
- Have you/are you seeking refugee status?
- May I inspect your mobile telephone/laptop/electronic device?
- Have you ever participated in an armed conflict?
- Has anyone you know ever participated in an armed conflict?
- Have you ever been the subject of violence or threats of violence because of your beliefs?
- Has anyone you know ever been the subject of violence or threats of violence because of their beliefs?
- How do you feel about (local terrorist group or affiliates)?
- Do you know anyone connected with (local terrorist group or affiliates)?
- Do you know anyone who has advocated, planned, supported or committed terrorist activities?
- Have you ever advocated, planned, supported or committed terrorist activities?

## 10. INTERVIEWING SUSPECTS

- Do you know anyone capable of carrying out terrorist attacks?
- Do you know anyone willing to carry out terrorist attacks?
- Have you heard of anyone recruiting FTF's?
- Have you ever been approached by anyone recruiting FTF's?
- Have you received any training, at camps or otherwise, that could be used in terrorist activities?
- Do you know anyone who has received any training, at camps or otherwise, that could be used in terrorist activities?
- Do you know anyone that is raising funds for terrorist groups or activities?
- Do you know anyone that has contributed funds towards terrorist groups or activities?
- Have you ever raised, or contributed funds towards terrorist groups or activities?
- Do you have any knowledge in, or have you ever been trained in the use of weapons?

Your secondary interview with a suspected terrorist or FTF may be a protracted affair and require asking many of the previously mentioned questions again. Remember this list is not exhaustive. You should also clarify any information you have obtained by examining their telephone, laptop, social media accounts or anything of a contradictory nature.

At the completion of the secondary interview you should contact your NIS or CT units to seek advice or notify them of your intentions. They may wish to release the suspect and place them under surveillance with the objective of collecting further intelligence on their terrorist network.

After questioning you may also decide to deny entry to the person on grounds that you suspect they are travelling to a conflict zone. Should you do this ensure that you share this intelligence with the relevant authorities as they may try and gain access via another border check-point.

## 11. SECURING THE EVIDENCE

You should only search for and seize evidence of terrorist activities or FTF if you are lawfully entitled to do so.

There are many ways that evidence relating to terrorist activities and FTF may come into your possession. It may be as a result of a person search, vehicle or vessel search, searching baggage, a container or searching a residential or business premises. Irrespective of how this evidence comes into your possession you must document the scene and record the actions you take when you seize the digital media device or other supporting evidence.

This evidence may consist of different items that help prove evidence that helps prove this trafficking. This may include:

- Cell phones
- Computers
- Bank statements
- Travel documentation
- Accommodation documentation
- Cash
- Transporter documentation
- Digital media devices



### **Prior to the search you should:**

- Photograph and/or video the search area
- Draw a map of the scene
- If you have other officers to assist you assign each a specific role i.e. search, exhibit officer, officer in charge and photographer



### **During the search you should:**

- Search the area systematically
- Video the search
- Document the location where each item is found
- Bag or secure items seized clearly labelling each with a unique identification number
- Create a record of all items seized
- Complete chain of custody documentation

Exhibits may also contain traces of DNA and fingerprints. You should enquire with your Supervisor whether your agency have the facilities to collect and analyse this type of evidence. It may be crucial evidence in identifying other suspects within the terrorist organisation or those supporting them.



## 12. CHAIN OF CUSTODY

Chain of Custody refers to the chronological documentation and/or paper trail showing the seizure, custody, control, transfer, analysis and disposition of evidence. Because evidence can be used in court to convict someone of a crime, it must be handled in a careful manner to avoid allegations of tampering or misconduct which can potentially compromise a case.

You are responsible for making a record of any evidence that comes into your possession and what you subsequently do with that evidence. If you hand it to another officer, or to an expert, or even back to the suspect you must make a record of this movement on a Chain of Custody form.

There are many examples of Chain of Custody forms available on the internet, but you should first check whether your Department has its own form before using one of these.

A chain of custody form should as a minimum include the following information about the evidence you have seized:

- Date Collected
- Time Collected
- Item Number or Barcode Number
- Case or Event Number
- Who collected the item
- Where the item was collected
- The suspect's name
- A thorough description of the item
- Offence for which the item was collected
- Where the item is stored
- Any person who came into possession of the item, the reason for this, and the date and time that this occurred

Suspects involved in terrorism are engaged in criminal activity that requires the transfer of large sums of money to pay for criminal activities, the movement of personnel and engaging in conflict. When you are investigating a terror related offence or an FTF case always ensure that you consider a parallel financial investigation for money laundering. These types of investigations can help you identify the sources of income for terrorist groups and other actors within their network.

If you do not have the necessary skills to undertake these types of investigations speak with your supervisor or the relevant unit within your department.

If you do not have this unit in your department speak with the relevant intelligence agency

or Financial Investigations Unit. Steps that you can take to collect evidence of money laundering can occur at different times within your investigation. These include:

### **Suspect Profiling:**

- Obtaining court orders or warrants for examination of financial records, including bank records, phone records and tax returns
- Using services of a forensic accountant to examine financial records
- Conducting business and property checks

### **When conducting surveillance:**

- What banks do they use?
- What credit cards do they use?
- What vehicles do they use?
- What properties do they control?



## 13. FINANCIAL INVESTIGATIONS

### **When searching a crime scene or suspect, look for:**

- Mobile telephones
- Bank documents
- Property documents
- Business records
- Financial records
- Computers
- Cash
- Receipt books/invoices
- Passports
- Digital recording devices

### **When interviewing a suspect:**

- What is their income and expenses?
- What properties and assets do they own or lease and how they were funded?
- What businesses or companies do they own?
- Who do they work for?
- What bank accounts do they have in your country or overseas?
- Who is their accountant?

### **Also consider:**

- Conducting forensic examination of digital devices
- Are they using the services of money lenders or Hawala operators?

Terrorist Organisations are not bound by the rule of law and do not recognise state boundaries. They move between jurisdictions and seek to establish new networks where they can avoid detection and/or carry out operations. They also move operatives, equipment and FTF's into and out of conflict zones.

Similarly, law enforcement does not operate in a bubble. The sharing of intelligence is crucial to effectively address terrorist organisations, whether that sharing has a domestic or international focus.

As a frontline law enforcement officer, you may come across individuals who are suspected terrorist or are an FTF. Information in relation to these individuals could be vitally important to your NIS or CT units or those of another country.

Ensure that you adhere to your agency's procedures in relation to intelligence sharing.

**You can share your intelligence in several different ways including:**

- Through a graded intelligence report
- Through an email
- In a phone call
- Via a messaging application
- In person

You may also wish to share intelligence with your neighbouring BLO's through your established intelligence sharing mechanisms.

Terrorist networks can be sophisticated, adaptable and aware of law enforcement methodologies. To defeat these networks will take a network of law enforcement and intelligence agencies working together towards a common goal. Do not restrict yourself to your local intelligence landscape but look at this issue globally.



Regional Office for South East Asia and the Pacific  
United Nations Building, 3rd Floor B Block, Secretariat Building  
Raj Damnern Avenue, Bangkok 10200, Thailand  
Tel. (66 - 2) 288 100 Fax (66 - 2) 281 2129 E-mail: [fo.thailand@unodc.org](mailto:fo.thailand@unodc.org)  
Website: [www.unodc.org/southeastasiaandpacific](http://www.unodc.org/southeastasiaandpacific)