UNODC
United Nations Office on Drugs and Crime

Foreign Terrorist Fighters

Manual for Judicial Training Institutes South-Eastern Europe

Cover images: istockphoto.com/xijian, istockphoto.com/bubaone

UNITED NATIONS OFFICE ON DRUGS AND CRIME
Vienna

Foreign Terrorist Fighters

Manual for Judicial Training Institutes South-Eastern Europe

UNITED NATIONS
Vienna, 2017

Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

Foreword

Every year, acts of terrorism kill, injure and harm thousands of innocent victims of all races, cultures and religious beliefs all over the world.

In the past, victims of crime, including terrorism, have too often been the forgotten parties in the criminal justice system. In recent years, however, there has been greater recognition of the rights and roles that these important actors have within the criminal justice framework.

An integral part of the international community's efforts to counter terrorism is bringing perpetrators of terrorist acts to justice and holding them to account for their actions, in accordance with the rule of law and human rights. This fundamental principle requires that Member States establish and implement effective, rule of law-based national measures for the investigation and prosecution of such crimes, and to protect and support victims of such crimes, within the criminal justice system.

In light of this, the United Nations Office on Drugs and Crime (UNODC) was requested by Member States in General Assembly resolution 68/187 of 18 December 2013, among other measures, to "continue to enhance specialized legal knowledge through the preparation of best practices, in close coordination with Member States, on assistance to and support for victims of terrorism, including the role of victims within the criminal justice framework".

This publication represents the outcome of an expert group meeting convened by UNODC and held on 24 and 25 November 2014. At this meeting, experts from Member States, the United Nations, civil society and relevant bodies met to share experiences and discuss challenges and approaches to providing greater support to victims of terrorism within the criminal justice framework. As a result of these discussions and deliberations, including on available international, multilateral and regional instruments and normative frameworks, the experts elaborated a number of recommended good practices, which are set out in this publication.

These recommendations are aimed at assisting Member States to establish and enhance policies, laws and institutional capacity to provide improved outcomes for victims, while fully respecting the rule of law and rights of accused persons. We hope the publication will contribute to the growing body of jurisprudence in this important subject area.

Yury Fedotov
Executive Director
United Nations Office on Drugs and Crime

Contents

Annexes

Abbreviations

CHIS	Covert Human Intelligence Source
CII	Covert Internet Investigator
CSV	Comma Separated Value
DHCP	Dynamic Host Configuration Control Protocol
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)
ECtHR	European Court of Human Rights
ESI	Electronically Stored Information
EXIF	Exchangeable Image File Format
FIU	Financial Intelligence Unit
FTF	Foreign Terrorist Fighters
FTP	File Transfer Protocol
GIMF	Global Islamic Media Front
GPS	Global Positioning System
HTML	Hypertext Markup Language
IACP	International Association of Chiefs of Police
ICCPR	International Covenant on Civil and Political Rights
IP	Internet Protocol
ISP	Internet Service Provider
MLA	Mutual Legal Assistance
OS	Operating system
OSINT	Open Source Intelligence
P2P	Peer-to-Peer
RAM	Random Access Memory
SEE	South-Eastern Europe
SNA	Social Network Analysis
TCP	Transmission Control Protocol
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network

Introduction

The mission of United Nations Office on Drugs and Crime (UNODC) is to contribute to the achievement of security and justice for all by making the world safer from crime, drugs, and terrorism. In the context of global counter-terrorism, UNODC is mandated to provide assistance to requesting countries in their efforts to address the legal and criminal justice aspects of countering terrorism.

There are several trends that can be observed regarding terrorism in the last few years.[1] First of all, terrorist attacks have increasingly targeted private citizens. While the total number of deaths as a result of terrorist attacks rose by 80 per cent between 2013 and 2014, the deaths of civilians increased by 172 per cent during that same period. Further, Boko Haram and Islamic State of Iraq and the Levant (ISIL/Da'esh) were jointly responsible for 51 per cent of all claimed global fatalities in 2014.[2]

The foreign terrorist fighters (FTF) phenomenon is a growing threat to many countries. The flow of FTF into Iraq and Syria continued in 2014 and 2015 and it is estimated that between 25,000 and 30,000 FTF have arrived to Syria and Iraq since 2011.[3]

Reports identify South-Eastern Europe (SEE) as one of the main sources of FTF, along with Western Europe and the Middle East. Features common to people leaving Western Balkan countries for Syria and Iraq include links to diasporas in the EU, particularly in Austria and Germany; pre-departure criminality; poor education; unemployment; dysfunctional or broken families; and mental health issues. With regard to motives, individuals often attempt to escape something—unhappy marriages, domestic violence, debt, criminal prosecution, alcohol and drug abuse—or seek something, such as a spouse, an adventure, or belonging and purpose in life through religion.[4] The average age of FTF from the Western Balkans in Syria and Iraq is 31 for males and 30 for females. When compared to other European countries, more women (36 per cent among Bosnians and 27 per cent among Kosovars, which is almost double the European average), are joining men travelling to Syria and Iraq. Compared to the European average, women and children (non-combatants) make up far more (up to 55 per cent) of the Western Balkan people going to Syria and Iraq.[5]

Given the cross-border nature of the threat and the similarity of the problem in different States, cooperation among countries in SEE is crucial to ensure that the threat is

[1] This manual does not aim to provide an overview of the most prominent terrorist organizations and networks. Such overview can be found with the very basic information in the US Department of State Report, Chapter 6. Available from: http://www.state.gov/documents/organization/45323.pdf. Another elaborate overview on proscribed terrorist organizations is provided by the UK Home Office at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/538297/20160715-Proscription-website-update.pdf.

[2] Institute for Economics and Peace, *Global Terrorism Index 2015: Measuring and Understanding the Impact of Terrorism* (2015).

[3] For detailed elaboration of the trends see *Global Terrorism Index 2015*, pp. 33-61.

[4] For more detailed overview see ibid. p. 13.

[5] Sajjan Gohel and Vlado Azinovic, "The challenges of foreign terrorist fighters: a regional perspective", policy paper presented at the conference on "Foreign Terrorist Fighters and Irregular Migration Routes: Prevention and Resilience", held in Durrës, Albania, from 13 to 15 September 2016, p. 12.

contained. To that end, UNODC undertook a project in the region, covering Albania, Bosnia and Herzegovina, Kosovo (under United Nations Security Council resolution 1244), the former Yugoslav Republic of Macedonia, Montenegro, and Serbia. The project addresses the complex and interrelated challenges posed by the FTF threat to the criminal justice systems of these States. One of the most important outputs of the project is an FTF training module that will be utilized by judges and/or prosecutors and incorporated into existing training courses delivered by national training institutes.

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 wilfully 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. This legal instrument, together with other relevant international and regional legal instruments, provides the basis for the development of this manual.

The Government of the United States of America generously provided UNODC with funding for the above-mentioned project, which led to the publication of this manual. The project built upon ongoing cooperation with Member States from the region relating to the development of an effective and a sustainable legal regime against FTF, based on the rule of law, due process, and human rights. In the course of the project, the UNODC team collaborated closely with the following institutions: School of Magistrates of Albania (Tirana); Judicial Academy of Serbia (Belgrade); Academy for Judges and Public Prosecutors "Pavel Shatev" (Skopje); Centre for Judicial and Prosecutorial Training of the Federation of Bosnia and Herzegovina (Sarajevo); Centre for Judicial and Prosecutorial Training of the Republika Srpska (Banja Luka, Bosnia and Herzegovina); Judicial Commission of the Brčko District (Brčko District, Bosnia and Herzegovina); Academy of Justice (Pristina); and Judicial Training Centre of Montenegro (Podgorica). The team visited and interviewed judges, prosecutors and managers in the region, and trainers of the aforementioned judicial institutes. The discussions revolved around issues such as the type of terrorism and FTF-related training currently provided, the extent and the nature of the FTF problem in the region, challenges of investigations, prosecutions and adjudication of FTF cases.

These discussions revealed four specific areas in which additional expertise is needed. They are:

- The extent, structure and dynamics of the FTF phenomenon;
- The elements of the FTF-related offences;
- Investigation of the FTF offences, with special regard to online and financial investigations;
- Human rights implications of the investigation and adjudication of FTF-related cases.

This manual will address the first three issues. The human rights aspect has already been covered in the Counter-Terrorism Legal Training Curriculum Module 4 on *Human Rights and Criminal Justice Responses to Terrorism* of the UNODC.[6]

[6]See https://www.unodc.org/unodc/en/terrorism/technical-assistance-tools.html.

1. The foreign terrorist fighter phenomenon

1.1. Scope of the term "foreign terrorist fighter"

Despite the fact that use of the term "foreign terrorist fighter" has emerged recently, foreign fighters should not be regarded as a new phenomenon. FTF participated in the Spanish civil war, the war in Afghanistan following the 1989 Soviet invasion, the war in Bosnia and Herzegovina in the 1990s, and the political conflict in Chechnya and Dagestan in the 1990s.[7] 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".[8]

The term "foreign terrorist fighters" 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".[9]

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).[10] The use of mercenaries is covered by both international and regional conventions, and domestic laws, and will not be addressed in this document.[11]

---

[7] Geneva Academy of International Humanitarian Law and Human Rights, *Academy Briefing No. 7—Foreign Fighters under International Law* (Geneva, 2014), p. 3.

[8] Ibid., p. 6.

[9] Security Council resolution 2178 (2014), preamble para. 9. The term "foreign terrorist fighter" was first mentioned in the Security Council resolution 2170 (2014). With this resolution the Council condemned "gross, systematic and widespread abuse" of human rights by ISIL (Da'esh) and Al-Nusra Front. In an annex to the text of the resolution, the Council also named the individuals subject to the travel restrictions, asset freezes and other measures targeted at Al-Qaida affiliates. This resolution, however, did not define "foreign terrorist fighter".

[10] United Nations, Security Council, Report of the Analytical Support and Sanctions Monitoring Team on foreign terrorist fighters (S/2015/358), para. 29.

[11] International instruments include the International Convention against the Recruitment, Use, Financing and Training of Mercenaries (1989), Additional Protocol I and II to Article 47 of the Geneva Convention (1949), and regionally, the Organisation of African Unity (OAU) Convention for the Elimination of Mercenaries in Africa (1972). Examples of domestic laws regulating the activities of mercenaries include South Africa's Prohibition of Mercenary Activities and Regulation of Certain Activities in Country of Armed Conflict Act (2006), New Zealand's Mercenary Activities (Prohibition) Act (2004), and France's Law No 2003-340 of 14 April 2003 relating to the repression of mercenary activity (2003).

1.2. The evolution of the phenomenon

The FTF phenomenon developed in three waves. The first wave of FTF joined Al-Qaida in Afghanistan and consisted of mostly Middle Eastern Arabs fighting the Soviets in the 1980s. They tended to be well educated and from solidly middle-class backgrounds. The second wave consisted mostly of elite expatriates from the Middle East who went to the West to attend universities. The separation from family, friends, and culture led many to feel marginalized and in some cases led them to radicalization. Many of them then travelled to Al-Qaida's training camps in Afghanistan in the 1990s. The terrorism phenomenon from the 1970s to the 1990s was marked by individuals who had been trained in terrorist camps, or answered to individual leaders. The new generation of terrorists tend to be self-recruited, without leadership, and globally connected through the Internet. They are on average younger and are also driven by thrills and a sense of significance and belonging in their lives. Thus the third wave of FTF consisted mostly of individuals who formed fluid, informal networks that were self-financed and self-trained. They had no physical headquarters or sanctuary. The virtual environment of the Internet offered them a semblance of unity and purpose. Theirs was a scattered, decentralized social structure—a leaderless jihad. It has been argued that the developments in Syria and the rise of ISIL (Da'esh) have led to a fourth wave, which resembles its immediate predecessor by the local dynamics of their respective networks.[12] These networks too are formed among friends and family who have known each other for years. However, the rise of ISIL (Da'esh) provides the opportunity to link up with one another on the battlefield. As a result, FTF can acquire technical expertise and transfer skills.

Unsurprisingly, FTF are perceived to be a major terrorist threat. The fear they create ranges from the possibility that they will get involved in terrorist acts outside of their home country, to the threat that, once they return to their home countries, they will utilize their knowledge and experience of handling weapons and explosives in order to plan and carry out terrorist acts, set up new terrorist cells, recruit new members, or provide funds or training for future terrorist acts.

1.3. What we know about foreign terrorist fighters—the typology

The motivational factors for individuals to join a terrorist group overseas are not unique. Some FTF belong to pre-existing kinship gangs for whom joining a terrorist group in Syria or Iraq is a shift to another form of deviant behaviour, transforming them from ordinary criminals into individuals with what they see as a political cause. Others are individuals without any criminal background who are unknown to law enforcement agencies. These tend to be relatively young people who may suffer from feelings of exclusion and an absence of belonging to their local communities or national societies at large. Notably, "vulnerability, frustration, perceptions of inequity, and a feeling that

[12] Rik Coolsaet, "Facing the Fourth Foreign Fighters Wave—What Drives Europeans to Syria, and to Islamic State? Insights from the Belgian State", *Edgmont Paper 81* (March 2016), pp. 18-27.

by joining the fight in Syria they have nothing to lose and everything to gain, are common traits among both groups".[13]

Referring to the potential recruits as seekers, some literature refers to four primary types of FTF: (1) the Revenge Seeker (diffusely 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); and (4) the Thrill Seeker (attracted to the group because of the prospects for excitement, adventure, and glory).[14]

[13] Ibid., p 3.

[14] John M. Venhaus, "Why Youth Join al-Qaeda", United States Institute for Peace, Special Report 236 (Washington, May 2010), pp. 8-11.

2. Foreign terrorist fighters—the international legal framework

2.1. The international legal framework

The terrorist attacks committed in the United States of America on 11 September 2001 led to the adoption of a number of international and regional legal instruments requiring Member States of various international and regional organizations to take firm and immediate actions with regard to preventing terrorism. Whereas the list of those legal instruments is extensive,[15] the most relevant ones in terms of the investigation and adjudication of FTF-related criminal offences in the European context are the following:

- United Nations Security Council (UNSC) resolution 2178 (2014);[16]
- Council of Europe Convention on the Prevention of Terrorism (2005) CETS 196;
- Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (2015) CETS 217 (Additional Protocol).

2.1.1. United Nations Security Council resolution 2178 (2014)

Security Council resolution 2178 of 24 September 2014, operative paragraph 6, recalls its decision in resolution 1373 (2001), requiring all Member States to:

> ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice, and *decides* that all States shall ensure that their domestic laws and regulations establish serious criminal offences sufficient to provide the ability to prosecute and to penalize in a manner duly reflecting the seriousness of the offence:
>
> *(a)* Nationals who travel or attempt to travel to a State other than their States of residence or nationality, and other individuals who travel or attempt to travel from their territories 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;

[15] See the following United Nations website for a current list of the international legal instruments to prevent terrorist acts: www.un.org/en/counterterrorism/legal-instruments.shtml.

[16] Security Council resolution 2178 (2014) is another instrument addressing the FTF issue. However, it will not be addressed in this document as it does not relate to the investigation and adjudication of FTF.

(b) The wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to finance the travel of 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; and,

(c) The wilful organization, or other facilitation, including acts of recruitment, by their nationals or in their territories, of the travel of 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.

2.1.2. Council of Europe Convention on the Prevention of Terrorism (2005) CETS 196

Following the September 2001 attacks in the United States, the Council of Europe formed a working group to review its counter-terrorism legislation and began work on the Convention on the Prevention of Terrorism in 2003. After a number of meetings, the Council of Europe Committee of Experts on Terrorism drafted the Council of Europe Convention on the Prevention of Terrorism, which was opened for signature on 16 May 2005 in Warsaw.[17] This Convention does not define new terrorist offences in addition to those included in the existing conventions against terrorism. However, it creates three new offences which may lead to the terrorist offences as defined in those conventions. These new offences are: public provocation to commit a terrorist offence (article 5), recruitment for terrorism (article 6) and training for terrorism (article 7). They are coupled with a provision on accessory (ancillary) offences (article 9) providing for the criminalization of complicity (such as aiding and abetting) in the commission of all of the three aforementioned offences and, in addition, of attempts to commit an offence under articles 6 and 7 (recruitment and training).[18]

One of the characteristics of the new crimes introduced by the Convention is that they do not require that a terrorist offence within the meaning of article 1 (i.e., any of the offences within the scope of and as defined in one of the international treaties against terrorism listed in the appendix) is actually committed. This is explicitly stated in Convention article 8, based on an equivalent provision in the International Convention for the Suppression of the Financing of Terrorism. Consequently, the place where such an offence is committed is also irrelevant for the purposes of establishing the commission of any of the offences set forth in articles 5 to 7 and 9. In addition, these offences must be committed unlawfully and intentionally, as is explicitly stated in each article, as found below.[19]

[17] See http://www.coe.int/en/web/counter-terrorism.

[18] Council of Europe, Explanatory Report to the Council of Europe Convention on the Prevention of Terrorism, *Council of Europe Treaty Series*, No. 196, paras. 32 and 33.

[19] Ibid., paras. 34 and 35.

Article 5—Public provocation to commit a terrorist offence:

> For the purposes of this Convention, "public provocation to commit a terrorist offence" means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed.
>
> Each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

Article 6—Recruitment for terrorism:

> For the purposes of this Convention, "recruitment for terrorism" means to solicit another person to commit or participate in the commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group.
>
> Each Party shall adopt such measures as may be necessary to establish recruitment for terrorism, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

Article 7—Training for terrorism:

> For the purposes of this Convention, "training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence, knowing that the skills provided are intended to be used for this purpose.
>
> Each Party shall adopt such measures as may be necessary to establish training for terrorism, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

2.1.3 Additional Protocol to the Council of Europe Convention on Prevention of Terrorism (2015) CETS 217

Following the unanimous adoption by the Security Council of resolution 2178 (2014), in which the Security Council called on Member States to take a series of measures aimed at preventing and curbing the flow of FTF to conflict zones, the Council of Europe Committee of Experts on Terrorism examined the issue of radicalization and FTF. The result of these discussions was a proposal to the Committee of Ministers to draft terms of reference for a committee to be established for the purpose of drafting an Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (2015) CETS 196. The main objective of the Additional Protocol was to supplement the aforesaid Convention with a series of provisions aimed at implementing the criminal law aspects of Security Council resolution 2178. As the result, in

January 2015, the Committee of Ministers adopted the terms of reference for the Committee on Foreign Terrorist Fighters and Related Issues. This Committee, under the authority of the Committee of Experts on Terrorism, was tasked with preparing an Additional Protocol which supplements the Council of Europe Convention on the Prevention of Terrorism by adding provisions on the criminalization of acts related to terrorist offences and a provision on the exchange of information. The offences set forth in the Protocol, like those in the Convention, are mainly of a preparatory nature in relation to terrorist acts. These offences are: Participating in an association or group for the purpose of terrorism (article 2); Receiving training for terrorism (article 3); Travelling abroad for the purpose of terrorism (article 4); Funding travelling abroad for the purpose of terrorism (article 5); and Organising or otherwise facilitating travelling abroad for the purpose of terrorism (article 6), as found below.[20]

Article 2—Participating in an association or group for the purpose of terrorism:

1. For the purpose of this Protocol, "participating in an association or group for the purpose of terrorism" means to participate in the activities of an association or group for the purpose of committing or contributing to the commission of one or more terrorist offences by the association or the group.

2. Each Party shall adopt such measures as may be necessary to establish "participating in an association or group for the purpose of terrorism", as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

Article 3—Receiving training for terrorism:

1. For the purpose of this Protocol, "receiving training for terrorism" means to receive instruction, including obtaining knowledge or practical skills, from another person in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence.

2. Each Party shall adopt such measures as may be necessary to establish "receiving training for terrorism", as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

Article 4—Travelling abroad for the purpose of terrorism:

1. For the purpose of this Protocol, "travelling abroad for the purpose of terrorism" means travelling to a State, which is not that of the traveller's nationality or residence, for the purpose of the commission of, contribution to or participation in a terrorist offence, or the providing or receiving of training for terrorism.

[20] For a more detailed account of the background to the Protocol see Council of Europe, Explanatory Report to the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, *Council of Europe Treaty Series*, No. 217, paras. 2-12.

2. Each Party shall adopt such measures as may be necessary to establish "travelling abroad for the purpose of terrorism", as defined in paragraph 1, from its territory or by its nationals, when committed unlawfully and intentionally, as a criminal offence under its domestic law. In doing so, each Party may establish conditions required by and in line with its constitutional principles.

3. Each Party shall also adopt such measures as may be necessary to establish as a criminal offence under, and in accordance with, its domestic law the attempt to commit an offence as set forth in this article.

Article 5—Funding travelling abroad for the purpose of terrorism:

1. For the purpose of this Protocol, "funding travelling abroad for the purpose of terrorism" means providing or collecting, by any means, directly or indirectly, funds fully or partially enabling any person to travel abroad for the purpose of terrorism, as defined in article 4, paragraph 1, of this Protocol, knowing that the funds are fully or partially intended to be used for this purpose.

2. Each Party shall adopt such measures as may be necessary to establish the "funding of travelling abroad for the purpose of terrorism", as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

Article 6—Organising or otherwise facilitating travelling abroad for the purpose of terrorism:

1. For the purpose of this Protocol, "organising or otherwise facilitating travelling abroad for the purpose of terrorism" means any act of organisation or facilitation that assists any person in travelling abroad for the purpose of terrorism, as defined in article 4, paragraph 1, of this Protocol, knowing that the assistance thus rendered is for the purpose of terrorism.

2. Each Party shall adopt such measures as may be necessary to establish "organising or otherwise facilitating travelling abroad for the purpose of terrorism", as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

3. Criminal offences related to foreign terrorist fighters

Terrorism has been on the agenda of the international community since the 1930s. Beginning in 1964, a total of 19 universal legal instruments have been adopted for the purpose of addressing terrorism and terrorists. These conventions deal with terrorism-related issues such as civil aviation, protection of international staff, taking hostages, nuclear material, maritime navigation, explosive materials, terrorist bombings, nuclear terrorism, and financing of terrorism. All these instruments call on States Parties to take firm steps in the fight against terrorism and to undertake a number of measures to enhance national, regional and international efforts to counter terrorism.[21]

The primarily legislative and legal efforts required from States Parties to these legal instruments were given a comprehensive policy structure with the adoption of the reviewed United Nations Global Counter-Terrorism Strategy on 8 September 2006.[22] In the fourth pillar of the strategy, States Parties commit themselves

> To make every effort to develop and maintain an effective and rule of law-based national criminal justice system that can ensure, in accordance with their obligations under international law, that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in support of terrorist acts is brought to justice, on the basis of the principle to extradite or prosecute, with due respect for human rights and fundamental freedoms, and that such terrorist acts are established as serious criminal offences in domestic laws and regulations.[23]

[21] A list of these instruments can be found at the end of this document.

[22] The General Assembly reviews the Strategy every two years. The Fifth Review of the United Nations Global Counter-Terrorism Strategy took place on 1 July 2016. In resolution 70/291, the General Assembly, inter alia, "urges Member States to provide full coordination and afford one another the greatest measure of assistance, in accordance with their obligations under international law, in criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, especially with those States where, or against whose citizens, terrorist acts are committed, including obtaining evidence for the proceedings involving terrorist organizations, terrorist entities or foreign terrorist fighters, and recalls that all States must cooperate fully in the fight against terrorism on the basis of mutual legal assistance and the principle of extradite or prosecute, welcoming their efforts to elaborate on the existing extradition and mutual legal assistance mechanisms;" (para. 32); and "calls upon all Member States, in accordance with their obligations under international law, to cooperate in efforts to address the threat posed by foreign terrorist fighters, including by preventing the radicalization to terrorism and recruitment of foreign terrorist fighters, including children, preventing foreign terrorist fighters from crossing their borders, disrupting and preventing financial support to foreign terrorist fighters, and developing and implementing prosecution, rehabilitation and reintegration strategies for returning foreign terrorist fighters, and in this regard encourages all Member States to develop effective strategies to deal with returnees, including through repatriation, in accordance with relevant international obligations and national law" (para. 44).

[23] Global Counter-Terrorism Strategy, Pillar IV, "Measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism", point 5, at www.un.org/counterterrorism/ctitf/en/un-global-counter-terrorism-strategy.

The most important legal instruments that require States to criminalize the actions of FTF are Security Council resolutions 1373 (2001) and 2178 (2014). In the former, Member States are called to ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice. In the latter, the United Nations officially recognized that addressing the threat posed by FTF requires comprehensively addressing underlying factors, including by preventing radicalization to terrorism, stemming recruitment, inhibiting FTF travel, disrupting financial support to FTF, countering violent extremism, which can be conducive to terrorism, and countering incitement to terrorist acts motivated by extremism or intolerance.[24]

In addition to these United Nations instruments, there are a number of conventions and protocols adopted within the Council of Europe framework which are relevant to SEE, and which have been instrumental in developing criminal offences related to FTF. The most important of these are the Council of Europe Convention on the Prevention of Terrorism (2005) CETS 196 and its Additional Protocol, as introduced in section 2 above. These instruments contain specific definitions of FTF-related criminal offences called for in Security Council resolutions 1373 (2001) and 2178 (2014), and provide interpretative notes for the defined elements of the offences. The analysis below, which aims to provide a more comprehensive understanding of the elements of FTF-related criminal offences, is thus based on the relevant provisions of these Council of Europe instruments.

3.1. Public provocation to commit a terrorist offence—article 5 (CETS 196)[25]

Freedom of expression, enshrined in article 19 of the International Covenant on Civil and Political Rights (ICCPR), is a fundamental human right that is essential for the promotion and protection of human rights.[26] Likewise, in the European context, freedom of expression (as expressed in article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)) has been found to be one of the essential foundations of a democratic society.[27] It applies not only to ideas and information that are favourably received or regarded as inoffensive but also to those that "offend, shock or disturb".[28]

Certain rights, such as the prohibition of torture and inhuman and degrading treatment or punishment as found in article 2(2) of the Convention against Torture, and Other Cruel, Inhuman or Degrading Treatment or Punishment, are absolute and may not be

[24] See the preamble of Security Council resolution 2178.

[25] For a general overview of the right to freedom of expression and terrorism-related offences, see chapter 2 of UNODC Counter-Terrorism Legal Training Curriculum Module 4 on Human Rights and Criminal Justice Responses to Terrorism.

[26] Human Rights Committee, General Comment No. 34 (CCPR/C/GC34), 12 September 2011, p. 1.

[27] ECtHR, *Lingens* v *Austria*, Application No. 9815/82, Judgment of 8 July 1986.

[28] Council of Europe, Explanatory Report 196, (see footnote 18), para. 89.

derogated from in any circumstances. Conversely, restrictions[29] and even derogation[30] on freedom of expression may be allowed under specific circumstances.[31] For instance, incitement (as a publicly expressed statement) to racial hatred falls outside of the protection given by the right to freedom of expression.[32] Likewise, messages that might constitute a public provocation (indirect incitement) to violent terrorist offences may be outside of the scope of protection afforded by freedom of expression.[33]

What seems to remain a difficult issue is determining where the boundary lies between public provocation to commit terrorist offences and the expression of views that "offend, shock or disturb", but do not constitute public provocation. The drafters of this offence tried to respond to this question by providing the definition.[34] To that end, public provocation to commit a terrorist offence is defined as "the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed".[35]

When drafting this provision, the Council of Europe Committee of Experts on Terrorism considered the opinions of the Parliamentary Assembly and of the Commissioner for Human Rights of the Council of Europe, the latter of which suggested that such a provision could cover "the dissemination of messages praising the perpetrator of an attack, the denigration of victims, calls for funding for terrorist organisations or other similar behaviour" which could constitute indirect provocation to terrorist violence.[36] The decision was made to use a generic formula, as opposed to a more casuistic one, and requires States Parties to criminalize the distributing or otherwise making available of a message to the public advocating terrorist offences. Whether this is done directly (directed towards a particular person or a particular group of persons) or indirectly (directed to the general public) is irrelevant for the application of this provision.[37]

Direct provocation does not raise any particular problems insofar as it is already a criminal offence, in one form or another (incitement/instigation as a form of complicity), in most legal systems. The aim of making indirect provocation (or public provocation) a criminal offence is to remedy the existing lacunae in international law. Article 5

[29] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, art. 10(2).

[30] European Convention on Human Rights, art.15.

[31] United Nations, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, *Treaty Series*, vol. 999, p. 171. See also Council of Europe, Explanatory Report 196, (see footnote 18) para. 90.

[32] United Nations, *International Convention on the Elimination of All Forms of Racial Discrimination*, 21 December 1965, United Nations *Treaty Series*, vol. 660, p. 195, art. 9. See also Council of Europe, Explanatory Report 196, (see footnote 18) para. 91.

[33] ECtHR, *Hogefeld v Germany,* Application No. 35402/97, Judgement of 20 January 2000.

[34] This definition relies heavily on the Additional Protocol to the Cybercrime Convention concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. Council of Europe, Additional Protocol to the Convention on Cybercrime, *European Treaty Series No. 189*, art. 3.

[35] Council of Europe Convention on the Prevention of Terrorism (2005) CETS 196, art. 5.

[36] Council of Europe, Explanatory Report 196, (see footnote 18) para. 95. For further information on the Council of Europe Committee of Experts on Terrorism see www.coe.int/en/web/counter-terrorism, and Council of Europe, Opinion of the Commissioner for Human Rights, Alvaro Gil-Robles, on the draft Convention on the Prevention on Terrorism, 2 February 2005.

[37] Council of Europe, Explanatory Report 196, (see footnote 18) para. 96.

affords States Parties a certain amount of discretion with respect to the definition of the offence and its implementation. For instance, presenting a terrorist offence as necessary and justified may constitute the offence of public provocation. An example of this could be the release of a video featuring a person talking about the heresy of the Western world when it comes to celebrating New Year's eve, and calling believers to, in the name of God, actively take part in jihad and do everything they can to "teach the Westerners a lesson". In the video, short clips of explosions in cafes and attacks on squares are shown.

There are two elements to the offence of public provocation contained in article 5; first, there has to be a specific intent to incite the commission of a terrorist offence, which is supplemented with the requirements that the provocation be committed unlawfully and intentionally (article 5 (2)). Second, the result of such an act must be to cause a danger that such an offence might be committed. When considering whether such danger is caused, the nature of the author and of the recipient of the message, as well as the context in which the offence is committed shall be taken into account.[38] The significance and the credible nature of the danger should be considered when applying this provision in accordance with the requirements of domestic law.[39]

With regard to provocation and the offences set forth in the International Convention for the Suppression of the Financing of Terrorism, the latter may play an important role in the chain of events that leads to the commission of the terrorist offences.[40] While the prospect of violent crime is fairly remote from the act of provocation, it is this prospect that ultimately justifies the criminalization of public provocation to commit the offence of terrorism. In other words, the purpose of criminalizing public provocation to commit a terrorist offence is to make the provocation punishable even if it is not acted upon by anyone, as long as it created a real risk that the terrorist offence may be committed.

The term "distribution" in article 5 refers to the active dissemination of a message advocating terrorism, while the expression "making available" refers to providing that message in a way that is easily accessible to the public, for instance, by placing it on the Internet or by creating or compiling hyperlinks in order to facilitate access to it.[41]

The term "to the public" in article 5 makes it clear that private communications fall outside the scope of this provision. In order to make a message available to the public, a variety of means and techniques may be used. For instance, printed publications or speeches delivered at places accessible to others, the use of mass media or electronic facilities, in particular the Internet, which provides for the dissemination of messages by email or for possibilities such as the exchange of materials in chat rooms, newsgroups or discussion forums.[42]

[38] Ibid., paras. 97-100.

[39] Ibid.

[40] Ibid., para. 101.

[41] Ibid., para. 102.

[42] Ibid., paras. 103-105.

In the end, and for the purpose of understanding the offence, it has to be borne in mind that there is no universal comprehensive legal definition of "terrorism" and "terrorist offences". In contrast, the Council of Europe Convention on the Prevention of Terrorism (CETS 196) defines "terrorist offence" as any of the offences within the scope of and defined in the treaties listed in the appendix of this Convention and can therefore be used by SEE jurisdictions as a guidance.[43] Adjudication of the cases in the SEE jurisdictions will nevertheless depend on the definition of "terrorism" and "terrorist offence" in those jurisdictions.

3.2. Recruitment for terrorism—article 6 (CETS 196)

Article 6 intends to criminalize the recruitment of potential future terrorists. Recruitment is understood here as solicitation of other persons to carry out terrorist offences whether individually or collectively, whether directly committing, participating in or contributing to the commission of such offences.[44] The Convention on the Prevention on Terrorism does not define the terms "association or group", which enables Member States to choose to interpret the term to mean "proscribed" organizations or groups in accordance with their national law and/or in accordance with the general principles of international law.[45]

The act of solicitation can take place by various means, for instance, via the Internet or directly in person. For the completion of the act, it is not necessary that the addressee actually participate in the commission of a terrorist offence or that he or she join a group for that purpose.[46] However, for the crime to be completed, it is necessary that the recruiters be successful in approaching and persuading a person to either commit or participate in the commission of a terrorist offence.[47] One example could be a person or an organization releasing a recruitment video (like the one released by ISIL (Da'esh) entitled "Honour is in Jihad", which was aimed at encouraging potential recruits to come to Iraq and Syria. The video featured fighters from Bosnia, Albania, and Kosovo). As a result, a number of individuals from a third country joined ISIL (Da'esh). Another example could be a person or an organization increasing the number of its members/affiliates by offering money to people from impoverished Balkan countries. As a result,

[43]The treaties listed in the appendix are: 1 Convention for the Suppression of Unlawful Seizure of Aircraft, signed at The Hague on 16 December 1970; 2 Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, concluded at Montreal on 23 September 1971; 3 Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, adopted in New York on 14 December 1973; 4 International Convention Against the Taking of Hostages, adopted in New York on 17 December 1979; 5 Convention on the Physical Protection of Nuclear Material, adopted in Vienna on 3 March 1980; 6 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, done at Montreal on 24 February 1988; 7 Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, done at Rome on 10 March 1988; 8 Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, done at Rome on 10 March 1988; 9 International Convention for the Suppression of Terrorist Bombings, adopted in New York on 15 December 1997; 10 International Convention for the Suppression of the Financing of Terrorism, adopted in New York on 9 December 1999; 11 International Convention for the Suppression of Acts of Nuclear Terrorism, adopted in New York on 13 April 2005.

[44]Council of Europe, Explanatory Report 196, (see footnote 18) para. 106.

[45]Ibid., para. 107.

[46]Ibid., paras. 108-110.

[47]Ibid.

a number of persons may join that person or that organization in the preparation and execution of terrorist offences.

If the solicitation is commenced but not completed (for example, the person is not persuaded to be recruited, or the recruiter is apprehended by law enforcement authorities before successfully recruiting the person), the conduct is still punishable as an attempt to recruit.[48] The offence will still be committed even if the solicited person has actually neither participated in the commission of a terrorist offence nor joined an association or group for that purpose.[49] What is important is that the recruiter intends that the persons they recruit commit or contribute to the commission of a terrorist offence or join an association or group for that purpose.

3.3. Training for terrorism—article 7 (CETS 196)

Article 7 criminalizes the provision of training for the purpose of carrying out or contributing to the commission of a terrorist offence.[50] Training for terrorism is defined as providing instruction in methods or techniques that are suitable for use for terrorist purposes, including in the making or use of explosives, firearms and noxious or hazardous substances.[51] Examples of training may also involve various types of paramilitary training such as small unit tactics and techniques of guerrilla warfare. It may also include covert communications, document falsification, methods of surveillance, martial arts, employment of disguise, and procedures for jamming communications. Occasionally, some terrorists may also be trained in evaluating security systems, assessing the vulnerability of various targets, defensive driving and evasion methods to reduce the likelihood of their victim's escape. What is important to know is that regardless of the type of training, for such conduct to be criminally liable, it is necessary that the person providing the training know that the skills provided are intended to be used for the commission of or the contribution to commit a terrorist offence.[52]

The offence itself does not contain a definition of weapons, firearms and explosives, or noxious or hazardous substances. The Council of Europe, in its Explanatory Report to the Convention on the Prevention of Terrorism, suggests that the term "explosive" could be defined according to the article 1(3)*(a)* of the International Convention for the Suppression of Terrorist Bombings, as "an explosive or incendiary weapon or device that is designed, or has the capability, to cause death, serious bodily injury or substantial material damage."[53]

[48] Council of Europe Convention on the Prevention of Terrorism (2005) CETS 196, art. 9(2).

[49] Council of Europe, Explanatory Report 196, (see footnote 18) paras. 111-113.

[50] Ibid., paras. 114 and 115.

[51] This offence does not criminalize the fact of receiving such training. For the elements of that offence, see "Receiving training for terrorism purposes", below at section 3.5.

[52] Council of Europe, Explanatory Report 196, (see footnote 18) para. 122.

[53] Council of Europe, Explanatory Report 196, (see footnote 18) para. 118.

Equally, the Explanatory Report suggests defining "firearm" within the meaning of appendix I to the European Convention on the Control of the Acquisition and Possession of Firearms by Individuals (ETS 101).[54] Further, the term "other weapons" can be understood in the sense of "lethal weapon" as defined by the International Convention for the Suppression of Terrorist Bombings, article 1(3)*(b)*, which characterizes it as "a weapon or device that is designed, or has the capability, to cause death, serious bodily injury or substantial material damage through the release, dissemination or impact of toxic chemicals, biological agents or toxins or similar substances or radiation or radioactive material".[55]

The Explanatory Report further suggests defining "noxious or hazardous substances" in line with its meaning in article 1(5) of the International Maritime Organization (IMO) Protocol on Preparedness, Response and Co-operation to Pollution Incidents by Hazardous and Noxious Substances (2000), which defines them by reference to lists of substances included in various IMO conventions and codes. These include "oils; other liquid substances defined as noxious or dangerous; liquefied gases; liquid substances with a flashpoint not exceeding 60°C; dangerous, hazardous and harmful materials and substances carried in packaged form; and solid bulk materials defined as possessing chemical hazards."[56]

3.4. Participating in an association or group for the purpose of terrorism—article 2 (CETS 217)

When the Additional Protocol was drafted, the Council of Europe Committee on Foreign Terrorist Fighters and Related Issues was tasked with examining the criminalization of "being recruited, or attempting to be recruited, for terrorism".[57] This phrase is contained in article 6 of the Convention, which criminalizes the "active recruitment" (see section 3.2 above) of others, which was intended to accompany a provision on "passive recruitment" in the Protocol. It became apparent through the process of deliberation that requiring criminalization of "passive" behaviour ("being recruited for terrorism") would create legal challenges in a number of jurisdictions.[58] Additionally, "finding an appropriate legal definition of 'being recruited for terrorism' which captured sufficiently 'active' behaviour also posed certain problems. Ultimately, the Additional Protocol to the Convention criminalises 'participating in an association or group for the purpose of terrorism'".[59]

Participating in an association or group for the purpose of terrorism is defined in article 2 of the Additional Protocol as "to participate in the activities of an association or group for the purpose of committing or contributing to the commission of one or more

[54] Ibid., para. 119.

[55] Ibid., para. 120.

[56] Ibid., para. 121.

[57] Council of Europe, Explanatory Report 217, (see footnote 20) para. 31.

[58] Ibid.

[59] Ibid.

terrorist offences by the association or group". Thus, the criminalization of passive membership of a terrorist association or a group, or the membership of an inactive terrorist association or group, is not required under this offence.[60] In contrast to active membership, which means participation in a wide range of the group's activities, passive membership presupposes some association with the group has been established (i.e. a person is registered as a member of a particular terrorist group or organization), yet no involvement in the group's/organization's activities has been found.

For example, active membership would exist if a person is acting as an interpreter in training, knowing the purpose of the training and intentionally contributing to the success of the training. Another example would be the one of a woman in charge of cooking and providing food for a group of persons trained for committing terrorist offences knowing the purpose of their training and intentionally contributing to the success of the training. An example of passive membership would be a woman who purposely marries an ISIL (Da'esh) combatant, without any intention to directly contribute to the activities of terrorist group.

Participation in the activities of an association or group for the purpose of terrorism "may be the result of contacts established via the Internet, including social media, or through other IT-based platforms".[61] Interestingly, the drafters did not consider it necessary to criminalize the attempt or the aiding or abetting of this offence, however States Parties may do so if it is appropriate in their domestic legal systems.[62]

The Explanatory Report to the Additional Protocol notes that the Protocol does precisely define the nature of the association or group, as the criminalization "depends on the commission of terrorist offences by the group regardless of its officially proclaimed activities".[63] Notably, there is no internationally binding definition of a "terrorist association or group". To that end, States Parties may define such associations or groups to mean those that are prohibited in their domestic laws.[64]

3.5. Receiving training for terrorism purposes—article 3 (CETS 217)

The criminalization of receiving training for terrorism enables States Parties to investigate and prosecute training activities which may lead to the commission of terrorist offences.

Article 3 criminalizes the receiving of training which would enable the recipient to carry out or contribute to the commission of terrorist offences. The wording and terminology used for the definition of this offence thus closely reflects that used in the offence of training for terrorism, as explained above (see section 2.1.3 above for this definition).[65]

[60] Ibid., para. 33.
[61] Ibid., para. 35.
[62] Ibid., paras. 35 and 36.
[63] Ibid., para. 37.
[64] Ibid.
[65] Ibid., para. 38.

This applies in particular to the terms "explosives, firearms or other weapons or noxious or hazardous substances".

The Explanatory Report to the Additional Protocol notes that receiving training for terrorism may take place in person through, for example, attending a training camp run by a terrorist group, or through electronic media, including through the Internet.[66] Merely visiting websites containing information or receiving communications, which could be used for training for terrorism purposes, is not an offence under this article. The perpetrator must take an active part in the training in order to come under the purview of this article by, for example, participating in interactive training via the Internet. The article 3 definition does not cover "self-study", which States Parties may criminalize domestically.[67]

It is important to note that terrorism training must be received with the purpose of carrying out or contributing to the commission of a terrorist offence. The individual must act both "unlawfully" and "intentionally".[68] Thus, participation in activities that would otherwise be lawful, such as taking a chemistry course at university, may also be captured in article 3 as unlawfully committing a criminal offence of receiving training for terrorism if it can be demonstrated that the person receiving the training has the criminal intent to use it to commit a terrorist offence.[69]

3.6. Travelling abroad for the purpose of terrorism—article 4 (CETS 217)

The definition of the offence of travelling abroad for the purpose of terrorism in the Additional Protocol is intended to provide the legal framework for facilitating the implementation of Member States' obligations contained in operative paragraph 6(a) of Security Council resolution 2178 at the European level.[70] The article reflects the drafters' view that the seriousness of the FTF threat demanded a strong response which is fully compatible with human rights and the rule of law.[71]

The aim of article 4 of the Additional Protocol is to require States Parties to criminalize the act of travelling to a State other than that of the nationality or residence of the traveller from the territory of the Party in question, or by its nationals, if the purpose of that travel is to commit, contribute to or participate in terrorist offences, or to provide or receive training for terrorism as defined in article 7 of the Convention and article 3 of th[e] Protocol. The travel to the State of destination may be direct or by transiting other States on route.[72]

[66] Ibid., para. 40.
[67] Ibid.
[68] Ibid., para. 41.
[69] Ibid.
[70] Ibid., para. 43.
[71] Ibid., para. 46.
[72] Ibid., para. 44.

The drafters took note of the right to freedom of movement enshrined in article 12 of the ICCPR and article 2 of Protocol No. 4 to the ECHR, both of which allow for restrictions of this right in certain circumstances, such as for the protection of national security, and in the case of Protocol No. 4, for the prevention of crime.[73]

The Explanatory Report to the Additional Protocol notes that the Protocol does not require States Parties to criminalize all travels to certain destinations, or introduce administrative measures, such as the withdrawal of passports. Rather, this provision requires criminalization of the act of travelling under specific conditions which must be proved in accordance with the domestic law of a State Party. The evidence submitted must also be "submitted to an independent court for scrutiny in accordance with the specific, applicable criminal procedures of the Party and the general principle of the rule of law".[74]

There are two elements to the offence of travelling abroad for the purpose of terrorism that must be proven in accordance with domestic law under this article. First, the person must travel for the purpose of committing or participating in terrorist offences, or to receive or provide training for terrorism, in a State outside their State of nationality or residence. Second, the person must commit the act intentionally and unlawfully.[75] For example, State's authorities of a State X inform the Turkish authorities that the state's citizen named "A" is flying to Istanbul and that he intends to cross over to Syria. He gets intercepted in Istanbul Atatürk Airport the same day and is interviewed by border officials. During the interview "A" states that he comes to Turkey as a tourist, yet he does not have a return ticket and no hotel reservation. His luggage contains camouflage gear and military boots. In the course of the investigation, and faced with evidence against his initial claims, he admits that he was in fact travelling to Syria to fight for ISIL (Da'esh).

Importantly, article 4 only applies to travels undertaken from the territory of the State Party, or by its nationals. Thus, the article applies to all State Party nationals travelling, irrespective of their place of residence or starting point of travel.[76] In other words, the provision may apply to a citizen of Bosnia and Herzegovina who resides in Germany and is travelling to Turkey from Austria.

There are some differences between the wording of the Protocol and that included in Security Council resolution 2178. The Additional Protocol uses language consistent with the wording of the Convention for the Prevention of Terrorism rather than the formulation in operative paragraph 6*(a)* of Security Council resolution 2178, which uses the formulation "the perpetration, planning, or preparation of, or participation in, terrorist acts, or the providing or receiving of terrorist training".[77] In article 4(1), "the word 'commission' has been used instead of 'perpetration', and 'contribution' has been

[73] Ibid., paras. 44 and 45.

[74] Ibid., para. 47.

[75] Ibid., para. 48.

[76] Ibid., para. 49.

[77] Ibid., para. 52.

used to replace both 'planning' and 'preparation'. The phrase 'terrorist offences' is used instead of 'terrorist acts'. Finally, the phrase 'terrorist training' has been replaced by 'training for terrorism'."[78] These changes in wording were not intended to detract from the meanings contained in Security Council resolution 2178.

Interestingly, the Additional Protocol does criminalize the attempt to travel (article 4(3)). This offence must be established in accordance with the domestic law of a State Party, which "may choose to criminalise attempt to travel under existing provisions as a preparatory act or an attempt to the main terrorist offence".[79] Whether the offence will be prosecuted as an attempt to travel, preparatory activity in relation to terrorist offences, or travelling abroad for the purpose of terrorism, will depend on the domestic legislation.

3.7. Funding travelling abroad for the purpose of terrorism—article 5 (CETS 217)

Article 5(1) of the Additional Protocol defines "funding travelling abroad for the purpose of terrorism" in accordance with the definition of "travelling abroad for the purpose of terrorism" in article 4(1) as "providing or collecting, by any means, directly or indirectly, funds fully or partially enabling any person to travel abroad for the purpose of terrorism". The funds may come from a single source through, for example, a loan or gift provided by a person or a legal entity, or from various sources through some kind of collection.[80]

The funds may be provided or collected "by any means, directly or indirectly".[81] In addition to acting intentionally and unlawfully, the perpetrator must know "that the funds are fully or partially intended to finance the travelling abroad for the purpose of terrorism".[82] The drafters refer to the definition of "funds" in article 1(1) of the International Convention for the Suppression of the Financing of Terrorism:

> "assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit."

Usually, persons who fund travelling abroad for the purpose of terrorism will be associated with those recruiting future terrorists. For example, a citizen of Albania may be recruiting people in that country to join ISIL (Da'esh), as a result of which a number

[78] Ibid.

[79] Ibid., para. 53.

[80] Ibid., para. 56.

[81] Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (2015) CETS 217, art. 5(1).

[82] Ibid., art. 5(1).

of Albanian citizens decide to go to Syria. At the same time, another person may provide funds for flight tickets from Tirana to Istanbul and additional funds for travelling from Istanbul to Syria.

Article 5(2) requires States Parties to establish "funding travelling abroad for the purpose of terrorism", as a criminal offence domestically, when committed unlawfully and intentionally. The Additional Protocol does not require States Parties to criminalize the attempt or the aiding or abetting of this offence, though States Parties are free to do so.[83]

3.8. Organising or otherwise facilitating travelling abroad for the purpose of terrorism—article 6 (CETS 217)

This offence provides for the criminalization of any act of "organisation or facilitation" which assists a person who is committing the crime of travelling abroad for the purpose of terrorism.[84] "Organisation" covers conduct related to practical arrangements connected with travelling, such as the planning of itineraries, while "facilitation" refers to conduct that does not constitute "organisation" but which assists the traveller in reaching their destination (for example, assisting in unlawfully crossing a border).[85] Under article 6, the perpetrator must act intentionally, unlawfully and with the knowledge that the assistance is provided for terrorism purposes. This offence may also be "criminalised as a preparatory act or as an element of aiding or abetting to the main offence".[86]

For example, a group from Bosnia and Herzegovina may have close links with other nationals who left for Syria and have joined ISIL (Da'esh). Their mutual understanding is that those living in Bosnia and Herzegovina will organize the travelling of a number of persons from Bosnia and Herzegovina to Syria by making plans and providing funds for their route through Montenegro and Albania. From Albania the new recruits fly to Turkey, where locals help them cross the border to Syria. The locals in Montenegro and Albania assist the recruits to enter the borders of their respective countries illegally and see them off to the next border or the airport. In such case, the group in Bosnia and Herzegovina involved in the logistical/practical arrangements connected with the travelling would be investigated and charged for "organising travelling abroad for the purpose of terrorism" whereas the Montenegro and Albania locals would be investigated and charged for "otherwise facilitating travelling abroad for the purpose of terrorism".

[83] Council of Europe, Explanatory Report 217, (see footnote 20) para. 59.

[84] Ibid., para. 60.

[85] Ibid., paras. 60-62.

[86] Ibid., para. 61.

4. Investigation of offences related to foreign terrorist fighters

4.1. Introduction

During the early part of 2016, UNODC completed a series of need assessment missions in SEE, in which training on online investigations and the collection of computer-based evidence was identified as a priority in the investigation and prosecution of FTF. This section will seek to address some aspects of this area. Computers and the Internet are rapidly becoming one of the key features of modern terrorism investigations, and each can be used in the commission of crime, can contain evidence of crime, and can even be targets of crime.

There are a number of official publications available that discuss online investigations and e-evidence, including:

- The United Nations—UNODC publication "Use of the Internet for Terrorist Purposes" (2012);
- The European Union Council of Ministers Preparation of the Council meeting (Justice Ministers) report "Collecting E-evidence in the digital age—the way forward" (2014);
- The United Kingdom Association of Chief Police Officers publication "Good Practice Guide for Computer-Based Electronic Evidence" (2012);
- The United States Department of Justice publication "Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition" (2012).

All of these documents are available online and are referenced when referred to in the text.

The increased dependency on communication and data networks, storage of information within the cyberdomain, together with a lack of robust mutual consent between countries on the effective control of operations in that domain, present new challenges to law enforcement and prosecutorial authorities in combating the threat posed by terrorism, and FTF in particular. Terrorists are resourceful, creative and flexible and have been among the first groups to exploit these new technologies for criminal purposes.

In 2004, Charles Lister, a terrorism expert at the Brookings Institute said:

> …In many ways, Syria has revolutionised the jihadist use of PR and the jihadist' use of information—the dominance of social media to communicate, stay connected, provide statements—and for people to have their own accounts has been

> profound. I don't think any other conflict has come anywhere near the quantity or scale of social media use we are seeing in Syria. This effect is going to continue for years to come … it has been hugely valuable in terms of recruitment.[87]

The importance of digital evidence in the investigation and prosecution of FTFs has been widely acknowledged.[88]

In the United Kingdom of Great Britain and Northern Ireland, for instance, evidence used in court includes, inter alia, Skype conversations, photographs of training camps, as well as photographs taken in Syria.[89]

The spread of radicalization on social media is causing increasing concern, with a reported 90,000 Twitter accounts being controlled by ISIL (Da'esh) to target and recruit young people into a war where hashtags are becoming the new weapons. However, alongside other groups, ISIL (Da'esh) members have proven difficult to track due to their use of technological tools, such as encryption applications, social media platforms and encrypted instant messaging platforms. It was recently reported by a number of news outlets that ISIL (Da'esh) has released a manual for its fighters, entitled "How to Tweet Safely Without Giving out Your Location to NSA", which purports to explain how to avoid surveillance.[90] Other examples of how technologically competent Islamist terrorists have become include a number of applications developed by terrorists themselves, such as:

- **Tashfeer al-Jawwal**—an encryption platform for mobile phones, developed by the Global Islamic Media Front (GIMF), released in September 2013;
- **Asrar al-Ghurabaa**—another alternative encryption program developed by ISIL (Da'esh), which was released in November 2013, around the same time the group broke away from the main Al-Qaida following a power struggle;
- **Amn al-Mujahid**—an encryption software (released in December 2013) developed by the Al-Fajr Technical Committee, which is a mainstream Al-Qaida organization;
- **Alemarah**—an application that lists news, feeds, websites, and calendars that contain information relating to ongoing terrorist operations, released in April 2016;
- **Amaq v 1.1**—an Android application usually used by a number of terrorist organizations to disseminate information. It has various versions and Amaq 2.1 uses a configuration file that allows the applications distributor to change the URL (uniform resource locator) where the application is hosted, in case any of their websites are taken down. This technique has also been used by cybercriminals for managing malware.[91]

---

[87] *Financial Times*, 28 March 2014, available at https://next.ft.com/content/907fd41c-b53c-11e3-af92-00144feabdc0.

[88] Europol, Terrorism Situation and Trends Report, 2015. Available at www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-2015.

[89] Ibid.

[90] Pierluigi Paganini, "Covert Communication Techniques Used by Next Gen High Tech Terrorists", 12 May 2016. Available from: http://securityaffairs.co/wordpress/47243/terrorism/covert-communications-terrorists.html.

[91] Ibid.

Aside from the use for propaganda purposes, these applications mainly serve to facilitate secure communications, making it increasingly difficult for authorities to monitor and disrupt terrorist-related activities.

Alongside these bespoke applications there are also many proprietary software options and online techniques available to terrorists to facilitate security of their data and activities. Studies have indicated communications through "normal" channels (email etc.) using secret encoding techniques such as steganography and hidden watermarking remain an option.[92] These techniques, when employed with encryption create serious challenges for intelligence, law enforcement and prosecution services. One example of this can be found in the 2017 case of a man in the United Kingdom convicted for being a member of ISIL (Da'esh) as well as for terrorist training, preparing terrorist acts and possessing articles for terrorist purposes. The man had set up an online self-help guide for terrorists with techniques on encryption, ways to avoid detection from police and security services and instructional videos on how to secure sensitive data and remain anonymous online.[93] Some of the software included:

- **Tails Operating System (OS)**—A secure operating system that "boots" from a USB drive and leaves no trace on a computer unless explicitly set up to do so. All outgoing connections to the OS are forced through The Onion Router (TOR—see below) and therefore anonymous. Non-anonymous incoming connections are blocked.
- **ZeroNet**—A peer-to-peer network that allows the creation of websites that are virtually impossible to censor or take down as contents are stored on multiple users' computers, rather than on a server.
- VeraCrypt—A software which creates an encrypted volume on a hard drive, hidden within another volume. Thus, a suspect can willingly give up passwords to access a device in the knowledge that the hidden volume cannot be seen.

Other techniques and software include Tor (an acronym for The Onion Router) which is a web browser that is often referred to as the deep or dark web, a part of the Internet that is not indexed by search engines such as Google, and that encrypts connections to disrupt the possibilities of tracking web activity.[94]

In situations where encryption may not be possible, for example on an insecure channel, terrorists have been using techniques such as "chaffing and winnowing". In digital

[92] Steganography is data hidden within data—hiding a text file within an image, for instance. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method by which to protect data. Hidden watermarking is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication.

[93] See: "IS supporter Samata Ullah branded a 'new and dangerous breed of terrorist'", http://www.computerweekly.com/news/450417940/ISSamata-Ullah-was-a-new-and-dangerous-breed-of-terrorist; 'Cufflink terrorist' Samata Ullah jailed for eight years, http://www.bbc.com/news/uk-wales-south-east-wales-39736792.

[94] Retirely, "How terrorists communicate—Dark Web". Available from: www.retire.ly/how-terrorists-communicate-dark-web/.

communications, this technique allows the sender to send a message without encryption, as readable text with the receiver and sender sharing a common secret key they use for verification. With this method, the confidentiality of the message is secured by a third person who concurrently sends an expressly manufactured message through the same channel as the sender.[95]

4.2. Online investigations

The capability to effectively carry out online investigations is, more and more, becoming an essential element in all prosecutions. Of course, these types of investigations are just one aspect of a successful prosecution and complement established, traditional methods as well as other special investigative techniques.

The Internet is a huge system of interconnected computer networks, and consists of millions of private, public, academic, business, and government networks, linked by a broad array of electronic, wireless, and optical networking technologies. These links are possible due to a number of global protocols, the most important of which for an investigator is the Internet Protocol (IP). The worldwide web (www) is an information space where documents and other resources can be accessed on the Internet. At the time of development of the "web", three specifications for web technologies were defined: URL; Hypertext Transfer Protocol (HTTP); and Hypertext Markup Language (HTML).

The basis for Internet communication is a process of assigning an address to each device attached to the Internet. This address allows a device to connect and communicate with any other device connected to the Internet using this scheme. This scheme is commonly referred to as the IP address, and can be compared to something like the postal system. It allows a person to address a package and drop it in the system. The other part of the communication protocol is known as Transmission Control Protocol (TCP). TCP is one of the main protocols in TCP/IP networks. Whereas the IP deals only with packets of data, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

There are two versions of IP: IPv4 and IPv6. IPv4 uses a 32-bit address scheme allowing for the possibility of over 4 billion addresses. With the massive growth of the Internet it is expected that the number of unused IPv4 addresses will eventually run out. Due to the fact that each connected device requires a unique address, a new Internet addressing system Internet Protocol version 6 (IPv6) is being deployed to fulfil the need for more Internet addresses.

[95] Ibid.

What do IP (v4 and v6) addresses look like?

A 32-bit numeric address (IPv4) is written in decimal as four numbers separated by full stops. Each number can be zero to 255. For example, 1.160.10.240 could be an IP(v4) address.

IPv6 addresses are 128-bit IP address written in hexadecimal[96] and separated by colons. An example IPv6 address could be: 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

The two IP versions will be running in tandem for some time in the future, so investigators can expect to see both versions during their research.

There are two ways in which a device can be allocated an IP address when it connects to the Internet; either with a dynamic or static allocation. Dynamically assigned addresses are done through a process called Dynamic Host Configuration Protocol (DHCP). This protocol is software running on a server or router, for example, that determines the assignment of IP addresses to other devices in the network. Effectively, the DHCP assigns the address out of a pool of addresses. This becomes part of the investigation trail that needs to be followed. A static IP address is normally allocated, for instance, to a server providing a service such a web page. Assigning a static (or permanent) address allows devices to return to that same location on the Internet.

Once an IP address has been identified an Internet search will reveal the Internet Service Provider (ISP) through which the device associated with the IP connected to the Internet. As all ISPs are based on subscriptions to the company, these companies have records of every subscriber's Internet activities.

The time frame that ISPs retain data from subscribers varies; therefore the investigation must move quickly. Investigators can make a formal request to the ISP requesting that they preserve the data in question while a subpoena, warrant, or court order is made requiring production of the records. As there is no common data retention policy in place in Europe, and ISPs have the discretion to decide on data retention time frames, some ISPs retain data for 6 months, some for 2 months, and some for as little as 14 days.

What is an online investigation?

It is important to consider the term "online investigation", which could cover a number of concepts, including:

- **Covert intelligence operations** (monitoring known or suspected terrorist sympathizers prior to judicial proceedings)—normally this type of task falls under the competence of security or intelligence services and as such will not be discussed in this document.

[96]Hexadecimal is an easier way to represent binary values in computer systems because they significantly shorten the number of digits, as one hexadecimal digit is equivalent to four binary digits.

- **Open source intelligence gathering (OSINT)**—this includes general research on the Internet, accessing information that is available to anyone without the need for a surveillance authority, a subpoena or warrant.
- **Undercover law enforcement operations**—these are fully authorized covert activities by specially trained law enforcement officers. This type of Internet investigation will not be covered in this document as it is governed by domestic legislation and therefore differs among jurisdictions.

Open source investigations

There is a public expectation that the Internet will be subject to routine "patrol" by law enforcement agencies, even though it only concerns accessing open source information. As a result, many bodies engage in proactive attempts to monitor the Internet and to detect illegal activities. In some cases, this monitoring may evolve into "surveillance" and in these circumstances investigators should refer to their respective legislation for the appropriate authority to continue.[97]

The investigator should always ensure that they are using an anonymous, stand-alone computer when surfing the Internet for this purpose. There are, more than likely, policies and procedures in place to cover investigators' open source activity, but some techniques to consider include:

- **Virtual Private Networks (VPN)**—a VPN extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and thus benefit from the functionality, security and management policies of the private network.
- **PROXY servers**—in computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients (in this case, the investigator's computer) seeking resources from other servers.
- **Pay-as-you-go subscriber identity module (SIM) cards**—use of a cellular phone network from a local provider to access the Internet, using a different SIM card each time the Internet is accessed.
- **The Onion Router (Tor)**—Tor is free software which enables anonymous communication, for all users, including investigators. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than seven thousand relays which conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult for Internet activity to be traced back to the user. This includes "visits to websites, online posts, instant messages, and other communication forms".[98] Tor is

[97] See United Kingdom Association of Chief Police Officers, "Good Practice Guide for Computer-Based Electronic Evidence". Available from: https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf.

[98] See www.nytimes.com/2006/01/25/technology/techspecial2/privacy-for-people-who-dont-show-their-navels.html.

intended to protect the personal privacy of users, as well as their freedom and ability to conduct confidential communications by preventing their Internet activities from being monitored.

When carrying out open source research, investigators should ensure that IP addresses are changed each time they log on to the Internet. Ideally they should be choosing which IP address is associated with the device they are using to connect.

It is highly desirable that investigators tasked with OSINT research are suitably trained in order to ensure the integrity of their work, and the security of the computer network through which that research is carried out. Without such cover, the investigator may be disclosing over the Internet who they are, or who they work for, and thus hamper any future investigations.

Social media

Social media applications can be powerful tools for monitoring events and/or people for intelligence purposes. It should be stressed that Open Source Intelligence (OSINT) relates to open information, freely posted by individuals or groups to the Internet, and available without the need to access restricted areas of the world wide web (for instance, so-called "closed forums", which are password protected and moderated by nominated users and would, more than likely, require surveillance authorities or warrants prior to an investigation). The veracity of the intelligence should be treated with care and, in practice, corroboration of OSINT is always desirable before executive action is considered.

The figures below give some idea of the challenges faced by investigators in terms of the volume of information available on social media alone.

It is reported that every minute of every day:

- Twitter users send 347,222 tweets;
- Instagram users like 1,736,111 photos;
- YouTube users upload 300 hours of new video;
- Facebook users like over 4 million posts.

There are numerous programs available (commercial and freeware) that can assist in analysing mass data (for instance, a number of Twitter accounts that are interconnected and that distribute messages across the globe). Many of these programs provide a "picture" of a network of connections and can assist in identifying key individuals in that network, i.e. those that are best placed to reach out to the network and those who may be targeted to disrupt the effectiveness of a given network. One of the most widely used tools for online network investigations is a commercial analysis program made by Paterva called Maltego.[99]

[99] See www.paterva.com/web7/.

There are other examples of online search tools that are available to the investigator, free of charge and worthy of consideration when embarking on OSINT research:

- Intel Techniques—a commercial OSINT training portal that offers (free of charge) a list of online Internet search tools;[100]
- NetBootCamp—a learning and resource website focused on online investigation skills and techniques. The content is intended for law enforcement officers, corporate investigators, private investigators, analysts, prosecutors, and attorneys. NetBootCamp also provides a number of online search tools.[101]

Many users of social media create an alias as their username; often this alias will be used across a variety of platforms. In many cases, investigators can discover what aliases a person uses by simply searching for the person's real name. Twitter, for example, will show a username associated with a person's real name. SocialMention[102] and CheckUserNames[103] are also useful tools for finding other sites where usernames appear.

Smartphones often tag pictures with Global Positioning System (GPS) coordinates (known as a GeoTag), which enables identification of where a picture was taken by looking inside its Exchangeable Image File Format (EXIF) data.[104] This information is deleted from photographs uploaded to Facebook but is often preserved on Twitter and Photobucket.

There is also a special Google search operator that shows files stored on uncovered servers. This search format is known as "Advanced Google Search Operator". Using this method, it is possible to discover files belonging to a person, for example, a résumé. To access this function, type the following command into Google:

> in title: "index of" "parent directory" john doe (John Doe should be replaced with subject's name or alias).

Finding people who visit certain websites can be difficult. Many sites (especially blogs) do not have a built-in "user search" function that shows all pages where the subject has left a comment or created a profile, for example. It is, however, possible to perform the following search in Google, which will show all comments made by an individual on whatever website is searched for:

> site: [domain.com] ["John Doe"] says: (replacing the domain.com and John Doe with name of the site and subject's name/nickname). E.g.: site: twitter.com "[Suspect's Name, User Name or Alias]" says:

[100] See https://inteltechniques.com/intel/menu.html.

[101] See http://netbootcamp.org/osinttools/.

[102] See www.socialmention.com/#.

[103] See http://checkusernames.com/.

[104] The standard that specifies formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners and other systems handling image and sound files recorded by digital camera. See https://en.wikipedia.org/wiki/Exchangeable_image_file_format.

This can be useful for building a suspect's profile. People often mention personal details in comments, such as the city they may be visiting, websites they frequent, or places where they spend time. This a good source of additional leads and a chance to apply other investigative techniques.

Facebook

After registering to use Facebook, users can create a user profile, add other users as "friends", exchange messages, post status updates and photos, share videos, use various apps, and receive notifications when others update their profiles.

Additionally, users may join common-interest user groups organized by their workplace, school, or other characteristics, and categorize their friends into lists such as "People From Work" or "Close Friends". Facebook is the most popular social networking site in several English-speaking countries, including Canada, the United Kingdom, and the United States. In regional Internet markets, Facebook penetration is reported to be highest in North America, followed by Middle East-Africa, Latin America, Europe, and Asia-Pacific. Facebook penetration in the relevant SEE jurisdictions vis-à-vis Internet use by June 2016 is set out in the table below:[105]

Jurisdiction	Internet usage/penetration (% of population)	Facebook usage/penetration (% of population)
Albania	1,823,233 / 62.6%	1,400,000 / 48.1%
Bosnia and Herzegovina	2,628,846 / 69.3%	1,500,000 / 39.5%
Kosovo (under UNSC resolution 1244)	1,523,373 / 80.4%	560,000 / 29.5%
Former Yugoslav Republic of Macedonia	1,439,089 / 69.1%	1,000,000 / 48.0%
Montenegro	379,480 / 61.0%	320,000 / 51.4%
Serbia	4,705,141 / 66.2%	3,600,000 / 50.6%
Europe	630,710,269 / 76.7 %	328,273,740 / 39.9%
World	3,396,240,430 / 49.2 %	1,679,433,530 / 22.3%

Privacy

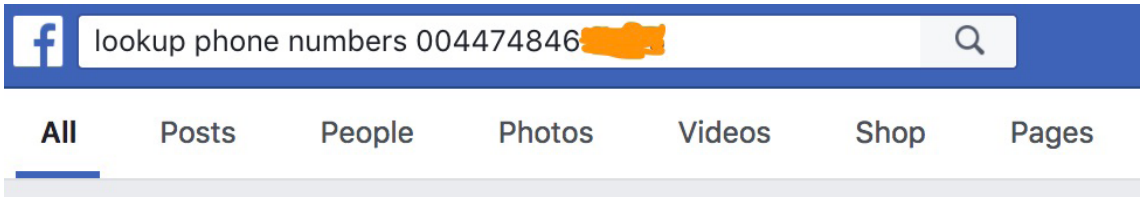
Facebook enables users to choose their own privacy settings and choose who can see specific parts of their profile. The website is free to its users and generates revenue from advertising, such as banner advertisements. Facebook requires a user's name and

[105] Internet World Stats, http://www.internetworldstats.com/stats4.htm#europe. Facebook penetration statistics were last updated in June 2016. Site accessed 7 August 2017 (see also http://www.internetworldstats.com/surfing.htm).

profile picture (if applicable) to be accessible by everyone. Users can control who sees other information they have shared, as well as who can find them in searches, through their privacy settings.

Facebook investigations

Facebook can look up telephone numbers. Enter a phone number into Facebook's search box to find the account associated to a phone number. Alternatively search for a person's profile by entering email addresses into the search box.



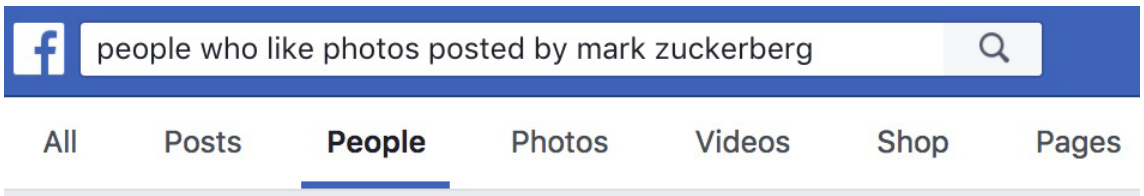
Graph searching

By using Facebook's own search engine, various bits of information can be found. For example, people can access a list of publicly viewable photos people have "liked" and read comments that have been posted. Also, by using the unique ID code that every page on Facebook has, additional means of research beyond mere word searches are possible. For instance, if research is being carried out on someone with the name "William" who live near Edinburgh, type "People named 'William' who live near Edinburgh, Scotland". There are also a number of other terms that may be used to trace a person, including:

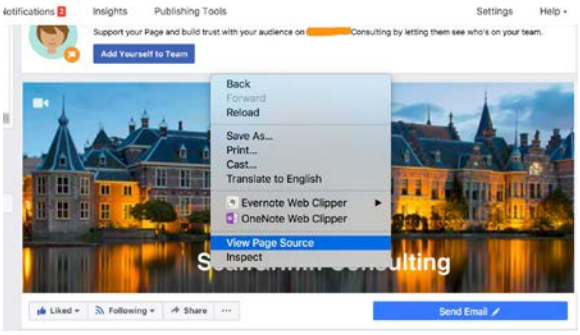
- Find friends of people named "first.name last.name";
- Find photos of people named "first.name last.name";
- Find people who have visited "place name".

Even if the person being researched has blocked himself or herself from public view, they may still be able to be found through family members.

A friends list may have been made "private", but people can still see who has liked a user's photos. Often friends will have clicked "like" on some of the photos uploaded and a list of these people can be obtained by searching for "People who like pictures posted by [suspect]". Additionally, anyone who "friend requests" the suspect will see [the suspect's] private friends suggested to them as "people you may know", whether or not the suspect accepts that person's friend request.



Each person and every page on Facebook has a unique ID code. These codes are useful as they allow researchers to specify a person, place or thing in "advanced" Facebook searches. This code can be found by looking in the html code for a profile page. To do this, right click on the page and look for "view source".



This will bring up a window that displays html code for that page. This is program language that tells a web browser (for example Safari, Google Chrome of Firefox) how to display a web page. The coding looks something like the picture below.

This file can be searched using the "Control" key and "f". Look for "profile_id" and the number shown next to that is the unique Facebook ID number. The same technique also works for subject pages on Facebook.

Facebook can also be searched via Google, using the syntax "site:facebook.com". Words which should be in the title of the Facebook page can be specified by using "intitle:" followed by the word. For example, to search Facebook pages that are about INTERPOL, but mention Sweden, the search term would read:

Sweden intitle: INTERPOL site:facebook.com

Images

It is possible to trace photographs back to a Facebook account. Images on web pages have their own file names. Some of them might be named after the subject (e.g. "englandrugby.gif") and others may have had a file name automatically generated by the camera that took the photo (e.g. "dsc_1234.jpg"). Some pictures are named by a website's database. When a photograph of interest is discovered, "right-clicking" on the picture and then "saving" the image will reveal the file name of that particular image.

When an image is uploaded to Facebook (or Instagram), the name of the image will be changed, usually to something consisting of three groups of numbers separated by underscores and finishing with "n.jpg", for example, "xxxxxx_12345678910_xxxxxxxxxx_n.jpg". Therefore, if an image with this type of file name is discovered, the image has probably been posted on Facebook. The second group of numbers in these file names relate to the Facebook account to which the image was uploaded and can be copied into a "facebook.com" web address in order to find the user of the account where the picture is, or was, originally posted.

In the case of the above example the web address (submitted using the computer browser window) would read "http://www.facebook.com/12345678910".

There are a number of Internet tools that allow image searches, in order to establish where else the pictures may appear. This is known as reverse image searching and is particularly useful in cases where people use the same profile picture on various websites and social networks.

- Tineye—upload a saved image and follow on-screen instructions;[106]
- Google Images—click on the camera icon in the search window to upload the image for searching. Google will then show you addresses of other pages where your chosen image appears, e.g. Twitter accounts, blogs and personal websites.[107]

Facebook itself provides guidelines for law enforcement officers on its website entitled "Information for law enforcement authorities" outlining procedures for investigators who may be seeking records from the website.[108]

Twitter

Twitter is an online social networking service that enables users to send and read short 140-character messages called "tweets". Registered users can read and post tweets, while those who are not registered can only read them. Users access Twitter through

[106] See www.tineye.com.

[107] See https://images.google.com/.

[108] See https://www.facebook.com/safety/groups/law/guidelines/.

the website interface, SMS or mobile device app. By May 2015, Twitter had more than 500 million users, out of which more than 332 million were active.

Users can group posts together by topic or type by using hashtags—words or phrases prefixed with a "#" sign. Similarly, the "@" sign followed by a username is used for mentioning or replying to other users. To repost a message from another Twitter user and share it with their own followers, a user can click the retweet button within the tweet.

With approximately 46,000 Twitter accounts operating on behalf of ISIL (Da'esh), social media represents a powerful instrument in ISIL (Da'esh) propaganda.[109]

Privacy and security

Twitter messages are public, but users can also send private messages. Information about who has chosen to follow an account and who a user has chosen to follow is also public, though accounts can be changed to "protected", which limits this information (and all tweets) to approved followers.

Twitter collects personally identifiable information about its users and shares it with third parties as specified in its privacy policy.

Twitter investigations

The first thing to understand in conducting Twitter investigations is that Twitter search results are divided into several sections. It is possible to switch between the following categories within the application itself: People, Images, Tweets, and Videos.

Results are determined by Twitter's search algorithms, and one of the first results returned after a search will be the "top" tweets (i.e. the most popular). If a more stringent search is required, be sure to click "All".

- **Location-based search**—searches can be carried out for tweets that come from or are near to a certain location. e.g. Type "near:NYC within:5mi" to return tweets sent within five miles of the New York City.
- **Search for tweets with links**—if only tweets that contain links are required, add filter:links to your search phrase.
- **Search for tweets from a certain user**—if a keyword search for data from one particular person is required, type "from:[username]" to search within his or her stream.

[109] International Centre for Counter-Terrorism, "The Foreign Fighters Phenomenon in the European Union", April 2016. Available from: http://icct.nl/wp-content/uploads/2016/03/ICCT-Report_Foreign-Fighters-Phenomenon-in-the-EU_ 1-April-2016_including-AnnexesLinks.pdf.

- **Search up to/from a date**—it is possible to search Twitter for content up to and after certain dates. Typing "since:2012-09-20" will show tweets sent since 20 September 2012, while "until:2012-09-20" will show those sent up to the same date.
- **Search for tweets from certain sources**—if an investigator is searching for tweets sent via SMS, or from a particular Twitter client, the "source" search operator should be used. For example, "source:txt" will bring up tweets sent via SMS.

All of these operators can be found on Twitter's "Advanced Search" page, many of which are provided there in a template for ease of use.

Other (free to use) online tools include:

- **Geosocial Footprint**;[110]
- **Tweetpaths**—when the name of a user on Twitter is known, searching for that name on either of these tools will display results on a map, showing the location from where that user's tweets were posted.[111]
- **Conweets**—enter the user names of two Twitter users and this software will display conversations between the them.[112]
- **Twazzup**—provides real-time monitoring and analytics for Twitter.[113]

Tools for downloading and analysing Twitter data:

- **BirdSong Analytics**—BirdSong Analytics is a useful tool that facilitates the download of all followers of any Twitter account. This is a commercial tool that requires purchasing. The export comes in the form of an Excel spreadsheet and contains each username, number followers/following, real name, Twitter URL, bio, number of tweets, date when the account was created, location, verified status and how many lists the account is included into. The use of an Excel export offers the investigator many options in analysing mass data and is compatible with many programs favoured by law enforcement (e.g. I2 or Analysis Notebook). Excel itself offers sorting, filtering and searching options; you can now find most-followed accounts, search bios by a keyword, sort accounts by location, etc. For example, you can download all people your suspect follows and investigate their habits, sites, etc. Or you can download all accounts that @[your_suspect] is following for further research.
- **NodeXL**—a simple, but very thorough tool. It is an open source template for Microsoft Excel that works by integrating data pulled from a CSV (comma separated value) file into an informative network graph in order to, for instance, create a visual representation of your tweets from any period you choose.

[110] See http://geosocialfootprint.com/.

[111] See www.tweetpaths.com.

[112] See www.conweets.com/.

[113] See http://twazzup.com/.

A recent investigation in the UK (Operation Road) led to the first British conviction related to fighting in Syria. The subject of the investigation, Mashudur Choudhury, is reported to have been very active on Twitter, posting in the region of 10,000 tweets (messages) and having 3,000 accounts listed as "followers".

Twitter could be seen as an Internet version of mobile telephone "SMS" texts, and researching such a potentially vast number of messages and connections can be a daunting task. Twitter provides information for investigators on procedures for seeking records from the company.[114]

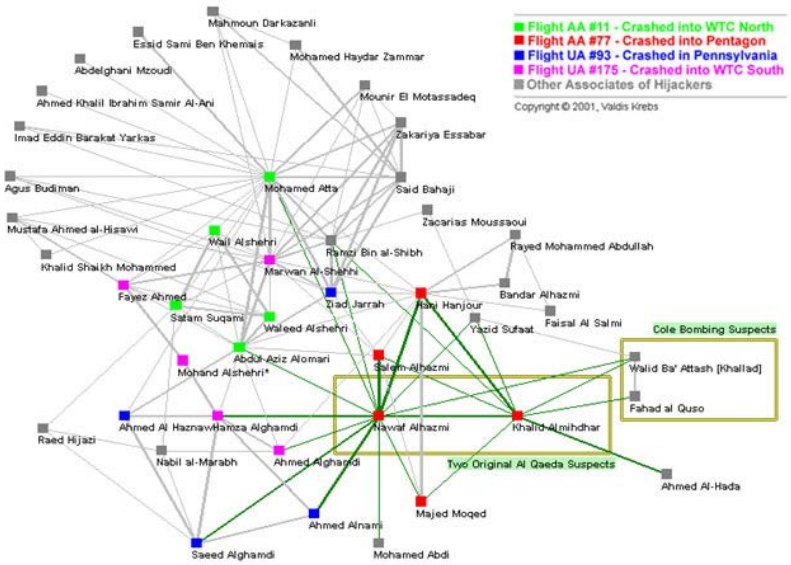
Alongside the analytical tools already discussed, there is also the possibility to use this mass data to map a social network (social network analysis or SNA). SNA provides a visualization of a network and, through a series of algorithms, works out a particular person's place in his or her network. The term used in SNA is the "centrality measure", i.e. how "central" to the group a person is in terms of influence, access, direct contact and as a go-between.

Centrality measure	Interpretation in social networks	Another way of putting it...
Degree	How many people can this person reach directly?	In network of music collaborations: how many people has this person collaborated with?
Betweenness	How likely is this person to be the most direct route between two people in the network?	In network of spies: who is the spy though whom most of the confidential information is likely to flow?
Closeness	How fast can this person reach everyone in the network?	In network of sexual relations: how fast will a sexually transmitted disease (STD) spread from this person to the rest of the network?
Eigenvector	How well is this person connected to other well-connected people?	In network of paper citations: who is the author that is most cited by other well-cited authors?

An excellent example of the power of SNA can be found in a paper by Dr Valdis Krebs, who produced an analysis of the 9/11 hijack teams purely from open source information (mainly news articles as this article was written pre-Twitter and Facebook).[115] His results come remarkably close to the actual position within the network for each of the hijackers.

[114] See https://support.twitter.com/articles/41949.

[115] Valdis Krebs, "Uncloaking Terrorist Networks", *First Monday,* April 2002. Available from: http://firstmonday.org/ojs/index.php/fm/article/view/941/863%20network%20analysis%20of%20terrorist%20networks.



All nodes within two steps/degrees of original suspects

4.3. What evidence to collect

In common with established methods of investigation, the collection of computer- or Internet-based evidence should be conducted in accordance with domestic legislation and procedures.

The following definitions discuss what is meant by "e-evidence", and are provided as examples when discussing methods of collecting such evidence:

- **ESI (electronically stored information)** includes any information created, stored or utilized with digital technology. Examples include, but are not limited to, word-processing files, email and text messages (including attachments), voice-mail, information accessed via the Internet, including social networking sites; information stored on cellular phones; information stored on computers, computer systems, thumb drives, flash drives, CDs, tapes and other digital media.[116]
- **Computer-based electronic evidence** is information and data of investigative value that is stored on or transmitted by a computer. As such, this evidence is latent evidence in the same sense that fingerprints or DNA (deoxyribonucleic acid) evidence is latent. In its natural state, we cannot see what is contained in the physical object that holds our evidence. Equipment and software are required to make the evidence available.[117]

[116] United States Department of Justice and Administrative Office of the U.S. Courts Joint Working Group on Electronic Technology in the Criminal Justice System, February 2012, p. 12.

[117] Association of Chief Police Officers, Good Practice Guide, (see footnote 97).

- **Digital evidence** can be classified as information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination. Digital evidence is latent (like fingerprints or DNA evidence) and crosses jurisdictional borders quickly and easily. It can easily be altered, damaged, or destroyed and can be time-sensitive.[118]

In all instances, the investigation and prosecution of cases involving digital evidence requires specialist criminal investigation skills, as well as the expertise, knowledge and experience to apply those skills in a virtual environment. A sound familiarity of legal and procedural requirements relating to admissibility and rules of evidence, domestically and internationally, is also required.

When deciding on what ESI or digital evidence to collect, consideration should be given to the environment in which such information and evidence will be gathered—through online investigation, or at a crime scene.

As previously discussed, an initial phase in an investigation may include an amount of OSINT gathering. Throughout this phase and as an investigation moves to the next stage (by concentrating research towards proving specific criminal acts) records should be kept of the process and progress of the research. These records form the foundation of the online evidence chain.

One of the first phases of an investigation in identifying the person(s) responsible for online criminal activity is to trace and follow IP addresses. As stated above, IP addresses provide the basis for online communication. Tracing IP address and domains is a key part of any Internet investigation and there are many resources available on the Internet to assist with this process. Firstly, there are the entities responsible for the addressing system itself, the Internet Assigned Number Authority, where searches can be carried out by region through the Regional Internet Registries.[119] Each site has a "WHOIS" function that allows investigators to identify IP registration information.[120] The registration information refers to the registrant, the person or entity paying for the service. In order to access, for instance, payment information or IP logs, investigators would need to contact the registrar, again in accordance with their respective domestic guidelines, procedures and legislation.

Once an IP address has been traced the investigator will be able to request data from an ISP in order to determine who is actually behind the device to which with IP address refers. Such requests are usually in the form of a subpoena or warrant to the local judge depending upon domestic legislation and procedures.

[118] United States Department of Justice, "Electronic Crime Scene Investigation: A Guide for First Responders", Second Edition, April 2008. Available from: www.ncjrs.gov/pdffiles1/nij/219941.pdf

[119] See www.iana.org/.

[120] WHOIS is an Internet utility that returns information about a domain name or IP address. For example, if you enter a domain name such as microsoft.com, WHOIS will return the name and address of the domain's owner (in this case, Microsoft Corporation).

Other online tools for tracing and investigating IP addresses include Network Tools[121] and Robtex.[122]

Websites and cookies

Ultimately, any information on the Internet physically resides on one or more computer systems and, therefore, it could be retrieved through a forensic examination of those physical devices. However, some of this information may be volatile (e.g. instant messaging content), or it could be altered or deleted prior to the location and examination of those devices (e.g. website content). In such cases, it may be necessary to capture evidence directly from the Internet, possibly during "live" interaction with a suspect or by capturing live website content.[123] There are many tools freely available to assist, including:

- HT Tracks;[124]
- Wget;[125]
- Wayback Machine—a website archive site;[126]
- Scrapbook—a "plug in" for the Google Chrome and Firefox browsers.

Once a website has been captured or collected, an investigator will have access to potentially useful investigative information. The pages themselves can be reviewed, as can the way in which the browser produces the page. An investigator can look for who wrote the page, and also check on names of people, organizations or groups that claim responsibility for the site. There may be an email address for a person or group, and an investigator can research the email address through a search engine to establish if it is used elsewhere on the Internet. If the site is not grammatically correct and contains typing errors this may be an indication of the level of understanding of the language used and a possible indication of the origin of the author. If a foreign language website is encountered there are many resources to provide assistance in translation, but perhaps not to an evidential level, which would require an official translation to local judicial standards.

An investigator should also consider the use of "cookies". Cookies are small files that are stored on a user's computer. They are designed to hold a modest amount of data specific to a particular client[127] and website, and can be accessed either by the web server or the client computer. This allows the server to deliver a page tailored to a particular user (for instance a password), or the page itself can contain some script (a script is a list of commands that can be automatically executed) which is aware of the data in the cookie and so is able to carry information from one visit to the website (or related site) to the next.[128]

---

[121] See http://network-tools.com/.

[122] See www.robtex.com/.

[123] Association of Chief Police Officers, Good Practice Guide, (see footnote 97).

[124] See www.httrack.com/.

[125] See www.gnu.org/software/wget/manual/.

[126] See https://archive.org/web/.

[127] A client is a piece of computer hardware or software that accesses a service made available by a server.

[128] See www.whatarecookies.com/.

For example, imagine that a person who is known to have been in Syria is arrested upon their return from the region and a mobile telephone is recovered during the arrest. An examination of the phone is conducted, which reveals that the suspect accessed their Facebook account while in Syria. The Facebook website would have left a cookie on the suspect's mobile phone (unless of course cookies were denied or deleted by the user). Upon investigation, it is discovered that the same Facebook cookie is associated with a number of other Facebook users. This could possibly indicate that the suspect's phone was used by other foreign fighters while in Syria, which provides intelligence leads for further development.

Internet logs

Computer documents, emails, SMSs and instant messages, transactions, images and Internet histories are examples of information that can be gathered from electronic devices and can be used very effectively as evidence. Websites themselves maintain IP logs. For instance, the Google email site Gmail would maintain IP logs for account holders and for the original IP from where the account was registered. Also, mobile devices, laptops and desktop computers use online-based backup systems, also known as the "cloud".

With regard to mobile devices, cloud-based systems can provide forensic investigators with access to text messages and pictures taken from a particular phone, and keep an average of 1,000-1,500 (or even more) of the last text messages sent to and received from that phone. In addition, many mobile devices store information about the locations where the device may have travelled and provide an idea as to when exactly it had been there. To obtain this information, investigators can access an average of the last 200 cell locations accessed by a mobile device. Satellite navigation systems and satellite radios in cars can provide similar information. Photos taken with a GPS-enabled device contain file data that shows when and exactly where a photo was taken.[129] A potentially useful site for converting location-based information (GPS coordinates or longitude/latitude references) is Hamstermap, which offers a facility for mass data entry (for instance from CSV Excel files).[130]

Encryption and anonymizing techniques employed in connection with other forms of Internet communication are similarly applicable to files shared via, inter alia, peer-to-peer (P2P) and file transfer protocol (FTP) technology. File-sharing websites that provide parties with the ability to easily upload, share, locate and access multimedia via the Internet include Rapidshare, Dropbox and Fileshare. Some file-sharing networks may maintain transfer logs or payment information, which may be relevant in the context of an investigation.

The data servers used to provide these services might also be physically located in a different jurisdiction from that of the registered user, with varying levels of regulation

[129] Association of Chief Police Officers, Good Practice Guide, (see footnote 97).

[130] See www.hamstermap.com.

and enforcement capabilities. Close coordination with local law enforcement may therefore be required to obtain key evidence for legal proceedings.[131] In such cases, competent national authorities should make use of the available tools for international cooperation, e.g. requesting mutual legal assistance (MLA).[132]

Investigators should also consider referring to the UNODC document "Basic tips for investigators and prosecutors for requesting electronic/digital data/evidence from foreign jurisdictions"[133] which outlines a number of good practices including, for instance, the need to have exhausted internal/national sources for obtaining electronic data/evidence prior to sending requests to a foreign country and, in consideration of an investigative strategy, to verify with the requested authority whether an account holder may learn of any preservation request (for instance if it is the policy of an ISP to notify their clients).

It could be also explored whether the formal requirements in the MLA procedures may be further differentiated depending what data is requested (for example, whether it is subscriber, traffic or content data).[134] In many jurisdictions, requirements for access to subscriber data tend to be lower than for traffic data, while the most stringent regime applies to content data.[135]

Cooperation with the private sector is also an essential element in securing digital evidence and in some cases, competent authorities could consider addressing a request directly to the foreign-based service providers, which may be allowed under domestic legislation to disclose non-content data on a voluntary basis to law enforcement authorities. Many Internet and communication-based companies have developed guides to assist law enforcement officials in understanding what information is available and how that information may be obtained. Links to publicly available guides for some of those sites, including Facebook and Twitter, can be found on the website of the International Association of Chiefs of Police.[136]

However, any evidence obtained in this manner may not be admissible before the court before it has been "officialized" through the MLA framework.

[131] UNODC, "Use of the Internet for Terrorist Purposes", 2012. Available from: www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

[132] UNODC Manual on Mutual Legal Assistance and Extradition. Available http://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf

[133] See annex 5.2. Available at https://www.unodc.org/documents/legal-tools/Tip_electronic_evidence_final_Eng_logo.pdf.

[134] Subscriber data relates to an individual paying for, or subscribing to, a service; traffic data means information relating to the connections made between telephones or computers; content data relates the actual content of a message or conversation.

[135] Council of the European Union, "Collecting E-evidence in the digital age—the way forward" (13689/15), 4 November 2015. Available from: http://data.consilium.europa.eu/doc/document/ST-13689-2015-INIT/en/pdf.

[136] See International Association of Chiefs of Police, "Center for Social Media Tools and Tutorials". Available at: http://www.iacpsocialmedia.org/resources/tools-tutorials/.

4.4. How to collect e-evidence

The challenges facing law enforcement and prosecutors carrying out "digital" or online investigations are underlined in the EU report "Collecting E-evidence in the digital age—the way forward", which states that "The effective collection, sharing and admissibility of e-evidence in criminal proceedings present one of the main challenges from a criminal justice perspective…".[137]

While there are several challenges in collecting e-evidence, there are many examples of good practice, some of which will be discussed in the following section.

As previously stated, there may be two types of crime scenes in a digital investigation: the online scene, where the investigator does not have physical possession of evidence, and the classic scene, where physical evidence can be recovered, and forensically examined. A physical crime scene in the sense of a digital investigation would also include an element of non-physical evidence, such as information accessed in the cloud from a suspect's device.

Handling digital evidence at a scene

Precautions should always be taken in the collection, preservation, and transportation of digital evidence in order to maintain its integrity. The UK Association of Chiefs of Police guidelines for computer evidence discuss good practice principles in capturing ESI or Digital Evidence:

- Devices, peripherals and other materials may be collected once a crime scene has been secured and a legal authority is in place to seize evidence.
- Before recovering anything, first photograph or video the scene and all the components including the leads in situ. If no camera is available, draw a sketch plan of the system and label the ports and cables so that the system(s) may be reconstructed at a later date.
- Document any activity on the computer, components, or devices, again by taking a photograph and record any information that can be seen on the screen.
- Physical searches of suspects and the location of computers may reveal personal identification numbers (PINs) and passwords.
- Recover associated chargers, cables, peripherals and manuals, along with thumb drives, cellular phones, external hard drives and electronic photo frames etc.
- Many of these devices are examined using different tools and techniques, and this is most often carried out in specialized laboratories.
- To prevent the alteration of digital evidence during collection, document any activity on the computer, components, or devices by taking a photograph and recording any information on the screen.

[137] Council of the European Union, "Collecting E-evidence in the digital age—the way forward" (see footnote 135).

- The mouse may be moved (without pressing buttons or moving the wheel) to determine if something is on the screen.[138]

It is important to remember that device operating systems and other programs frequently alter and add to the contents of electronic storage. This may happen automatically without the user necessarily being aware that the data has been changed. The following four principles are worthy of consideration during this stage of an investigation:

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
2. In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.[139]

In considering the issue of volatile information, the second principle is key to any decisions taken when weighing up the possibility of losing volatile information against the need to preserve, as much as possible, the original state of the devices at the time of evidential recovery.

Live forensics

Evidence handling is one of the most important aspects in the expanding field of computer forensics. The never-ending innovation in technologies tends to keep best practices in constant flux in an effort to meet industry needs. One of the recent shifts in evidence handling has been the shift away from simply "pulling the plug" as a first step in evidence collection to the adoption of methodologies to acquire evidence "live" from a suspect's computer.

Effectively, "live forensics" provides for the collection of digital evidence in an order that is based on the life expectancy of the evidence in question. Perhaps the most important evidence to be gathered in digital evidence collection today and for the foreseeable future exists only in the form of the volatile data contained within the computer's RAM (Random Access Memory).[140] However, this crucial piece of evidence

[138] Association of Chief Police Officers, Good Practice Guide, (see footnote 97).

[139] Ibid. p. 4.

[140] Elsevier SciTech Connect, "Incident Response: Live Forensics and Investigations", p. 103. Available from: http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Incident-Response-Live-Forensics-and-Investigations.pdf.

is easily captured using live forensic and investigative tools, allowing the entire contents of RAM to be captured locally and even remotely.

The traditional "pull-the-plug" approach overlooks the vast amounts of volatile (memory-resident) data that could be lost. Today, investigators are routinely faced with the reality of sophisticated data encryption, as well as hacking tools and malicious software that may exist solely within memory.[141] If a computer is on, using a computer forensic expert is highly recommended, as turning off the computer may result in the loss of evidence relating to criminal activity. However, if a computer is on but is running destructive software (formatting, deleting, removing or wiping information), power to the computer should be disconnected immediately to preserve whatever is left on the machine.

The need for changes in digital evidence collection is being driven by the rapidly changing computing environment:

- Applications are installed from removable media such as a USB (Universal Serial Bus) devices and are then virtualized in RAM without leaving a trace on the hard disk.
- Malware is fully RAM-resident, with no trace of existence on the hard disk.
- Users regularly utilize covert/hidden encrypted files or partitions (areas of a hard drive) to hide evidence.
- Popular web browsers offer the user the ability to cover their tracks—log files of user activity are created but deleted when the browser is closed.

Capturing and working with volatile data may provide the only route towards finding important evidence that would not normally be present if the machine was powered down for a post-mortem investigation. This information can consist of, inter alia, user accounts, passwords, unsaved document content, malicious software, running processes, event logs, network information, registered drivers, and registered services.

Often, computer users are unaware of the existence of services running on a computer, as the service runs in the background and may not belong to a user. This means that while at a crime scene conducting live forensic examinations an agent may be able, for instance, to see a driver for a digital camera.[142] Such a discovery could possibly indicate that a digital camera has recently been used with the computer, and a search could then be undertaken to locate the digital camera before the agent leaves the scene, thereby potentially securing valuable evidence. Thus, discovering registered drivers may give investigators information about the peripheral devices associated with a suspect's machine.

[141] Association of Chief Police Officers, Good Practice Guide, (see footnote 97).

[142] A driver is a program that controls a device. Every device, whether it be a printer, disk drive, or keyboard, must have a driver program. Many drivers, such as the keyboard driver, come with the operating system. For other devices, you may need to load a new driver when you connect the device to your computer. See http://www.webopedia.com/TERM/D/driver.html.

Seizing mobile devices

If a mobile device is switched off, the investigator should not attempt to turn it on and should remove the batteries, if possible. A phone that is switched off preserves cell tower location information and call logs and also prevents the phone from being used, which could potentially change the data on the phone. Additionally, if the device remains on or is switched on, there is always the possibility that remote commands could be used to destroy any evidence without the investigator's knowledge. Some phones have operating system updates set to automatic, and updates could compromise data on the device, so battery removal is optimal.

If a mobile device is switched on, every attempt should be made to keep it on for as long possible. The investigator should consider including chargers for a variety of devices in the their kit to facilitate this. Also, if at all possible, the investigator should attempt to keep the screen unlocked, if the device was discovered in this mode (touch the screen at regular intervals). This will negate the need for a passcode to unlock the device.

The device should be placed in "aeroplane" mode in order to disable Wi-Fi, Bluetooth or other communication systems. If the mobile device is switched on but locked, plugging it in to a power source will (in most cases) force the device to synchronize with any cloud services running. This should maximize the amount of evidence potentially available in the cloud. However, capturing this evidence may pose some major challenges, as the target machine(s) may be cited outside of the concerned State's jurisdiction, or evidence itself could be easily changed or deleted.

In such cases, retrieval of the available evidence has a time-critical element and investigators may resort to screen captures, with time and date, of the relevant material or to obtaining a digital extraction of the entire content of particular Internet sites (commonly termed "ripping").

When accessing material on the Internet with a view to evidential preservation, investigators should take care to use anonymous systems. Failure to utilize appropriate systems could compromise current or future operations. Investigators should consult their force Computer Crime Unit if they wish to rip and preserve website content.[143]

4.5. Special investigative techniques and foreign terrorist fighters

Undercover operations online

Successful investigations against FTF increasingly rely on the use of human intelligence sources and the use of undercover law enforcement officers. The following definitions are worthy of consideration in relation to the use of undercover officers:

[143] Association of Chief Police Officers, Good Practice Guide, (see footnote 97).

Undercover activities means:

- Any investigative activity involving the use of an assumed name or cover identity.

Undercover operation means:

- An investigation involving a series of related undercover activities over a period of time by an undercover employee.[144]

Covert human intelligence source (CHIS)—A person can be considered as a CHIS if:

a) They establish or maintain a personal or other relationship with a person for the covert purpose of facilitating anything falling within paragraph b) or c);

b) They covertly use such a relationship to obtain information or to provide access to any information to another person; or

c) They covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.[145]

In circumstances where investigators wish to covertly communicate with an online suspect, the skills of a trained, authorized covert internet investigator (CII) are paramount. CIIs receive specialist training which addresses the technical and legal issues relating to undercover operations on the Internet. Such interactions with the suspect(s) may be in the form of email messaging, instant messaging, or through another online chat medium.[146]

Policies, procedures, and even legislation on the use of special investigative techniques differ from jurisdiction to jurisdiction, but there are a number of recommendations for consideration when officers undertake this course of action:

- Require investigators to submit a written request to the Chief of Police or nominated deputy, detailing the scope and purpose of any investigation necessitating the development of a fictitious online profile.
- Requests should include proposed usernames, email address, date of birth, and other information that will become part of the fictitious profile.
- Requests should include any photographs, video, or other media that will be associated with the fictitious profile. Special attention should be directed to the purpose and source of such media as well as to securing any necessary waivers or release documents.

[144] United States of America Office of the Attorney General, "Guidelines on Federal Bureau of Investigation Undercover Operations". Available from: https://fas.org/irp/agency/doj/fbi/fbiundercover. pdf.

[145] United Kingdom, Covert Human Intelligence Sources Code of Practice, 2010. Available from: www.gov.uk/government/uploads/system/uploads/attachment_data/file/384976/Covert_Human_Intelligence_web.pdf.

[146] Association of Chief Police Officers, Good Practice Guide, (see footnote 97).

- Establish an evaluative process for these requests at the command level. Every request should be analysed to determine the investigatory purpose and need for undercover investigation.
- Maintain a record of all submitted requests, both approved and disapproved, in the agency record management system.
- Establish protocols for which computer systems may be used for the development and management of fictitious profiles. Only systems with the requisite security features should be utilized in order to keep the fictitious profile from being traced back to the originating agency.
- Prohibit the use of personal, non-agency-established Internet accounts or ISP access when using fictitious profiles.
- Ensure investigators are trained on how to legally access social network user accounts by way of subpoena, warrant, or other court order. This includes instruction on pertinent parts of individual social network policies.
- Ensure investigators understand when and how to get a social networking account shut down and preserved for evidentiary purposes. Training should also include details on how to capture information, including metadata, and how to properly preserve the chain of custody.[147]
- The Chief of Police, or deputy, should establish protocols for documenting and recording investigations activity and communications.
- Ensure investigators are trained in how to set tone, pace, and subject matter of online conversations in addition to other entrapment considerations.

Regardless of which policy considerations are implemented, a social networking investigations policy and the use of fictitious profiles should generally mirror those relating to conventional undercover investigations.[148]

4.6. Financial components of foreign terrorist fighter investigations

The act of travelling to and from a conflict zone and participating in terrorist activities while there intrinsically requires a level of logistical planning. Whether it is a simple case of an individual purchasing a flight ticket to travel, buying specialist clothing and equipment for use when in the conflict zone, or a wider network of individuals recruiting, training and facilitating these activities, financial transactions are required to be conducted to commit an FTF offence. Such transactions which wilfully provide material support to the traveller may constitute a terrorism financing offence.[149]

[147] Metadata describes how and when and by whom a particular set of data was collected, and how the data are formatted.

[148] Michael D. Silva, "Undercover Online: Why Your Agency Needs a Social Network Investigations Policy", *The Police Chief*, May 2013. Available from: www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2923&issue_id=52013.

[149] See www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2178%20(2014).

Using financial information for the furtherance of an FTF investigation is an incredibly powerful tool. Financial information can aid in determining an individual or group's logistical capabilities, may uncover a network of collaborators, and can reveal information about the suspects that otherwise would not have been found. This information is available to law enforcement through several investigative techniques, some of which are described below. It provides a powerful tool to identify any vulnerabilities that allow for arrest and prosecution for a terrorism-related offence or for identifying any disruption opportunities that may exist. The financial infrastructure of the FTF is particularly vulnerable because of the wide range of potential disruption tools which can be brought to bear against them. These tools are owned by different government agencies, the private sector and civil society (non-governmental organizations, charities, etc.). They are discussed in the Financial Disruption Workbook of the UNODC, and may offer disruption planners both individual and multiple integrated options for delivering effects against the critical vulnerabilities in the FTF's financial infrastructure.

The Workbook provides several options that should be considered (which to use to disrupt a financial structure, which are applicable to FTF financially related activities, including ways in which they can be employed concurrently and/or consecutively):

Law enforcement: summons, arrest, search of person/property/vehicle, multiple specimen charges, property/cash seizure, pretrial custody, restrictive bail conditions, conviction, imprisonment, restrictive orders, passport seizure, visa refusal/cancellation, immigration bail, deportation, travel restrictions, cyberdisruptions (website block, shut down, redirect).

Information and media: key leader engagement, community outreach, social media, journalist briefing, local leafleting, radio, television, printed media. "Being first with the truth." (Note that wilful dissemination of false information to the public is not recommended in this methodology.)

Private sector/civil society partnerships: alerts to financial/private sector (including Designated Non-Financial Business or Profession or DNFBPs), private sector watch lists, ad hoc/regular briefing and training, religious rulings, community statements, create/support forums, chambers of commerce, community focus groups.

Economic: regulator intervention (not-for-profit, financial, company registration), asset freeze, financial reporting orders (internally or by external auditor), tax investigation, fines/penalties for administrative offences, unilateral de-risking/closing accounts by financial institutions, denial of insurance.

Diplomatic and international: UNSCR and national-level sanctions listing (UNSCR 1988 / 1989), supply intelligence cases to other countries for national sanctions listing, United Nations-brokered resolutions (Security Council, General Assembly, Commissions, INTERPOL Notices).

Security agencies and military: support to law enforcement officers conducting high threat/hostile environment operations, search and detention, lethal/non-lethal

military options, show of force, electronic warfare, cybereffects, surveillance, interception of communications.[150]

The recommendations of the Financial Action Task Force require that financial institutions and other designated non-financial businesses and professions keep records of transactions and clients conducting transactions and make a disclosure to the relevant authorities if the transaction or activity is considered suspicious or unusual.[151] Such financial information is initially received by the national financial intelligence unit (FIU) and then distributed to the investigation team, which may also allow investigators to collect enough evidence to apply an additional charge for the financing of terrorism for the wilful material support provided to the traveller.

There are two primary ways in which a financing of terrorism investigation can be initiated in the case of FTF. First, it can be initiated by prosecutors or law enforcement. In this instance, a parallel financial investigation into the offence of travelling to participate in a foreign conflict is initiated by an investigation team. The investigation team will be required to set up a parallel investigation to investigate the financing of the activities and to ensure for financial information and intelligence to be considered within the main investigation. It is recommended that a parallel terrorism financing investigation is opened in the pre-arrest phase, where risk of investigation disclosure is low and to maximize the value of financial information. Second, it can be initiated by an FIU. In this instance, assistance from the FIU is provided proactively to investigators. Investigators are then required to determine whether the intelligence is credible enough for the creation of a formal investigation.

4.6.1. Managing the parallel terrorism financing investigation

The primary objective of any terrorist financing investigation is to identify the methods the terrorists use to raise, store, move, and use their finances. Managing parallel terrorism financing investigations can be incredibly complex and require a defined approach to be executed in a coherent and efficient manner. For this reason, it recommended that the financial investigator(s) is involved from the outset of any investigation, that they are regularly and thoroughly briefed, and they understand both the strategy and tactics of the investigation. The investigation is broken into six key strategic steps:

1. Understanding the FTF investigation;
2. Assembling a team capable of understanding and managing the parallel terrorism financing investigation;
3. Identifying persons, assets and entities involved in the investigation, creating a profile for each and networking the individuals/assets/entities;
4. Obtaining domestic and international information and evidence on the persons, assets and entities involved in the investigation;

[150] UNODC, *Financial Disruption Workbook*, p. 28.

[151] See www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate).

5. Analysing the financial information and evidence;
6. Next steps for parallel financing of terrorism investigation.

Understanding the foreign terrorist fighter investigation

What is alleged to have occurred in the FTF case is paramount to operationalizing the parallel investigation. The FTF case will dictate the potential for terrorism financing charges, define the individuals/assets/entities involved and provide leads to acquire financial information. Understanding the case at hand will also allow for the proper assembling of an investigative team, and determine whether sufficient evidence is suspected to exist for a terrorism financing charge.

Such understanding can be framed in the classical investigative process of who, when, what, where and how to fully comprehend the scope of a potential parallel financing of terrorism investigation:

- **Who**—who is the alleged FTF, and who is allegedly providing material support to their activities?
- **When**—when did the financing occur?
- **What**—what financing or material support was provided?
- **Where**—where did these transactions or provisions of support take place?
- **How**—how did the transactions or provisions of material support take place?

4.6.2. Assembling an investigative team

The financial component of FTF investigations can be either simple, with self-funded or direct funding of operations, or very complex, involving opaque corporate vehicles, offshore centres and other financial machinations to blur the line of funding. The parallel investigation team needs to reflect the needs of the case and may include diverse skill sets, including the ability to:

- Understand financial documents, including bank statements, transaction records, contracts, real estate deals, etc.;
- Understand complex corporate structures and finding beneficial ownership of entities and assets;
- Coordinate diverse human and investigative resources, both domestically and internationally;
- Analyse, assess and organize significant information in a logical manner.

The parallel terrorism financing investigation team should include financial investigators, prosecutors, law enforcement, and potentially other specialized individuals, including financial analysts and forensic accountants. Individuals may be seconded from other domestic agencies including the FIU and tax authorities. Where particular skills could not be procured, outside expertise should be identified prior to formally beginning the case.

Normally, such an investigation is led by a senior prosecutor who can inform and manage relations with the judiciary if special investigative techniques are to be used. Law enforcement or prosecutorial agencies are tasked with acquiring information, intelligence and evidence to forward the case.

Upon formation of the parallel investigative team, the leader of the investigation should address strategic level considerations including:

- The level of secrecy of the investigation, potential for enhanced security clearances and secure channels for information exchange;
- The ability of required domestic and international partners to share information;
- Challenges of potentially prosecuting in absentia;
- The timing of the alleged financing and travelling, and how the timing affects the ability to apply charges, for example if the individual travelled to commit terrorist acts prior to travelling for terrorist acts being criminalized in the jurisdiction.

Identifying individuals, assets and entities involved in investigation

Financial investigation can become onerous in that financial records are numerous, complex and dense. It is recommended that subject profiles are created on each individual involved in the case, and other individuals of interest. Initial information will be populated from the FTF investigation, and means described in later sections will identify methods to acquire further required information. These profiles will need to be kept constantly updated and will be the "one stop shop" for all relevant information on that individual for the financial investigation.

Each individual's profile should include:

- Name, aliases and a recent photograph;
- Subject's identifying information (height, weight etc.);
- Copies of subject's identifying documents (birth certificate, passport etc.);
- Listing of subject's personal network (family members, business associates, other close associates etc.);
- Open source and title information;
- Listing of assets owned, including loan applications and agreements;
- Bank accounts with estimated holdings;
- Business, tax, asset and salary records;
- Identifying and acquiring financial data and other evidence.

To comprehend the potentially many connections between individuals involved in the investigation, it is recommended that a pictorial network chart be created to establish links among the individuals. As with the subject profiles, such a chart would require constant upkeep to maximize utility.

4.6.3. Obtaining domestic and international information and evidence

As described above, the purpose of the parallel investigation is twofold: first, to determine whether there is adequate evidence to support a financing of terrorism charge, and second, to utilize financial information to support the FTF investigation. To do so, investigators must identify the events that make up the offence of travelling for the purposes of terrorism, such as purchasing travel tickets, and acquire information, and eventually evidence, to demonstrate how these events were financed.

Securing such information and evidence can be complex given that numerous investigative techniques may be required to acquire all relevant information. Section 4.6 provides a number of investigative techniques investigators can use to acquire such information and evidence.

4.6.4. Obtaining domestic information and evidence and searching publicly available information

In the modern world, subjects normally leave a significant online footprint which is available through various search engines and social media platforms. Social media platforms are a particularly rich area to exploit when researching the financing of FTF as many travellers will have responded to online propaganda. A response to such propaganda may be accompanied by funding for travel facilitation, defined instructions for managing finances, or information on how to access funding inside of war zones. Such information may also be useful in providing the geographical location of subjects.

Open source information may also provide information on the subject's family, friends and other associates, who may be valuable in uncovering potential financial facilitation for training and travelling.

4.6.5. Acquiring information from government databases

Government databases can be a rich source of information as they may identify how an individual has paid for services such as licensing or utilities, as well as establish a view of the subject's wealth from tax authorities or auditing agencies, among other things. It is recommended that inquiries be made with the following government authorities for subject information:

- Border crossing, customs and immigration authorities;
- Providers of utilities (electricity, natural gas etc.);
- Licensing authorities (automobile etc.);
- Real estate and vehicle registries;
- Tax and auditing authorities;
- Corporate registries.

Access to information varies significantly across jurisdictions and agencies. Direct contact with an agency may be required to facilitate such information sharing requests.

4.6.6. Access to financial intelligence unit intelligence

The FIU is a very important tool in acquiring financial information given its mandate in collecting, analysing and disseminating financial intelligence. FIUs are provided with transaction reports from the private sector, including banks and remittance services, when the private sector institution has reasonable grounds to suspect that the transaction was related to the commission of a terrorism financing offence. Depending on the jurisdiction, they may also receive other reports proactively, including cash transactions at a particular threshold, international wire transfers and cross-border cash declarations.

FIUs may have the power to request further financial information from the private sector. The FIU would analyse this financial information and provide a package of financial intelligence on the subject and their associates if a legal threshold has been met.

FIUs have operational independence and their potential support in the parallel terrorism financing investigation can also be initiated through the provision of voluntary information on the investigation. Such voluntary information may include a case synopsis, subjects involved (with full subject profile) and any financial information already collected. The domestic FIU may be an administrative unit, which means that it sits outside of the law enforcement structure of the country, or it may be a police FIU, and is a division of the law enforcement structure. Depending on the type FIU, there may be specific protocol to follow when sharing voluntary information with the unit.

4.6.7. Physical surveillance

The surreptitious monitoring of an individual or pre-arrest collection of information can be a delicate and costly endeavour. Such surveillance must be, at minimum, coordinated through the FTF investigation, or run entirely through their human resources conducting physical surveillance. It is important that this surveillance captures information that could be relevant to a potential terrorism financing charge, specifically any information that would link the individual to a financial transaction or asset, including:

- Financial institutions and financial gatekeepers (e.g. lawyers) visited;
- Visits to travel agencies;
- Appearance in automobiles or on specific premises real properties;
- Interaction with potential financial supporters.

These leads to financial transactions and assets would allow investigators to uncover further information about how they were conducted or acquired.

4.6.8. Refuse searches

A refuse search allows investigators to sift through an individual's trash, where there is no expectation of privacy of its contents. Investigators must first determine whether or not such a search is permissible under local laws.

A refuse search can uncover important information such as banking and credit card statements, correspondence with facilitators, IOUs, bills or receipts. Refuse searches should be conducted regularly and on all subjects that may have been involved in financing the FTF.

4.6.9. Mail searches

A mail search allows investigators to view the covering of mail addressed to the investigation's subjects, where there would be no reasonable expectation of privacy for the mail. Investigators must first determine whether or not such a search is permissible under local laws.

A mail search can uncover important information such as the financial institutions or other services utilized by the subjects. Mail searches should be conducted regularly and on all subjects that may have been involved in financing the FTF.

4.6.10. Interviews

Interviews should be conducted with those individuals who may be able to provide further information on potential financing. Interviews are a more obtrusive technique than the previous techniques described and will, more than likely, result in the subject becoming aware of the investigation when they are conducted. For this reason, interviews should only be conducted either post-arrest, or when an appropriate risk of disclosure to the subject versus benefit of conducting the interview is reached.

Interviews should also only be conducted when other less obtrusive methods have already been employed so that interviewers are more prepared to ask about potential financing details, and have the interviewee corroborate or clarify the contents of documents and information already acquired. Investigators must be aware of and adhere to domestic legal rules of interviews prior to commencing.

4.6.11. Search/seizure orders

Search and seizure warrants of dwellings or businesses provide an excellent means to acquire financial information about investigative subjects. Generally, to obtain a search/seizure order, an investigator must create a written application containing a warrant and an affidavit. The warrant must clearly indicate the parameters of the search, such as where the search will be conducted, at what time and who will be conducting the search. The affidavit must provide reasonable grounds to believe that a financing of terrorism offence has been committed, and that items connected to the crime are likely to be found at the location of the search.

In executing search/seizure orders, the investigative team should ensure that a team of search/seizure professionals and financial investigations professionals comprise their search/seizure team. Financial professionals are required to identify financial information of relevance to the case for appropriate seizure.

4.6.12. Production orders

Investigations into the financing of FTF may require production orders, which compel a legal entity to disclose particular information to the investigative team. These orders are served on businesses that are unwittingly used as conduits for terrorism financing, such as financial institutions and Internet services, such as ISPs, email service providers, message board providers and social media companies such as Twitter, Facebook and YouTube.

Production orders are obtained in a similar manner to search/seizure orders described above. The production order must provide a listing of required information and should be written in such a manner as to allow the investigative team to acquire all relevant information to the offence from the legal entity. Relevant information can include account opening information, transaction records and client profile information. The entity providing the information should be treated as a partner in the investigation, and information representing undue burden should not be requested when not necessary.

4.6.13. Obtaining international information and evidence

Obtaining international information and evidence may be a key part of a financing of terrorism charge when suspected financing is coming from outside of the country, or was financed in another country. There are three main avenues for such international assistance:

- Foreign FIUs;
- Informal assistance;
- MLA.

As international cooperation can take longer than domestic requests for information, it is important that investigators ask for assistance as soon as it is required so that delays have minimal impact on the investigation.

4.6.14. Foreign financial intelligence unit information

A domestic FIU will be able to request financial intelligence from foreign FIUs, which will have substantially similar access to information as the domestic FIU. Such financial intelligence is generally transmitted on a legal threshold of "reasonable grounds to suspect" that the information would be relevant to a terrorism financing investigation, and providing the foreign FIU with sufficient information to meet this legal threshold is paramount to expediting the request for information.

The Egmont Group of Financial Intelligence Units provides its members with a secure channel, the Egmont Secure Web, to transmit such information between FIUs.

4.6.15. Informal assistance

Developing and keeping international contacts in your industry is critical to the success of both informal assistance, as well as MLA. These personal relationships will allow

requests to be correctly directed, executed more quickly, and with greater success. These personal relationships will also open the door to contacts' personal relationships in the foreign country working at other agencies.

Informal assistance with personal contacts is important to develop an operational plan with foreign counterparts, and they may be able to provide information where MLA is not required, such as surveillance reports, open source information, as well as the potential opening of a joint investigation. Generally information gathered through informal assistance is not admissible to court, and merely forms investigative leads.

4.6.16. Mutual legal assistance

MLA is the process by which a jurisdiction asks for assistance from another jurisdiction in gathering information relevant for an investigation, prosecution and adjudication of criminal cases. For the purpose of a terrorism financing case, MLA may be sought to obtain certified documents and sworn testimony, or have search/seizure and production orders executed in a foreign jurisdiction. It is important that informal assistance, described above, is used throughout the MLA request to ensure that proper information is sought, and it is provided in a timely manner.

MLA availability and processes differ significantly across jurisdictions, so investigators must become familiar with the unique procedures and conditions set out in the bilateral and multilateral treaties which allow for MLA. The procedures of MLA can be complex, and it is recommended that international best practices be observed to ensure proper assistance.[152]

4.6.17. Analysing the financial information and evidence

Financial analysis for terrorism financing cases is generally less complex than money-laundering or other financial crimes, and usually does not require advanced financial analysis techniques. Terrorism financing investigations for FTF require that the investigators work backwards from events related to the individuals' travelling and training activities that make up the offence of travelling to participate in conflict in a foreign country. The events could include the purchase of flight tickets, purchase of equipment or the provision training. Investigators must follow the money and determine how the events that constitute the FTF offence were paid for. To do so, a variety of techniques described above can be utilized to secure information, intelligence and evidence that demonstrates the funding sources for these events.

[152] See UNODC *Manual on International Cooperation in Criminal Matters related to Terrorism*, and UNODC *Counter-Terrorism Legal Training Curriculum* Module 3: International Cooperation in Criminal Matters, available at http://www.unodc.org/unodc/en/terrorism/technical-assistance-tools.html#Practical_guides and the UNODC e-book to aid in conducting MLA requests, available at www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf.

4.6.18. Next steps for parallel financing of terrorism investigations

Investigators must consider the evidence that has been gathered by the investigative team after it has exhausted all potential for further information. If sufficient evidence has been collected to support a financing of terrorism charge, then the parallel financing of terrorism investigative team should build a case to go to court with the charges of travelling to fight in a foreign conflict.

If insufficient evidence has been collected, then the information and evidence should be transferred to the investigative team charged with developing the case for travelling to fight in a foreign conflict. This information can help build a potential terrorist network and demonstrate the planning surrounding the alleged offence. The process of information sharing between investigative teams should be ongoing throughout the course of the parallel financing of terrorism investigation.

4.6.19. Case study—parallel terrorism financing investigation

An investigation into a potential FTF was opened by the prosecutor's office in Country A as there were reasonable grounds to suspect that a citizen of Country A had, two days prior, travelled to Syria to participate in a foreign conflict that constituted the participation in terrorist acts. At the onset of the investigation, a parallel terrorism financing investigation was opened by the prosecutor's office to determine whether there was financial support to the traveller that would constitute terrorism financing. The parallel financial investigation was led by the prosecutor's office and comprised financial professionals from competent law enforcement bodies, the State FIU, the secret service and a financial analyst.

The parallel financial investigation team first acquired the required knowledge of the potential offence through consultation with the FTF investigation, and, second, created an investigative plan for the terrorism financing investigation. As it was unconfirmed whether the individual had travelled to Syria to participate in terrorist acts, the investigative plan focused first on covert methods to investigate the potential terrorist financing offence.

Method used—searching publically available information

Investigators searched publically available information for the potential traveller and did not find any financial information that could be relevant to the case. They did, however, find that the potential traveller had a significant public social media presence. Investigators were able to identify individuals with close personal ties to the potential traveller through this presence.

Method used—financial intelligence unit

Investigators shared available relevant information with the FIU, which used the information to query their financial transaction databases. The potential traveller did not have any suspicious transaction reports filed on them.

The FTF investigation uncovered that the individual had indeed travelled to Syria and intended to commit terrorist acts, and now focused on acquiring details of the traveller's activities in Syria. With confirmation that the individual had travelled to Syria, the FTF investigation now moved to more overt techniques.

Method used—interviews

Interviews were conducted of individuals that were identified as being close associates with the traveller through social media. One individual indicated that the traveller frequented Bank A to conduct financial transactions.

Method used—financial intelligence unit

The bank name of the traveller was provided to the FIU. The FIU requested account information concerning the traveller from Bank A. The FIU conducted an analysis of the transactions conducted through the account of the traveller and determined that the traveller had received two wire transfers from an individual in Country B which indicated that they were "gifts", and that the traveller had used these funds to purchase a flight ticket to travel to Syria.

At this point in time, the FTF investigation uncovered credible evidence to suggest that the traveller was indeed participating in acts of terrorism in Syria.

Method used—informal cooperation

The prosecutor in charge of the parallel financial investigation contacted a colleague in Country B who he had met and worked with on numerous occasions through the Prosecutor's Network. He indicated that there was an investigation into potential terrorism financing and provided what information he could on an informal basis. An investigation was opened in Country B for the financing of terrorism.

Method used—production order and mutual legal assistance

The investigation team utilized a production order to obtain records from Bank A showing the wire transfer that was sent from Country B to purchase the flight ticket used by the suspect to travel to Syria to conduct terrorist activities. The investigation team also used MLA to acquire the evidence gathered by the investigation team in Country B which demonstrated that the sender of the wire transfers intended to facilitate the traveller's purchase of an flight ticket to travel to Syria and commit terrorist acts.

With the evidence acquired, the investigation team charged the sender of the wire transfers in Country B with a financing of terrorism offence.

Annexes

1. List of international legal instruments related to terrorism and foreign terrorist fighters

United Nations

Convention for the Suppression of Unlawful Seizure of Aircraft, signed at The Hague on 16 December 1970

Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, concluded at Montreal on 23 September 1971

Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, adopted in New York on 14 December 1973

International Convention Against the Taking of Hostages, adopted in New York on 17 December 1979

Convention on the Physical Protection of Nuclear Material, adopted in Vienna on 3 March 1980

Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, done at Montreal on 24 February 1988

Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, done at Rome on 10 March 1988

Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, done at Rome on 10 March 1988

International Convention for the Suppression of Terrorist Bombings, adopted in New York on 15 December 1997

International Convention for the Suppression of the Financing of Terrorism, adopted in New York on 9 December 1999

International Convention for the Suppression of Acts of Nuclear Terrorism, adopted in New York on 13 April 2005

Security Council resolution 2170 of 15 August 2014

Security Council resolution 2178 of 24 September 2014

Council of Europe

European Convention on the Suppression of Terrorism, ETS No. 090, 1977

Council of Europe Convention on the Prevention of Terrorism, CETS No. 196, 2005

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, CETS No. 198, 2005

Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, CETS No. 217, 215

2. Basic tips for investigators and prosecutors for requesting electronic/digital data/evidence from foreign jurisdictions

Global Programme for Strengthening the Capacities of Member States to Prevent and Combat Serious and Organized Crime (GPTOC—GLOT32)

.....

Basic tips for investigators and prosecutors for requesting electronic/digital data/evidence from foreign jurisdictions.[153]

- Prior to sending any request to a foreign country, make sure you have exhausted all internal/national sources of obtaining the required electronic data/evidence. Note that this data/evidence can be obtained, among other things, from open sources (i.e. publicly available information) and/or directly from Internet Service Providers (ISPs)[154] established/registered in your country as affiliate companies of foreign-based ISPs.
- Consider the gravity of the offence when request assistance as some countries will not execute foreign requests with regard to minor cases due to the certain limitations established by laws or practices (e. g. the U.S. will generally decline to execute any request involving less than to USD 5,000 in damages).
- Take steps to preserve electronic/digital data/evidence prior to sending the request for its disclosure as, unlike traditional evidence, various types of

[153] Tips were provided by participants of the Second Inter-regional Meeting on Sharing Practices in Requesting and Providing Digital Evidence in Organized Crime Investigations and Prosecutions, held in Tbilisi on 9-11 December 2014 in the framework of the UNODC "CASC" initiative *Establishing/Reinforcing the Network of Prosecutors and Central Authorities from Source, Transit and Destination Countries in response to Transnational Organized Crime in Central Asia and Southern Caucasus.*

[154] An internet service provider is an organization that provides capacity for accessing and using the Internet—including social networking services—creating a platform for accessing, using, or participating in the Internet. For example, Facebook, Google+, LinkedIn, Instagram and Twitter (USA); Vkontakte (Russia), Delphi, Draugiem.lv (Latvia), Hyves (The Netherlands) http://en.wikipedia.org/wiki/Internet_service_provider, http://en.wikipedia.org/wiki/Social_networking_service.

electronic/digital data/evidence[155] can be deleted permanently in a short time. For example, currently, laws of the U.S. and the majority of countries of Western Europe do not require Internet Service Providers (ISPs) to retain data for a certain time. Once deleted, data generally cannot be retrieved from an ISP. If your country and a requested country are members of the 24/7 Network (set up in accordance with article 35 of the Budapest Convention),[156] send the request for data preservation via your country official contact of the 24/7 Network. If your country is not a member of the 24/7 Network, send a request to a relevant investigative/prosecutorial body of the requested country. Consult with contacts of the CASC network and/or foreign liaison law enforcement officers located in your country regarding the entity to which the request should be sent, the procedure/channels (i.e. informal "Police to Police" or formal Mutual Legal Assistance channel), and the content of the request. Be ready to provide (i) very basic facts of the investigation, (ii) a precise description of the data to be preserved (i.e. specific account/IP address/website, all associated dates and times including time zones used, etc.), (iii) an explanation as to why/how the evidence sought (data to be preserved) is relevant to the investigation, and (iv) a statement that a MLA request for the data disclosure will be sent after the data is preserved.

- Given that some ISPs can accept requests for data preservation directly from foreign law enforcement/prosecutorial authorities, verify directly with the ISP in question and with the above contacts whether it is possible, and if so, send the request directly to the ISP and send a copy of the request to the above investigative/prosecutorial body of the requested country. Note that some ISPs are not "law enforcement friendly." Therefore, consult with the authorities of the requested country before sending a request directly to an unknown ISP.
- Verify with the requested authority whether an account holder may learn about the preservation request (either because of the ISP's technical design built into their servers or because the ISP notifies clients), and consider your investigative strategy accordingly.
- Consult with your cybercrime unit about the technical aspects of the request.
- Following data preservation, prepare your MLA request promptly. When/if available, study/use checklists/guidance for obtaining MLA drafted by the requested country.[157]
- Consult with the requested authority/authorities about the possibility of initiating/opening their own criminal investigation. Some countries won't be able to satisfy your MLA request with regard to certain types of assistance if they do not open their own investigations. For example, "…currently, U.S. law does not

[155] In particular, stored computer data e.g. transmission logs, subscriber information, contents of emails, and information on websites.

[156] The Council of Europe Convention on Cybercrime, 2001.

[157] E.g. Requesting Mutual Legal Assistance in Criminal Matters from G20 Countries: A Step-by-Step Guide, 2012; Requests for Mutual Legal Assistance in Criminal Matters: Guidelines for Authorities outside of the United Kingdom, 2012.

permit real-time interception of the content of telecommunications or computer messages pursuant to a request for assistance concerning a purely foreign offense. Interception of communications is available only in the context of a U.S. investigation… If U.S. and foreign authorities are investigating the same matter, it may be possible that U.S. authorities can share communications intercepted in their own investigation with foreign authorities."[158]

- The content of your MLA request depends on the types of assistance sought (i.e. electronic evidence requested), and the coercive measures needed to be taken in the requested country. Legal requirements for satisfying foreign requests for obtaining electronic evidence vary in different countries. Generally, the more intrusive the coercive measures, the more evidence you will need to satisfy a foreign MLA request. For example, if you need to obtain the content (e.g., email messages) in an email account, you would, as a general rule, have to provide more evidence to satisfy your MLA request than you would if you only needed to obtain subscriber information.[159] Consult with the requested authority about the justification/grounds for your request and the circumstances under which you can obtain data/evidence (including when you request data/evidence in emergency situations).
- Indicate the need for confidentiality.
- Explain the need for urgency if you ask for an urgent execution of your request.
- Explain whether the evidence needs to be certified to make it admissible in your court, and, if so, how it needs to be certified.
- Ensure the quality of the translation of your request.
- Maintain communication with your counterpart(s) in the requested country while your request is being executed.
- Provide contact details—for both informal and formal communication—in your request.
- Be specific and proportionate. Ask only for what is really needed.
- Send/discuss a draft request before sending it via official channels.
- Ask for confirmation of the receipt of your request.
- Don't leave your request unanswered—follow-up and check with the requested authority the reasons for not responding to you.

[158] Brief Guide to Obtaining Mutual Legal Assistance in Criminal Matters from the United States (as of 25 May 2012), Section IV, Paragraph G.

[159] Investigative Guide for Obtaining Electronic Evidence from the United States (as of 25 May 2012) contains description of various types of stored and real-time subscriber, transactional and content information available from ISPs.

UNODC

United Nations Office on Drugs and Crime

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

V.17-04090