UNODC
United Nations Office on Drugs and Crime

Foreign Terrorist Fighters

Manual for Judicial Training Institutes Middle East and North Africa

UNITED NATIONS OFFICE ON DRUGS AND CRIME
Vienna

Foreign Terrorist Fighters

Manual for Judicial Training Institutes Middle East and North Africa

First Edition
2021

UNITED NATIONS
Vienna, 2021

This handbook is a technical tool that has been developed for training purposes to support crime prevention and criminal justice practitioners in the Middle East and North Africa. (MENA).

Contents

Abbreviations

API	Advance Passenger Information Systems
AQI	Al-Qaida in Iraq
CDCT	The Council of Europe Committee on Counter-Terrorism
CGN	Carrier-Grade Network Address Translation
CHIS	Covert Human Intelligence Source
CII	Covert Internet Investigator
CODEXTER	The Committee of Experts on Terrorism
CSV	Comma Separated Value
CTC	United Nations Security Council Counter-Terrorism Committee
CTED	United Nations Security Council Counter-Terrorism Executive Directorate
DHCP	Dynamic Host Configuration Protocol
DNA	Deoxyribonucleic Acid
ESI	Electronically Stored Information
EUCTS	European Union Counter-Terrorism Strategy
EU-RAN	European Union Radicalisation Awareness Network
EXIF	Exchangeable Image File Format
FTF	Foreign Terrorist Fighters
FTP	File Transfer Protocol
GCTF	Global Counter-Terrorism Forum
GIMF	Global Islamic Media Front
GPS	Global Positioning System
HTML	Hypertext Markup Language
HTS	Hayat Tahrir al-Sham
HTTP	Hypertext Transfer Protocol
IACOmmHR	Inter-American Commission on Human Rights
IACP	International Association of Chiefs of Police
IAEA	International Atomic Energy Agency
IANA	International Assigned Number Authority
IAP	International Association of Prosecutors
IED	Improvised Explosive Device
IIJ	International Institute for Justice and the Rule of Law

IP	Internet Protocol
ISIL	Islamic State in Iraq and the Levant- Da'esh
ISP	Internet Service Provider
LAS	League of Arab States
MENA	Middle East and North Africa
MILF	Moro Islamic Liberation Front
MLA	Mutual Legal Assistance
OIC	Organization of Islamic Cooperation
OCTA	Organized Crime Threat Assessment
OS	Operating system
OSINT	Open Source Intelligence
P2P	Peer-to-Peer
PNR	Passenger Name Record
RAM	Random Access Memory
SDF	Syrian Democratic Forces
SIM	Subscriber Identity Module
SNA	Social Network Analysis
TCP	Transmission Control Protocol
TOR	The Onion Router
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
UNSC	United Nations Security Council
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network

Acknowledgements

The preparation of this handbook was made possible by the cooperative efforts and invaluable contributions of several individuals, Governments and international organizations.

The United Nations Office on Drugs and Crime (UNODC) wishes to extend its gratitude to the Member States who contributed to the consultation process related to the update of this handbook.

UNODC is grateful to the participants and experts from Member States in the Middle East and North Africa and beyond, for their invaluable inputs and discussions during 2019 and 2020, which have been considered to update and better tailor the content of this handbook to the current situation.

The production of this handbook was guided by Fernanda Lombardi and Ali Younes and reviewed by Carine Giraldou and Marco Venier. This handbook written and updated by Ahmed Genidy, using as a basis the first edition of "Foreign Terrorist Fighters manual for Judicial training Institutes South-Eastern Europe" and the contributions from consultations, meetings and workshops held since 2019.

UNODC wishes to express its gratitude for the support provided by the European Union towards the development of the handbook.

Introduction

This edition of UNODC's "Foreign Terrorist Fighters. Manual for Judicial Training Institutes, Middle East and North Africa" builds upon the "Foreign Terrorist Fighters. Manual for Judicial Training Institutes, South-Eastern Europe" publication, which was issued in 2017 and updated in 2019. This edition aims to present cases and provide information relevant to MENA criminal justice and law enforcement practitioners working on FTF-related issues.

Chapter 1 is expanded to elaborate on the FTF phenomenon and its evolution at the global and regional levels. It includes a section covering developments in the MENA region and sub-chapters on general FTF-related trends, which largely draw upon UNODC's earlier publications, such as "Investigation, Prosecution and Adjudication of Foreign Terrorist Cases for SEE" (2018). Chapter 2 includes details of global and regional legal documents on countering and preventing terrorism with a focus on FTF-related aspects. For example, this chapter features the United Nations Security Council Resolutions 2178 (2014) and 2396 (2017), which address the risks posed by FTF, including those seeking to return to their country of origin or to relocate to other countries. The updated Chapter 3 responds to the requests from the crime prevention and criminal justice practitioners to equip them with the updated information and tools on online investigations in terrorism cases. It provides examples of online search tools that are available to investigators for open-source intelligence gathering (OSINT).

"Foreign Terrorist Fighters. Manual for Judicial Training Institutes, Middle East and North Africa" aims to be utilized by judges and prosecutors and incorporated into existing training courses delivered by national training institutes in the region. This handbook is a technical tool that has been developed for training purposes to support crime prevention and criminal justice practitioners in the MENA. This edition is funded by the European Commission's Directorate-General for Neighbourhood and Enlargement Negotiations (DG NEAR).

Chapter 1

The foreign terrorist fighter phenomenon

1.1 Scope of the term "foreign terrorist fighter"

The concept of "foreign fighters" is not a modern invention. Fighters from abroad have participated in nearly 100 civil wars over the past 250 years.[1] The Spanish Civil War (1936-1939), which saw 50,000 volunteers from more than 50 countries, representing both sides of the conflict, is a prime example.[2]

The term "foreign fighter" was officially first used in reference to fighters travelling from outside the conflict zone to fight for Al-Qaida in Afghanistan. Later on, the term "foreign fighter" was employed in the context of the terrorist-led insurgency that started in Iraq in 2003. In the absence of a legal definition, commentators provided different meanings for the term.

One of the most widely accepted definitions was put forth by the Geneva Academy of International Humanitarian Law and Human Rights:

"A foreign fighter is 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".[3]

The phenomenon of terrorists travelling internationally to commit attacks, while not new, has gained traction since global travel became easier in the twentieth century. The first notable appearance of the term "foreign terrorist fighters", or "FTF", traces back to United Nations Security Council resolution 2170 (2014). The resolution was adopted in August 2014 in response to the then-escalating crises in Iraq and the Syrian Arab Republic. Condemning the terrorist acts undertaken in these territories and the resulting deaths of civilians, the Security Council called upon Member States to "suppress the flow of foreign terrorist fighters" to violent extremist groups vis-à-vis the two countries.[4]

A month later, on 24 September 2014, United Nations Security Council resolution 2178 (2014) was adopted to specifically tackle "the acute and growing threat posed by foreign terrorist fighters." The resolution emphasized the urgency of tackling the issue of FTF, in particular, those who have been

recruited by and have joined ISIL (Da'esh), the al-Nusrah Front and "derivatives" of Al-Qaida.[5] Resolution 2178 (2014) also provided a helpful definition of FTF:

---

5 United Nations Security Council Resolution 2178 (2014) S/RES/2178.

Foreign terrorist fighters are "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".[6]

In December 2017, the United Nations Security Council adopted resolution 2396 (2017) to reaffirm the definition of FTF and call upon Member States to tackle the threat posed by FTF returning or relocating from conflict zones.[7]

The definition adopted by the United Nations Security Council contains several elements, which should be highlighted. Firstly, the United Nations Security Council definition only applies to foreign fighters who travel for the purpose of "terrorist" activity. However, not all foreign fighters travel specifically for terrorist purposes. While these fighters may be guilty of a crime in their home state by virtue of privately engaging in an armed conflict in another country, they are not necessarily "terrorists" and, thus, cannot be treated as such.

Furthermore, the United Nations Security Council definition applies regardless of whether the FTF are engaged in an armed conflict. However, the International Committee of the Red Cross, for instance, has warned of the "potentially adverse effects" of conflating armed conflict with terrorism, and erroneously designating all non-State armed groups as terrorists.[8]

Finally, FTF also differ from mercenaries, who fight abroad on behalf of governments or privately financed entities[9] and are "motivated to take part in the hostilities essentially by the desire for private gain."[10] Nevertheless, where financial and political or ideological interests significantly overlap, such individuals may fall within the scope of the definition of FTF.

1.2 Typology and motivation

Who are foreign terrorist fighters?

A number of studies have been conducted into the backgrounds of the current wave of FTF. A common conclusion emerged that there was no standardized profile of FTF.

---

6 Ibid.

7 United Nations, "Security Council Urges Strengthening of Measures to Counter Threats Posed by Returning Foreign Terrorist Fighters, Adopting resolution 2396 (2017)", 21 December 2017, SC/13138.

8 International Committee of the Red Cross, "The applicability of IHL to terrorism and counterterrorism", 1 October 2015.

9 Charles Lister, "Returning Foreign Fighters: Criminalization or Reintegration?", Policy Briefing, Brookings Doha Center, August 2015.

10 Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts, adopted on 8 June 1977, 1125 UNTS 3, Art. 47. The use of mercenaries is covered by other international, regional, and domestic laws.

Rather, recruits were drawn from a diverse range of age, educational, vocational and socio-economic backgrounds. While the majority of recruits are males in the age range of 20-30, young teenagers and people of advanced age, close to and

over 60 years old have joined ISIL (Da'esh) as well.[11] A large percentage of FTF were young, economically disadvantaged males from socially or politically marginalized backgrounds.[12] There were many others with affluent backgrounds and well-educated. A report published by USAID suggests that "some are school dropouts, others have graduate qualifications … some FTF are itinerant workers, but others have successful professional careers as doctors, teachers, engineers and public servants."[13] Many FTF had troubled pasts, but others would have enjoyed great prospects had they not subscribed to terrorist causes. Not all FTF were pious either. While some had criminal records (often for petty crimes), a large percentage was previously unknown to law enforcement.

How are they recruited?

Community-based networks played an important role in motivating individuals to travel to the Syrian Arab Republic, with a large proportion influenced to leave by friends or relatives.[14] Religious leaders who subscribed to extremist ideologies were also responsible for radicalization and guiding individuals on a path to violent extremism. Furthermore, membership in non-violent radical groups and association played a role in influencing prospective fighters. The average recruitment age dropped with FTF recruited while still in school or college. Da'wah (religious outreach) groups at university campuses were cited as potential places for recruitment.

Some recruits may be former FTF or existing members of terror groups, but many have travelled without any prior contact with the terrorist organizations they seek to fight for. Others have been groomed and facilitated in their travels by recruiters working online, including by FTF who have already gone to the Syrian Arab Republic and subsequently encouraged their friends and acquaintances to do the same.

The January 2020 report from the European Union Radicalisation Awareness Network (EU-RAN) suggests that:

---

11 John Horgan and others, "A New Age of Terror? Older Fighters in the Caliphate", CTC Sentinel, vol. 10, No. 5 (May 2017), p. 13.

12 Hamed el-Said and Richard Barrett, "Enhancing the Understanding of the Foreign Terrorist Fighters Phenomenon in Syria", United Nations Office of Counter-Terrorism (July 2017).

13 Greg Fealy and John Funston, "Indonesian and Malaysian Support for The Islamic State", USAID Report, (6 January 2016).

14 el-Said and Barrett, "Enhancing the Understanding of the Foreign Terrorist Fighters Phenomenon in Syria" (see footnote 14).

"The Salafi-jihadi ideology and its interlocking narratives contribute to its popularity among youths. For some it provides a new identity for alienated individuals who discover (or rediscover) their religiosity, providing them with a sense of dignity and belonging. It is also attractive for many as the worldview of believers is binary and uncompromising, dividing everything into good and evil. For some it represents a protest ideology against the established order. For others it provides a utopia and promise of heavenly rewards in the afterlife. Whatever the underlying reasons for joining Salafi-jihadi groups, recruitment remains essential. There are multiple arenas that the Salafi-jihadi ecosystem exploit in their recruitment efforts to the cause. It is often a combination of making initial contact through online activity that is continued offline through social events, religious meetings or demonstrations".[15]

Advances in the means of communication over the Internet, through social networking sites and chat applications, have played a major role in assisting recruitment. Even when there is no online contact, the Internet enables potential recruits to view terrorist propaganda and discover terrorist narratives about the conflict, thus reinforcing decisions.[16] In a recent report by the United Nations Counter-Terrorism Executive Directorate (UN CTED) on the implementation of United Nations Security Council resolution 2178 (2014) in States affected by FTF, the UN CTED stated that the speed of transition

from initial interest to radicalization to commitment, to action, and ultimately to joining a foreign terrorist group has accelerated rapidly.[17]

Why do individuals become foreign terrorist fighters?

The motivations for joining terrorist organizations vary significantly. There is no unitary psychological profile. Studies on persons who have travelled to the Syrian Arab Republic have found several factors, political, religious, and personal, that account for the involvement with ISIL (Da'esh):

- Living in a caliphate: an FTF may possess a desire, coupled with a sense of duty, to live within a caliphate under the governance of sharia law in a manner that the FTF believes was ordained by the Prophet himself. The narrative of ISIL (Da'esh) involves labelling governments in Muslim countries as un-Islamic, whilst reinforcing the idea that Muslims should be living in a place where sharia is the supreme law guiding both political and

15 Radicalisation Awareness Network, "Islamist Extremism: A practical introduction" (Januray 2020).

16 el-Said and Barrett, "Enhancing the Understanding of the Foreign Terrorist Fighters Phenomenon in Syria" (see footnote 14).

17 United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), A compilation of three reports on "Implementation of Security Council resolution 2178 (2014) by States affected by foreign terrorist fighters" (S/2015/338; S/2015/683; S/2015/975).

social aspects of life. The caliphate is perceived as a utopian destination for the supposedly pious Muslim.

- A just war: especially in the early stages of the conflict in the Syrian Arab Republic, many FTF perceived their role as that of defending Islam and protecting followers of their own religion, all while fulfilling a religious requirement to undertake "hijra" and fight in a holy war. Some were genuinely driven by the humanitarian suffering of the Syrian people, reinforced by horrific images of the conflict and stories of government atrocities publicized in jihadist propaganda. It was only on arrival that many of these individuals fully adopted the jihadist doctrine and ideology.[18]

  The term "hijra", originally used to refer to the migration of the prophet Muhammad from Mecca to Medina, has been turned by both Al-Qaida and ISIL (Da'esh) into a rallying call to arms and construed as an obligation to migrate and undertake jihad in defence of Muslim lands.[19] Issue 3 of the ISIL (Da'esh) magazine Dabiq was titled "A call to Hijra". Containing articles such as "There is no life without jihad, and there is no jihad without hijra", followers were instructed to answer the call of their leader al-Baghdadi and move to the Khilafah [caliphate].[20]

- ISIL (Da'esh) success and legitimacy: the victories initially accomplished by ISIL (Da'esh) gave it an aura of power and invincibility. In defeating Syrian and Western-backed Iraqi forces and occupying large swathes of territory, ISIL (Da'esh) achieved more than any movement since the mujahideen war in Afghanistan. Control of territory enabled it to create the appearance of a credible functioning government, financed by oil revenues and other captured wealth. The symbolic power of this success was immense and interpreted by supporters as a sign of divine blessing, in affirmation of ISIL (Da'esh)'s path to creating a new world order.[21]

- Prophecies of the Final Battle: classical Islamic prophesies predict that Armageddon and Islam's final battle with its enemies will take place in the region of Sham (Greater Syria) and be led by the Mahdi (Muhammad's successor).[22] These prophecies became a fundamental part of the ideology of ISIL (Da'esh). According to ISIL (Da'esh) propaganda, the captured town of Dabiq was to be the scene of this final apocalyptic battle between Muslims

18 el-Said and Barrett, "Enhancing the Understanding of the Foreign Terrorist Fighters Phenomenon in Syria" (see footnote 14).

19 Rebecca Gould, "The Islamic State's Perversion of Hijra", *Project Syndicate*, 11 August 2015.

20 "A call to Hijrah", Dabiq, Issue 3, available at http://www.ieproject.org/projects/dabiq3.pdf.

21 Fealy and Funston, "Indonesian and Malaysian Support for The Islamic State" (see footnote 15).

22 Ibid.

and Christians. Many FTF viewed this as their chance to take part in the "battle to end all battles",[23] leading to the Day of Judgment and salvation for the righteous. Fighting is seen as a chance to atone for past sins and achieve martyrdom.

- Financial: ISIL (Da'esh)'s allure also extends to material benefits. Some defectors from ISIL (Da'esh) have mentioned promises of food, luxury goods and cars, and having their debts paid.[24]

While religion and ideology are typically treated as the main reason for enlisting, many FTF recruited in both Europe and Asia were also attracted by the "thrill factor" and excitement of fighting in a foreign conflict.[25]

A common motivation cited in interviews of FTF from Europe is one of feelings of exclusion and lack of belonging to their local communities, thus engendering "a feeling that by joining the fight in the Syrian Arab Republic they have nothing to lose and everything to gain".[26] ISIL (Da'esh) propaganda, by contrast, offered an attractive message of belonging, purpose, brotherhood, adventure and respect.[27] Stated another way, FTF could be categorized into four primary types[28]:

- "The Revenge Seeker": the frustrated and angry FTF seeks an outlet to discharge these emotions toward some person, group or entity whom he or she may see as being at fault.
- "The Status Seeker": this FTF seeks recognition and esteem from others.
- "The Identity Seeker": primarily driven by a need to belong and to be a part of something meaningful, this FTF defines his or her identity or sense of self through group affiliation.
- "The Thrill Seeker": the FTF is attracted to the group because of the prospects for excitement, adventure, and glory.

---

23 Thomas Koruth Samuel, "Radicalisation in Southeast Asia: A Selected Case Study of Daesh In Indonesia, Malaysia and the Philippines", Southeast Asia Regional Centre for Counter-Terrorism (2016).

24 "Victims, Perpetrators, Assets: The Narratives of Islamic State Defectors", International Centre for the Study of Radicalisation Report (18 September 2015).

25 Koruth Samuel, "Radicalisation in Southeast Asia: A Selected Case Study of Daesh In Indonesia, Malaysia and the Philippines", (see footnote 25).

26 Rik Coolsaet, "Facing the Fourth Foreign Fighters Wave: What Drives Europeans to Syria, and to Islamic State? Insights from the Belgian State", Royal Institute for International Relations Egmont Paper 81 (March 2016).

27 "Foreign Fighters: An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq", The Soufan Group (December 2015).

28 Randy Borum, "The Etymology of Radicalisation", in *The Handbook of the Criminology of Terrorism*, Gary LaFree and Joshua D. Freilich, eds. (Wiley-Blackwell, 2016).

The lack of any unitary profile poses a significant challenge for States attempting to identify potential FTF. Increasing numbers of women have also travelled, mainly in accompaniment of their husbands or to seek marriage with FTF and live under the caliphate.

Case study: Egypt

On 15 June 2013, then-President Mohamed Morsi gave a speech in Cairo Stadium, during which he encouraged supporting the Syrian people and fighting the Syrian Armed Forces. A group of approximately 60 males subsequently travelled from Egypt to Turkey, in small groups, and illegally entered Syria. They joined armed groups engaged against the Syrian armed forces, including Ahrar al-Sham Front and Victorious Sect (Jabhat Ahrar Alsham, Eltaifa Elmansoura). Less than a month later, in July, several of them returned to Egypt and formed a terrorist group under the leadership of Nabil Elmaghrabe, a known terrorist offended who had been a senior figure of the Al-Gama'a Al-Islamiya (GI). Elmaghrabe has also participated in the Afghan conflicts during the 1980s.

The group identified and monitored a number of targets, including embassies, Egypt's national Energy Centre, the subway command centre, the Ministry of Interior, the headquarters of the National Security Sector and the headquarters of the Military Intelligence. The individuals acquired precursors and manufactured explosives, with the intent to use an improvised explosive device (IED) against the identified targets.

Following their arrest, questions were raised as to whether the declarations made by then-President Mohamed Morsi could constitute permission to travel to Syria to engage in terrorist activities, based on Egypt's criminal and counter-terrorism laws. In its verdict, Supreme State Security Court ruled participation in military activities and operations within a foreign entity based outside of the country could only be lawful if resulting from written permission from the competent government agency. The court further clarified that the declarations of then-President Morsi could not be substituted to such permission. The defendants were convicted and received sentences ranging from one to ten years of imprisonment.

Case study: the Netherlands

In 2015, six men were convicted in the Netherlands for their roles in a "recruitment organization" which incited, recruited, facilitated and financed young people who wanted to travel to the Syrian Arab Republic to fight. The case raised fundamental questions in the Netherlands about the limits of freedom of speech, freedom of religion and activism. The defence lawyers unsuccessfully tried to argue that it was the men's "ideas" that were being prosecuted and the trial was "tantamount to criminalizing a religious persuasion". The men received sentences of up to six years imprisonment.[29]

Case study: Lebanon

A Syrian national called Abu Amer recruited 14 people in Lebanon to carry out a terrorist act within the Shiite presence area. Abu Amer travelled to Lebanon and reached out to a terrorist cell in support of ISIL, which secured a house in Tripoli to make explosives. These were made using scrap and other materials purchased from stores that sell agricultural fertilizers (to mislead potential investigators). The bombing took place in Burj Al-Barajneh and killed 46 people, in addition to injuring many more and causing substantial material damage. Security services were able to locate and arrest the remaining members of the cell, who were planning to carry out a terrorist act in an Alawite neighbourhood in Tripoli to create sectarian strife among the people of the region.30

1.3 Women and children

Women plays an important role, for example, about one in five of those who have travelled to the Syrian Arab Republic from Europe are females, many of them made the journey through Asia, the Gulf States and North Africa.[31] Although many wives have made the journey to accompany their husbands, single women and teenage girls have also been lured, often online, into travelling for the prospect of participating in the establishment of the caliphate and marrying ISIL (Da'esh) fighters idolized as heroes. Entire families have migrated in a desire of a better life in ISIL (Da'esh)-held territory, including children and grandparents. For instance, in 2015, 12 members of a British Bangladeshi family, ranging in age from 1 to 75, travelled from the United Kingdom to the Syrian Arab Republic via Bangladesh and Turkey.[32] There are many similar examples.

---

29 "Dutch court convicts nine for terror offences", BBC News, 10 December 2015.

30 Shaheen, Kareem. 2020. "ISIS Claims Responsibility as Suicide Bombers Kill Dozens in Beirut". The Guardian.

31 Bibi van Ginkel, Eva Entenmann, eds. "The Foreign Fighters Phenomenon in the European Union", *International Centre for Counter-Terrorism (ICCT) Research Paper* (April 2016).

32 John Simpson, "All 12 of us are here: Luton family announce arrival in ISIS held Syria", The Times, 4 July 2015.

Al-Qaida in Iraq and other similar groups have historically used females as combatants. In some cases, such as the ISIL (Da'esh) affiliate in Nigeria, Boko Haram, females may be deployed as suicide bombers.

However, ISIL (Da'esh) does not consider the function of females in the caliphate to be that of fighters. Instead, the principal roles of women are rearing children and looking after their husbands, as described in the ISIL (Da'esh) magazine Dabiq: "the wife of a mujahid and the mother of lion cubs".[33] According to ISIL (Da'esh) ideology, a "good mother" seeks to indoctrinate her children with the core values of ISIL (Da'esh), raise sons as fighters and potential martyrs, and teach daughters to follow their mother's example as the future wives of fighters.[34]

Women may, however, in some instances, receive firearms training and be permitted to carry arms in public. Similarly, some women have been issued with suicide bomb vests, but only for the purpose of defending themselves if attacked by enemy forces.[35] Alternatively, some female recruits have joined the al-Khansaa brigade, the all-female religious police force formed to deal with women accused of "un-Islamic" behaviour. Members of the unit are allegedly responsible for torturing prisoners and meting out punishment, such as floggings, to those found guilty of breaching the strict code of conduct of ISIL (Da'esh).

Other functions that women may undertake include teaching or nursing. However, one of the most critical roles women may assume is that of radicalizers and propagandists, utilizing their understanding of social media and online contacts. By engaging in online conversations with family, friends, other females and potential fighters, women FTF may encourage them to migrate and facilitate their travel.[36] Whichever role they partake in, women FTF may actively contribute to the running of terrorist organizations.

Case study: United Kingdom

British national Sally Jones, a white Muslim convert and former singer in a punk rock band, went to the Syrian Arab Republic in 2013 with her eight-year-old son to join and marry her boyfriend Junaid Hussain.37 In 2015, Jones issued a series of threatening messages on Twitter. Among other things, she called on Muslim

33 "From the battle of Al-Ahzab to the war of coalitions", Dabiq, Issue 11, available at shorturl.at/eklD6.

34 Radicalisation Awareness Network, "Responses to returnees: Foreign terrorist fighters and their families" (see footnote 17).

35 The Netherlands, General Intelligence and Security Service of the Ministry of the Interior and Kingdom Relations, *Life with ISIS: the Myth Unravelled*, (The Hague, January 2016).

36 Tanya Mehra, "Foreign Terrorist Fighters: Trends, Dynamics and Policy", *ICCT Policy Brief* (December 2016).

37 The United States of America, U.S. Department of State Bureau of Counterterrorism and Countering Violent Extremism, *Designations of Foreign Terrorist Fighters*, (Washington, D.C., 29 September 2015).

women to launch terrorist attacks in the United Kingdom during Ramadan.38 In June 2016, Jones was killed in a United States of America drone strike. Her son JoJo, who had appeared in an ISIL (Da'esh) video executing a prisoner by shooting him in the head, is believed to have died in the same strike.39

For female returnees who have committed terrorist offences and are considered security risks, the general criminal and administrative options remain largely the same as that for their male counterparts. However, the concrete approach to female returnees varies across different jurisdictions. Some States have prosecuted the wives of FTF for terrorism on the basis of their day-to-day support for their husbands. The other States do not consider such actions to be criminal in the absence of additional evidence of terrorist conduct.

Case study: the Netherlands

Laura Hansen, 22 years old, left the Netherlands in September 2015 together with her husband and two young children to live under ISIL (Da'esh) in the Syrian Arab Republic, where her husband joined the group as a fighter. They travelled via Turkey under the pretext of a family holiday. Ten months later, Hansen crossed the Iraqi border with her children, claiming that she had escaped after becoming disillusioned with life under ISIL (Da'esh). Helped by her father, she returned to the Netherlands, where she was arrested and charged with terrorism offences. At the trial, the Court concluded that Hansen had assisted her husband by providing a cover for his travel, and then supporting him, as his wife, while he was training and fighting for ISIL (Da'esh). In November 2017, she was convicted of "preparation or facilitation of a terrorist offence" and sentenced to a term of 24 months imprisonment, with 13 months of the sentence suspended for a period of 3 years.40

While the conventional view is that women may be less likely than men to engage in terrorist conduct, returning females may still constitute a considerable risk. Researchers have found that women who join terrorist groups tend to be motivated by ideology. They see themselves as "part of a social movement" and are dedicated to the cause they believe in.41 Transnational marriages bring the potential for future international collaboration among extremists.

---

38 Alexandra Sims, "Sally Jones: ISIS recruiter 'issues series of terror threats against UK cities' over Twitter", The Independent, 25 May 2016.

39 Fiona Hamilton, Lucy Fisher, "Sally Jones' son 'collateral damage", *The Times*, 13 October 2017.

40 Judgement of the Rotterdam District Court, Case No. 10 / 960288-16, 13 November 2017, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBROT:2017:8858. See also "Mother who took her children to Syria found guilty of aiding terrorism", DutchNews.NL, 13 November 2017.

41 Gaja Pellegrini-Bettoli, "Intrepid Sisters Reveal How ISIS Depends on Role of Women", *Syria Deeply*, 26 May 2017.

Case study: Jordan

In 2014, a female teacher working in Amman, Jordan, became interested in supporting ISIL, and started following the terrorist entity's news through the Internet (particularly media sites and social media). As she established communication with an ISIL member over the internet, she communicated her desire to join the organization in Syria and support the so-called "Sexual Jihad". Her counterpart in Syria encouraged her to do so and asked her to recruit other women in the process, to "marry" jihadist militants, providing sexual comfort and consequently boost fighters' morale. She recruited a former schoolmate with extremist tendencies, and both women were instructed to travel to Turkey for "tourism", before being smuggled across the border into Syria. They remained there for 10 months until their husbands were killed in battle, after which they decided to return home. They were smuggled across the border back into Turkey, from where they flew back to Amman, where they were arrested at the airport.

During the trial, judicial authorities convicted the first suspect of committing a felony for recruiting another individual to join a terrorist entity.

Notwithstanding the prohibition of women fighters within the caliphate, some female returnees may seek to undertake or encourage attacks outside the caliphate (either on their own accord or under the directions of ISIL (Da'esh)). In the first half of 2017, almost a quarter of all terrorist plots in Europe involved women suspects. Terrorist cells comprised entirely of females have been discovered in France, Morocco and the United Kingdom. Their members were subsequently charged with plotting bomb and knife attacks.

While large numbers of male FTF were killed in fighting in Iraq and the Syrian Arab Republic during 2017, many of their wives and children survived. In just one battle – the offensive to liberate Mosul from ISIL (Da'esh) – more than 1,300 women and children surrendered and were detained by Iraqi forces. These women, and others from across the region, seek to be repatriated with their children, to continue living freely in their home countries. Others, such as a 16-year-old German girl captured in Mosul, faced trial for being associated with ISIL (Da'esh).[42]

The average age of FTF from MENA in Syria and Iraq is between 18 to 43.[43] Compared to European countries, almost twice as many women joined the Balkan contingent of ISIS—women represented 36% of the Bosnians and 27% of the Kosovars who travelled to Iraq and Syria between 2012 and 2016.. Women and children (non-combatants)

42 Rachel Roberts, "German teenage 'ISIS bride' could face death penalty in Iraq", *The Independent*, 18 September 2017.

43 El-Said, H., & Barrett, R. (2017). Enhancing the understanding of the foreign terrorist fighters phenomenon in Syria. *United Nations Office of Counter-Terrorism*.

made up close to 55% of Western Balkan contingent that travelled to Syria and Iraq, with entire families (with up to three generations) relocating, often with no intention of returning to their countries of origin.[44]

Children who have accompanied their parents to the Syrian Arab Republic, or have been born there to FTF families, represent an especially troubling issue. Contraception was reportedly illegal under the rule of ISIL (Da'esh), while women were encouraged to bear multiple children.[45] Those born in conflict zones risk statelessness in case both parents are killed or imprisoned. Mothers may also try to claim the nationality of the father for their children.[46]

The recruitment and use of children have been a core part of ISIL (Da'esh) plans for future survival. In ISIL (Da'esh)-occupied territory, children attend school from about the age of six, where, besides being taught subjects such as English, Arabic and maths, they are indoctrinated into ISIL (Da'esh) ideology.

Boys as young as the age of nine, dubbed "cubs of the caliphate", have been trained to use weapons and taught to kill.[47] Between 2014 and 2016, ISIL (Da'esh) is believed to have recruited and trained more than 2,000 boys between the ages of 9 and 15.[48] Classes included both militarization and indoctrination. Weapons and explosives training were coupled with religious instruction.[49] Once trained, children could perform support roles such as treating the wounded. Alternatively, they could act as spies, snipers and frontline fighters.[50] A study of children and youths eulogized in ISIL (Da'esh) propaganda to die as martyrs found that a third of those killed while conducting attacks in 2015 came from countries other than Iraq and the Syrian Arab Republic.[51] In 2016, a 12-year-old Indonesian boy who travelled to the Syrian Arab Republic to fight with ISIL (Da'esh) was reported to be killed in an airstrike.[52]

ISIL (Da'esh) is unique among terrorist groups in its brazen use of child soldiers,

---

44 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.

45 Radicalisation Awareness Network, "Responses to returnees: Foreign terrorist fighters and their families" (see footnote 17).

46 For example, Louse Callaghan, "Islam Mitat: We escaped Raqqa, but I'm still haunted — and hunted — by ISIS", The Sunday Times, 22 October 2017. See also Shiraz Maher, "What should happen to the foreign women and children who joined ISIS?", New Statesman, 28 August 2017.

47 Richard Barrett, "Beyond the Caliphate: Foreign Fighters and the Threat of Returnees", *The Soufan Center*, October 2017.

48 Ibid.

49 Cassandra Vinograd, Ghazi Balkiz and Ammar Cheikh Omar, "ISIS Trains Child Soldiers at Camps for 'Cubs of the Islamic State'" *NBC News*, 7 November 2014.

50 Ibid.

51 Mia Bloom, John Horgan and Charlie Winter, "Depictions of Children and Youth in the Islamic State's Martyrdom Propaganda, 2015-2016", *CTC Sentinel West Point*, Volume 9, Issue 2 (February 2016).

52 Tom Allard, "Indonesian school a launchpad for child fighters in Syria's Islamic State", *Reuters*, 7 September 2017.

who were given a significant role in propaganda videos. Young boys, including the sons of FTF and the Yezidi kidnapped children[53], were filmed executing prisoners by detonating explosives, shooting or beheading them. The youngest known to date is a boy of four, taken to the Syrian Arab Republic as a baby by his British mother, who was shown in a video appearing to detonate car explosives, killing three prisoners.[54]

The welfare and psychological health of young children who return to their countries of birth or their parents' countries must be the number one priority of any multi-agency response. They are likely to be

severely traumatized and desensitized to brutality and violence. Many children will have little memory of any other sort of life and are likely to experience difficulties with integration into communities at home.

Older children who are indoctrinated by ISIL (Da'esh) teachers are likely to have undergone military instruction and have been taught to kill as part of their training. Therefore, any remnants of radicalization need to be countered to prevent problems in years to come.[55] Those who are above the age of criminal responsibility may be subject to prosecution, even as any prosecutorial decisions should balance the young person's level of involvement against the coercion they might have experienced.

Of the first three batches of deportees from Turkey to Indonesia in 2017, totalling 137 individuals, 79 per cent were women or children under the age of 15.[56] Not only have children been taken to the conflict zones, but large numbers were also born there to FTF. A minority of females would undoubtedly have been coerced or tricked into travelling to ISIL (Da'esh). Others would instead have experienced enforced domestication and possibly suffered from sexual slavery and violence. Women, children and other vulnerable individuals may require different treatment upon return, tailored to their individual circumstances. Prosecutors will face a dilemma in many cases as to whether to prosecute. Such decisions may have to take into consideration offences other than terrorism, such as endangerment of children by taking them to a conflict zone.

> "Member States should develop and implement strategies for dealing with specific categories of returnees, in particular minors, women, family members and other potentially vulnerable individuals, providers of medical services and other humanitarian needs and disillusioned returnees who have committed less serious offences"57.

53 "They Were Children When They Were Kidnapped by ISIS and Forced To Fight". 2020. Time.

54 Jay Akbar, "Shocking new ISIS video shows four-year-old British boy dubbed 'Jihadi Junior' blowing up four alleged spies in a car bomb", *Daily Mail*, 10 February 2016.

55 "German Intelligence Warns from New Generation of ISIS Recruits", *Asharq Al-Awsat Newspaper*, 21 October 2017.

56 Sidney Jones, presentation at UNODC Manila Workshop (November 2017).

57 United Nations Security Council Counter-Terrorism Committee, "Madrid Guiding Principles", 23 December 2015, S/2015/939.

1.4 Evolution of the phenomenon

> "Before the Arab Spring erupted in 2011, some 30,000 Muslim foreign fighters had already taken part in 18 different conflicts, ranging from Bosnia to Kashmir and the Philippines"[58].

The mujahidin war in Afghanistan in the 1980s was the first modern conflict to see high levels of foreign fighters' participation. This conflict witnessed the establishment of a global fighter community, replete with funding networks, credibility and battlefield proficiency. Estimates on how many individuals travelled to Afghanistan to fight in the conflict range from 10,000 to 35,000.[59] When the conflict eventually came to an end in 1989, many of the foreign fighters, known as the "Afghan Alumni", went back to their home countries. Some returned to resume a normal life, while others continued militant activities and were involved in the formation of terrorist organizations. At the same time, a large number of those who remained in Afghanistan were enlisted into the newly formed terrorist organization led by Osama bin Laden: Al-Qaida.

As the twentieth century ended, a large core of foreign fighters remained in Afghanistan, where Al-Qaida provided training camps for fighters such as the hijackers of the September 11 terrorist attacks. Examples of persons who are reported to have received training there include:

- Mukhlis Yunos: the leader of the Special Operations Group of the Philippines-based Moro Islamic Liberation Front (MILF) and an explosives expert.[60] Yunos was convicted for his role in a coordinated series of bomb attacks, including a public transport attack that killed 22 people and wounded scores of commuters in Metro Manila on Rizal Day in December 2000.[61] He is reported to have received military training in Afghanistan in the 1990s.[62]
- Ramzi Yousef: convicted of masterminding the attack on the World Trade Centre in New York in 1993 using a truck bomb that killed six people but was intended to kill hundreds more. He was also convicted of a plot, planned in the Philippines, to place bombs on passenger flights. Yousef fought in the mujahidin war in Afghanistan.[63]

58 Alex P. Schmid, "Foreign (Terrorist) Fighter Estimates: Conceptual and Data Issues", ICCT Policy Brief (October 2015.

59 Maria Galperin Donnelly, Thomas M. Sanderson and Zack Fellman, "Foreign Fighters in History", *Center for Strategic and International Studies*, (Washington, D.C.).

60 United States of America, U.S. Department of the Treasury, *Snow Announces Designation of 10 Jemaah Islamiyah (JI) Terrorists*, Press Release JS-700 (Washington, D.C., 5 September 2003).

61 Sandy Araneta, "Life terms for MILF Rizal Day bombers", *The Philippine Star*, 24 January 2009.

62 Maria Ressa, *From Bin Laden to Facebook: 10 Days of Abduction, 10 Years of Terrorism*, (London, Imperial College Press, 2013).

63 Benjamin Weiser, "Mastermind Gets Life for Bombing of Trade Center", *The New York Times*, 9 January 1998.

- Dr Azahari bin Husin: reported to have been Jemaah Islamiyah's chief bomb maker and responsible for the devices used in a series of attacks, including those against the Bali nightclubs in 2002, the Marriott Hotel in Jakarta in 2003 and Jakarta's Australian Embassy in 2004, which caused the deaths of 245 people. He is said to have received explosives training in Afghanistan in 1999.[64]

The attacks of 11 September in New York and Washington, planned from Afghanistan, gave Al-Qaida enormous credibility in the eyes of violent extremist communities. Whereas previous conflicts had been considered defensive wars on behalf of local Muslim populations, Al-Qaida was able to portray the ensuing Global War on Terror as a war against Islam and to call on Muslims to undertake their religious duty to rise up against the "West". When Afghanistan was invaded, as many as 10,000-20,000 foreign fighters were already present. They were joined by others, mainly from the Middle East, North Africa, China and the former Soviet Union, to fight on behalf of Al-Qaida and the Taliban.[65]

The subsequent invasion of Iraq in 2003 was again seized on by Al-Qaida to portray the Muslim world as being under attack. Soon after the invasion, foreign fighters started arriving in the country. As many as 4,000-5,000 FTF responded to Al-Qaida's rallying calls and joined local Sunni militants. These FTF comprised as much as 5 per cent of the total Iraqi insurgency. Mainly in their early 20s and from the Middle East, the recruits represented a new generation of fighters.[66]

Al-Qaida in Iraq (AQI) embarked on an excessively brutal and bloody campaign of suicide bombings and beheadings, targeting not just coalition forces and Westerners, but also the Iraqi Shia population. FTF volunteered to carry out most suicide bombings.[67] AQI began to lose power in 2006 following the death of its leader in an airstrike, and Sunni tribal leaders formed a new movement for the purpose of expelling the terrorist group. Many of AQI's leaders were killed or imprisoned, but the group continued to conduct attacks.

After the outbreak of civil war in the Syrian Arab Republic in 2011, one of AQI's commanders established an official Al-Qaida affiliate in the country, called the al-Nusrah Front. At the same time, remnants of AQI sought to create a safe haven in the Syrian Arab Republic. Both initially were part of an estimated 1,000-person armed opposition group in the Syrian Arab Republic[68] that soon became bolstered by an

64 "Dr Azahari the most dangerous terrorist", *The Star Online*, 15 August 2003.

65 Donnelly, Sanderson and Fellman, "Foreign Fighters in History" (see footnote 59).

66 Ibid.

67 Mohammed Hafez, Suicide Bombers in Iraq: The Strategy and Ideology of Martyrdom, Washington, D.C., *United States Institute of Peace*, 2007.

68 "Guide to the Syrian rebels", *BBC News*, 13 December 2013.

influx of foreign fighters, many of whom were initially motivated to protect their Sunni "brothers and sisters" against the perceived brutality of the Syrian government. AQI and the al-Nusrah Front recruited the majority of these new fighters, or merged with the militant groups they had joined, resulting in a multinational composition of fighters.

In 2013, the then leader of AQI, Abu Bakr al Baghdadi, moved to grab power and renamed AQI as the Islamic State of Iraq and the Levant, leading to a split from Al-Qaida and the al-Nusrah Front. Subsequently, the group captured large swathes of territory in both Iraq and the Syrian Arab Republic, leading Abu Bakr al Baghdadi in June 2014 to proclaim the creation of a caliphate, with the group rebranded as "Islamic State."[69] Muslims around the world were urged to fulfil their religious duty and migrate to the new "state".[70]

Despite its extreme use of violence, the persuasive use of propaganda by ISIL (Da'esh) (portraying its military successes and the benefits of life under the caliphate) led to an unprecedented flow of volunteers from around the world travelling to live under the rule of the terrorist group. This included not just male FTF, but also lone women and families.

While the eyes of the world are on Iraq and the Syrian Arab Republic, FTF are also engaged in terrorist activity with other branches or affiliates of ISIL (Da'esh) and Al-Qaida and with insurgent groups such as the Afghan Taliban.[71] Normally drawn from the same continent or from diaspora communities of the countries involved, they all potentially pose risks for the future. It is the numbers and multinational composition of those drawn to the Syrian conflict that is unique.

1.5 Global situation

At its peak, about 10 million people were living in areas under ISIL (Da'esh) control in Iraq and the Syrian Arab Republic[72] and the flow of foreign fighters across the Turkish-Syrian border was as high as 2,000 per month.[73] By 2015, approximately 40,000 individuals from over 120 countries had travelled to Iraq and the Syrian Arab Republic as fighters.[74] An estimated 80 per cent of those, migrated to join ISIL (Da'esh) and live in the caliphate,[75] creating a combined force with local Syrians and Iraqis assessed at around 100,000 fighters.[76]

INTERPOL has 53,000 names in its ISIL (Da'esh) database, including information collected from the battlefields in Iraq and Syria[77].

As part of its overarching aim to build a global Islamic caliphate, ISIL (Da'esh) has announced the establishment of a number of provinces outside of Iraq and the Syrian Arab Republic. Controlled by affiliated groups, these provinces are located in the Middle East (Egypt—Sinai, Libya, Yemen, and Saudi Arabia) and beyond (North Caucasus,

Algeria, Nigeria and on the Afghanistan/Pakistan border).[78] It is reported that more than 50 terrorist groups around the world have pledged allegiance to ISIL (Da'esh).[79]

The tightening of border controls - particularly by Turkey - after the adoption of United Nations Security Council resolution 2178 (2014), combined with the worsening situation on the ground in Iraq and the Syrian Arab Republic, meant that by September 2016 the flow of fighters crossing the border from Turkey had dropped to an estimated 50 per month.[80]

By December 2017, ISIL (Da'esh) had lost most of the land it held in Iraq, and was reduced to occupying only 7 per cent of Syrian territory (contrast this with December 2016, when ISIL (Da'esh) held almost 55 per cent).[81] The group was driven out of the main urban areas it controlled, including the Syrian city of Raqqa—the de facto capital of the caliphate—and its regional capital of Mosul in Iraq. The loss of seized oil fields also meant ISIL (Da'esh) lost its main revenue streams.[82]

The Global Coalition to Defeat ISIL (Da'esh) estimated there were less than 1,000 ISIL (Da'esh) terrorists in the coalition's area of operations at the end of 2017,[83] with an unknown but heavily reduced number in eastern Syria and western Iraq. The governments of Iraq and the Syrian Arab Republic both declared victory over ISIL (Da'esh), even as the terrorist group continued to conduct attacks against military and civilian targets.[84] Despite major territorial losses, ISIL (Da'esh) remains the "deadliest terrorist organization in the world".[85] It has gained the allegiance of established and emerging terrorist groups in other countries and directs or inspires terrorist attacks around the globe.

Broadly speaking, ISIL (Da'esh) attacks can be placed in three categories. Firstly, there are attacks conducted by "core" FTF operatives, who are trained by ISIL (Da'esh), based in and primarily active in Iraq and the Syrian Arab Republic.[86] Secondly, there are attacks where the person or group has not travelled to the conflict zone but is coached virtually by an ISIL (Da'esh) facilitator based in Iraq or the Syrian Arab Republic (often an FTF from their own country). Using encrypted messaging, these facilitators

78 Kathrine Bauer, "Beyond Syria and Iraq - Examining Islamic State Provinces", The Washington Institute for Near East Policy (November 2016).

79 Ibid.

80 Byman,"What's beyond the defeat of ISIS?" (see footnote 72).

81 OMRAN Center for Strategic Studies available at: https://omranstudies.org/. For an updated map of the areas controlled by ISIL (Da'esh), see https://isis.liveuamap.com/.

82 Jack Moore, "End of ISIS Approaching as Caliphate Loses Money and Land", *Newsweek*, 29 June 2017.

83 Ahmed Aboulenein, "Less than 1,000 IS fighters remain in Iraq and Syria, coalition says", *Reuters*, 27 December 2017.

84 Mohamad Rachid, "Why Reports of ISIS' Demise Have Been Greatly Exaggerated", Omran Center for Strategic Studies (18 December 2017).

85 START, "Overview: Terrorism in 2016", University of Maryland National Consortium for the Study of Terrorism and Responses to Terrorism, August 2017.

86 Ibid.

both encourage and instruct would-be attackers. Attacks conducted in this manner have been termed by some commentators as "remote-controlled attacks".[87] Finally, there are "lone wolf attacks", where the person or group self-affiliates with ISIL (Da'esh) but does not have any direct link with the group. These attacks have been referred to as "leaderless jihad".[88] Thirty-five such attacks were carried out across 16 countries in 2016, killing 172 people.[89] However, it is often difficult to correctly classify the attacks. Although contact with the ISIL (Da'esh) is frequently suspected, tangible evidence may not be found.

The future for ISIL (Da'esh)

While the caliphate appears to be on the verge of extinction, the organization of ISIL (Da'esh) is not. The threat it has created is multidimensional, constantly and rapidly evolving. ISIL (Da'esh) may seek to establish provinces in countries abroad[90] with the ultimate goal of establishing a new satellite State.

Branches of ISIL (Da'esh) in its provinces are increasing in influence. In Yemen, the group is reported to have doubled in size in 2017.[91] In Sinai and Afghanistan, increasingly lethal attacks are being carried out in the group's name. ISIL (Da'esh) fighters are also redeploying in Libya.[92] In Iraq and the Syrian Arab Republic, ISIL (Da'esh) could easily revert back to what the group was in its early days, namely, "a lethal insurgent force using tactics ranging from terrorist attacks to guerrilla warfare."[93]

The decision to withdraw U.S. troops from Syria in 2019 may contribute to providing ISIL (Da'esh) with the time and space to regrow its organization and extend its networks throughout the Middle East.[94]

What has happened to the fighters?

Research indicates that an estimated 14,910 FTF have already left Iraq and the Syrian Arab Republic,[95] many in the early stages of the conflict. The Global Coalition has stated that since the start of Coalition action in 2014, most ISIL (Da'esh) fighters have been

87 CBC radio, "Terror from afar: how ISIS inspires and directs attacks remotely", podcast, 24 March 2017.

88 Marc Sageman, *Leaderless Jihad - Terror Networks in the Twenty-First Century* (Philadelphia, University of Pennsylvania Press, 2008); see also Daniel, L. Byman, "Frustrated foreign fighters", Brookings Institution, 13 July 2017.

89 START, "Overview: Terrorism in 2016" (see footnote 84): see also Tim Lister et al., "ISIS goes global: 143 attacks in 29 countries have killed 2,043", *CNN*, 12 February 2018.

90 William Arkin, Robert Windrem and Cynthia McFadden, "New Counterterrorism 'Heat Map' Shows ISIS Branches Spreading Worldwide", *NBC News,*3 August 2016.

91 Andrew Blake, "Islamic State in Yemen has 'doubled in size' since 2016: Pentagon", *The Washington Times,* 21 December 2017.

92 Bel Trew, "ISIS regroups in Libya after defeats across Iraq and Syria" *The Times*, 18 August 2017.

93 Duncan Walker, "How real is the threat of returning IS fighters?", *BBC News*, 23 October 2017.

94 Rand Corporation, "How the U.S. Withdrawal from Syria Provides a Boost to ISIS", 21 October 2019.

95 Kim Kraig, "Foreign Fighter 'Hot Potato'", Lawfare, 26 November 2017; see also Barrett, "Beyond the Caliphate" (see footnote 48).

killed or captured.[96] However, reports suggest considerable numbers were still able to survive or escape. These FTF could have left disguised as civilians during evacuations from cities such as Raqqa, subsequently using established people smuggling routes to cross the border into Turkey.[97]

The FTF currently in Iraq and the Syrian Arab Republic may have no option but to stay and fight. FTF were overrepresented in the final battles for Mosul and Raqqa. Many are currently being tried in Iraqi courts[98] or in the custody of the Syrian Democratic Forces (SDF). Some, according to the Coalition, are moving into areas controlled by the Syrian government.[99]

> "We have killed, in conservative estimates, sixty thousand to seventy thousand. They declared an army, they put it on the battlefield, and we went to war with it."[100]

Not all FTF who leave will seek to return to their home States. Some might be unwilling to do so because of fear of executive action by law enforcement agencies. Others may instead be prevented from doing so because of removal of citizenship or other sanctions. They may look for refuge in other countries, where they could strengthen the capabilities of local violent groups. Still, some FTF may choose to remain in Turkey. More recent reports indicate that fighters who remain loyal to ISIL (Da'esh) are "laying low" while waiting for new developments in the Syrian Arab Republic, with the intention of returning to the conflict zone if world attention is diverted elsewhere and the situation changes in their favour.[101]

For FTF seeking new battlefields, there are several potential destinations. As stated above, the branches of ISIL (Da'esh) in Afghanistan, Libya, Sinai and Yemen are all very active, and already include FTF in their ranks. A movement of escaping fighters to this ISIL (Da'esh) provinces has already been reported.[102] Other terrorist groups affiliated with ISIL (Da'esh), such as in the Philippines, may also welcome FTF from the Syrian campaign.

The large flow of refugees and asylum seekers from conflict zones raises the risk that

---

96 Ahmed Aboulenein, "Less than 1,000 IS fighters remain in Iraq and Syria, coalition says" (see footnote 82).

97 Hannah Lucinda Smith, "Surge of ISIS fighters set to hit mainland Europe, Turkey warns", *The Times*, 5 December 2017.

98 Ahmed Aboulenein, "Iraq accused of violating due process for Islamic State suspects", *Reuters*, 5 December 2017.

99 Jeff Seldin, "IS Fighters Fleeing to Assad-controlled Parts of Syria", *Voice of America News,* 27 December 2017.

100 General Raymond Thomas, Head of United States Special Operations Command, speaking at the Aspen Security Forum in July 2017 about ISIL (Da'esh) fighters, in Robin Wright, "ISIS Jihadis Have Returned Home by the Thousands", The New Yorker, 23 October 2017.

101 Robin Wright, "ISIS Jihadis Have Returned Home by the Thousands", *The New Yorker*, 23 October 2017.

102 Evan W. Burt, "The Sinai: Jihadism's Latest Frontline", *Wilson Center*, 13 September 2017.
See also Jeff Seldin, "Afghan Officials: Islamic State Fighters Finding Sanctuary in Afghanistan", *Voice of America News,* 18 November 2017.

FTF will try to use the refugee system or migrant-trafficking routes, either to escape prosecution[103] or to move to new theatres of operation. According to the United Nations figures, over five million Syrians have fled abroad to escape the fighting in the Syrian Arab Republic; of that number, more than 970,000 have applied for asylum in Europe.[104] The two Iraqi suicide bombers at the Stade de France football stadium in Paris in 2015 had travelled on false Syrian passports using migrant routes through Greece.[105] Iraqi and Syrian fighters driven out of their own countries will potentially look to do the same. Genuine refugees, disaffected by their circumstances, may be vulnerable to recruitment.[106]

Al-Qaida

While governments across the globe and the public fear an attack by ISIL (Da'esh) the most,[107] the threat of other terrorist organizations should not be forgotten. In particular, Al-Qaida seeks to make a comeback and is making plans towards its "strategic objective … to incite the umma to undertake a global jihad to defend Muslims", seeking to fill any vacuum left by ISIL (Da'esh).[108]

Al-Qaida's continuing international danger was emphasized in 2013 when the organization embedded a core group of military specialists from Afghanistan and Pakistan to work under the protection of the al-Nusrah Front in the Syrian Arab Republic. According to publicly released intelligence, the purpose of the group—named by the United States of America officials as the Khorasan Group—was to coordinate with the Yemen-based Al-Qaida in the Arabian Peninsula to sneak explosives onto civil aviation.[109] By September 2014, the Khorasan Group was said by the Pentagon to be "in the final stages of plans to execute major attacks", resulting in the United States airstrikes against suspected bomb factories in the Syrian Arab Republic.[110]

Al-Qaida continues to be a significant worldwide threat, with its regional offshoots

---

103 United Nations Security Council Counter-Terrorism Committee, "Foreign terrorist fighters", available at https://www.un.org/sc/ctc/focus-areas/foreign-terrorist-fighters/.

104 "Islamic State and the crisis in Iraq and Syria in maps" (see footnote 69).

105 "Paris attacks: Who were the attackers?", *BBC*, 27 April 2016. See also "Paris attacks: IS claims two attackers were Iraqi nationals", *BBC News*, 20 January 2016.

106 There are terrorism cases currently awaiting trial in the United Kingdom and Germany of individuals allegedly radicalized to the cause of ISIL after their arrival to those countries.

107 Jacob Poushter and Dorothy Manevich, "Globally, People Point to ISIS and Climate Change as Leading Security Threats", *Pew Research Center*, 1 August 2017.

108 Katherine Zimmerman, "Al Qaeda's strengthening in the shadows", Statement before the House Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence on "The Persistent Threat: Al Qaeda's Evolution and Resilience", *American Enterprise Institute*, 13 July 2017.

109 "What is the Khorasan Group?", *BBC News*, 24 September 2014; see also Cruickshank, "A View from the CT Foxhole: Lisa Monaco, Former Assistant to President Barack Obama for Homeland Security and Counterterrorism", (see footnote 73).

110 "What is the Khorasan Group?" (see footnote 107).

conducting mass-casualty attacks.[111] Al-Qaida in the Islamic Maghreb, Al-Qaida in the Indian subcontinent, Al-Qaida in the Arabian Peninsula, al-Shabaab in East Africa, Jama'a Nusrat al Islam wa al Muslimeen and Al-Qaida in Afghanistan all remain active.[112] In an attempt to expand its sphere of influence, in 2017, Al-

Qaida announced a new affiliate in Jammu and Kashmir.[113] As it has done historically, the organization continues to recruit and utilize the services of FTF. Many of the Islamic State's affiliates who were previously tied to Al-Qaida could revert their allegiance.

Hamza bin Laden, the son of the previous leader Osama bin Laden, has become the new propaganda face of Al-Qaida. He has narrated two videos published in 2017. In the videos, he calls for attacks against the United States and its allies and, in the same fashion as ISIL (Da'esh), states that followers who live in the West do not need to migrate. Rather, they are instructed to conduct martyrdom attacks in their homelands. Outside of the western countries, he urges Muslims to rise up against "tyranny".[114]

In the Syrian Arab Republic, 20 per cent of FTF are estimated to have gone to militant groups other than ISIL (Da'esh),[115] such as the Al-Qaida-affiliated al-Nusrah Front. In July 2016, the al-Nusrah Front publicly disassociated itself from Al-Qaida, renaming the group Jabhat Fateh al-Sham, or Front for the Conquest of the Levant. Referred to as "one of the most formidable Al-Qaida affiliates",[116] its stated objective is to dominate "the armed opposition within the Syrian Arab Republic's civil war, with the ultimate goal of toppling Bashar al-Assad and establishing a jihadist emirate in Syria."[117] In 2017, it announced an alliance with four smaller factions to form Hayat Tahrir al-Sham (HTS), or Liberation of the Levant Organization.[118]

Many analysts view the Jabhat Fateh al-Sham element of the alliance "as a covert Al-Qaida affiliate",[119] simply rebranded to not only appear less extreme and win the support of other militant factions and the civilian population, but also to insulate itself from targeting by foreign governments.

As of July 2017, Hayat Tahrir al-Sham is estimated to have 30,000 fighters and to

---

111 United States of America, Country Reports on Terrorism 2016, *United States Department of State Bureau of Counterterrorism (Washington D.C., United States Department of State Publication*, July 2017).

112 Katherine Zimmerman, "Al Qaeda's strengthening in the shadows" (see footnote 106).

113 Riaz Wani, "How Al-Qaida Came to Kashmir", *The Diplomat*, 20 December 2017.

114 Jack Moore, "Hamza Bin Laden Calls on Muslims to Avenge the Death of His Father, Osama", *Newsweek*, 7 November 2017; see also Ahmet S. Yayla, "Al-Qaida Makes its Move with a Video Primer by Hamza bin Laden", The Soufan Group (20 June 2017).

115 Alex P. Schmid, "Foreign (Terrorist) Fighter Estimates: Conceptual and Data Issues" (see footnote 58).

116 John McQuaid et al., "Independent Assessment of U.S. Government Efforts against Al-Qaida", CNA, October 2017.

117 Ibid.

118 "Tahrir al-Sham: Al-Qaida's latest incarnation in Syria", *BBC News*, 28 February 2017.

119 Zack Gold, "Al-Qaida-Syria (AQS): An Al-Qaida Affiliate Case Study", *CNA*, October 2017.

occupy the "largest Al-Qaida safe haven since 9/11"[120] in Idlib province in the north of the Syrian Arab Republic. Standing to profit both politically and militarily from any decline of ISIL (Da'esh), the numbers of fighters are likely to grow as it integrates units from other defeated rebel groups. To date, the group remains relatively unscathed from any foreign military action.[121] The number of FTF that remain with HTS is unknown. If HTS starts to suffer losses, these FTF may also seek to return home.

1.6 Regional situation in Middle East and North Africa

Despite its military defeat in Iraq and Syria, ISIL and its affiliates continue to pose a significant threat worldwide. The threat posed by ISIL has entered a new phase, with more focus on less visible networks of autonomous individuals and cells leading to more difficult challenges for Member States with the emergence of new domestic terrorist threats[122]. In this respect, the combination of "frustrated travellers", ISIL sympathizers, skilled and trained returnees and relocators raises major concerns among Member States[123].

While many people were killed, thousands of fighters and family members are either in detention in Syria or in Iraq – or still on the run. Authorities worldwide are contemplating – or should be contemplating – the possible return of these fighters in the short to medium term and how to deal with them. In fact, more than a thousand fighters only from North Africa have already returned home since 2012.[124]

One of the main threats to the jurisdictions of the MENA region is FTF returning to their country of origin. [125] It is estimated that around 15,000 persons from other MENA countries have travelled to Iraq and the Syrian Arab Republic between the end of 2012 and 2017[126] (women and children constituted almost 35% of this group).[127]

---

120 Brett McGurk, Statement of the United States Special Presidential Envoy for the Global Coalition to Counter ISIS, in Middle East Institute, "Assessing the Trump Administration's Counterterrorism Policy", video, 27 July 2017.

121 Hashem Osseiran, "Al-Qaida Affiliate and Ahrar al-Sham Compete for Control in Idlib", *Omran Center for Strategic Studies* (3 July 2017).

122 Twenty-third report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities, S/2019/50. Sixth Report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat, S/2018/80.

123 Twenty-second report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities, S/2018/705.

124 Renard, Thomas. "Returnees in the Maghreb: Comparing policies on returning foreign terrorist fighters in Egypt, Morocco and Tunisia." *Egmont Paper* 107 (2019).

125 See, Sylvene. "Returning Foreign Terrorist Fighters: A Catalyst for Recidivism Among Disengaged Terrorists." Counter Terrorist Trends and Analyses, vol. 10, no. 6, 2018, pp. 7–15. *JSTOR*, www.jstor.org/stable/26435161. Accessed 8 June 2020.

126 Lydia Khalil; Rodger Shanahan (24 March 2016). "Iraq and Syria: How Many Foreign Fighters are Fighting for ISIL?". *The Telegraph*. Retrieved 28 September 2016.

127 "Foreign Fighters Trickle into the Syrian Rebellion". *The Washington Institute for Near East Policy*. 11 June 2012. Retrieved 1 July 2013.

Jordan, the Kingdom of Morocco, the Kingdom of Saudi Arabi and Tunisia have provided most of the FTF contingents and are now particularly exposed to the threats posed by returnees.[128] The region has suffered from many attacks conducted by returning combatants. Furthermore, returnees raise serious security concerns, not only to the MENA but also to the rest of the world.

Furthermore, terrorism in the region appears primarily linked not only to the returning FTF but also to individuals who self-radicalize and may commit lone-wolf attacks.[129] Recently, many such deadly attacks were carried out within the MENA and other regions. For example, on 4 November 2015, Faisal Mohammad stabbed and injured four people with a knife on the campus of the University of California. He was then shot dead by the police. The Federal Bureau of Investigation eventually concluded that was inspired to commit the attack by ISIL.[130] In addition, in November 2015, two suicide bombers in Lebanon conducted a terrorist attack targeting Bourj el-Barajneh that is inhabited mostly by Shia Muslims, which result in dozens of deaths.[131]

Historical perspective of the FTF phenomenon

The influx of foreign fighters to Iraq and the Syrian Arab Republic from 2014 to 2018 was not a new phenomenon in MENA. In 1979, the Soviet Union entered Afghanistan to defend its communist proxy government in Kabul from a growing insurgency. Almost immediately, madrassas (religious schools) in Pakistan began a campaign to encourage foreigners to travel to Afghanistan to join the jihad. At first, many of the Arab volunteers who travelled to Afghanistan with the help of Hijaz-based Islamic charities viewed themselves as humanitarian workers. These largely Arab volunteers sought to keep a low profile and to help Afghan refugees who were residing in Peshawar, Pakistan, after fleeing the conflict. In contrast, volunteers arriving during the latter half of the war were fighters facilitated by Abdullah Azzam, an influential Palestinian sheikh who called upon all Muslims to defend Afghanistan.[132]

As the Soviet existence in Afghanistan turned into a prolonged occupation, Peshawar became a hub for fighters to organize and mobilize across the border into Afghanistan. Facilitators like Azzam, who was publishing recruitment literature and teaching in

---

128 Cook and Vale. "From Daesh to 'Diaspora." International Centre for the Study of Radicalisation. *King's College London*. Pages 14-19.

129 United Nations Counter-Terrorism Committee Exceuitve Directorate (CTED) Trends Report: The Challenge of Returning and Relocating Foreign Terrorist Fighters: Research Perspectives". 2020.

130 Kuhn, Andrew (9 November 2015). "New questions emerge about background of UC Merced attacker". *Merced Sun-Star*. Retrieved 16 January 2016.

131 Barnard, Anne; Saad, Hwaida (12 November 2015). "ISIS Claims Responsibility for Blasts That Killed Dozens in Beirut". *The New York Times*. Retrieved 12 November 2015.

132 Donnelly, Maria Galperin, Thomas M. Sanderson, and Zack Fellman. "Foreign Fighters in History." *Center for Strategic International Studies* 5 (2017).

Islamabad, relocated to Peshawar to assist.[133] Azzam's extensive paramilitary experience and networks from his Islamic education in Egypt, Jordan, Saudi Arabia and Syria gave him the ideological and operational clout to effectively mobilize foreign fighters against the Soviets.

The departure of Soviet troops in February 1989 removed the raison d'être for many of the foreigners. Some fighters returned to their countries of origin, where they either demobilized or joined local entities.

At the onset of the civil war in the Syrian Arab Republic, volunteers from different MENA countries felt obliged to join the conflict to help their "fellow Muslims" in need. Most of the fighters from MENA were initially associated with various rebel groups in the Syrian Arab Republic, before joining ISIL (Da'esh) and Al-Qaida affiliated groups, such as the al-Nusrah Front.

Estimated figures of FTF contingents

The movement of terrorists through MENA to the conflict zones presents a unique challenge for the region. As travelling across the region to join the conflict was effortless. Therefore, individuals seeking to join ISIL (Da'esh) could cross the Syrian border with the help of operatives.[134] Flows between MENA countries and the Syrian Arab Republic reached their peak in 2011 and early 2013 when over 8,500 from the MENA region travelled to join the conflict.[135]

The pace of travel subsequently slowed in 2015, and almost came to a complete stop by mid-2016. This decline can be attributed to several factors. These notably include the military defeat of ISIL (Da'esh), international and regional efforts to prevent the movement of FTF into the conflict zones, as well as the gradual exhaustion of the pool of individuals willing to fight in Iraq and the Syrian Arab Republic.[136] Furthermore, it became harder for FTF to travel to ISIL (Da'esh)-held territory as the military coalition, capitalizing on ISIL (Da'esh) losses, began to exercise greater control within the areas formerly controlled by the group.

In a report conducted by CTED in 2019, the number of women who travelled from MENA region to Iraq and the Syrian Arab Republic is estimated to be 285. There is a lack of primary data on women travellers as many States do not record gender-disaggregated data on FTF [137]

133 Hegghammer, "The Rise of Muslim Foreign Fighters," 86.

134 Ibid.

135 Donnelly, Maria Galperin, Thomas M. Sanderson, and Zack Fellman. "Foreign Fighters in History." *Center for Strategic International Studies* 5 (2017).

136 Ibid.

137 CTED Trend Report, "Gender Dimensions of the Response to Returning Foreign Terrorist Fighters: Research Perspectives", February 2019, https://www.un.org/sc/ctc/wp-content/uploads/2019/02/Feb_2019_CTED_Trends_Report.pdf.

The following table lists persons from nine jurisdictions of MENA who are reported to have travelled to Iraq and the Syrian Arab Republic[138].

Jurisdictions	Total Official	Non-Official
Algeria	170	170[139]
Egypt	600	1000
Jordan	2000	3000[140]
Kuwait	N/A	150[141]
Lebanon	N/A	900[142]
Libya	N/A	600[143]
Morocco	1200	1623[144]
Saudi Arabia	2500	3244[145]
Tunis	6000	7000[146]
Total	**12470**	**17687**

Beyond the raw figures, it is important to analyse the number of departures as a percentage of the total population of the respective jurisdiction. For example, compared to Algeria, both Tunis and Saudi Arabia appear to have a higher rate of citizen engagement in the fighting in Iraq and the Syrian Arab Republic. In fact, the population of Algeria is around 42.23 million, and there have been approximately 266 Algerian foreign fighters or 6,29 FTF per one million inhabitants. The population of Tunis and Saudi Arabia are about 11.57 million and 33.7 million respectively, and they have contributed some 13000 and 5000 citizens to the foreign fighter contingent to Iraq and the Syrian Arab Republic. This makes the rate of foreign fighters from Tunis to be around 1123 per one million inhabitants and from Saudi Arabia 148 per one million inhabitants. This is much higher than the Algerian number, which is cited as the highest in the MENA region.[147]

---

138 Ibid.

139 "Algeria: Extremism & Counter-Extremism". 2021. Counter Extremism Project. https://www.counterextremism.com/countries/algeria

140 Richard Barrett, "Beyond the Caliphate: Foreign Fighters and the Threat of Returnees", *The Soufan Center*, October 2017.

141 Ibid.

142 R. Florida, "The Geography of Foreign ISIS Fighters", *Crisis Group*, 10 August 2016, https://www.crisisgroup.org/middle-east-north-africa/north-africa/178-how-islamic-state-rose-fell-and-could-rise-again-maghreb.

143 R. Barrett, 2017.

144 The Crisis Group, "How the Islamic State Rose, Fell and Could Rise Again in the Maghreb", 24 July 2017, https://www.crisisgroup.org/middle-east-north-africa/north-africa/178-how-islamic-state-rose-fell-and-could-rise-again-maghreb

145 R. Barret, (2017).

146 D.L. Byman, "Frustrated Foreign Fighters", *Brookings Institute*, 13 July 2017, https://www.brookings.edu/blog/order-from-chaos/2017/07/13/frustrated-foreign-fighters/.

147 Ibid.

Patterns of radicalization and recruitment

Radicalization and recruitment efforts by violent extremist groups pose a significant long-term challenge to the security of the MENA region. The Islamic tradition among Muslim communities in the North African region is generally oriented towards the Maliki school of thought within Sunni Islam. Maliki interpretations and practices are different from more conservative counterparts in the Arabian Peninsula (Hanbali). This, however, has not prevented some actors from exploiting socioeconomic disenfranchisement, lack of trust in state institutions, and other internal factors in promulgating extreme versions of Salafi doctrine. Research has identified several common "push" and "pull" factors which may have contributed to the radicalization process in the context of the MENA. These factors are, naturally, context-sensitive and vary from one jurisdiction to another.

"Push factors are the negative social, cultural, and political features of one's societal environment that aid in "pushing" vulnerable individuals onto the path of violent extremism. Push factors are what are commonly known as "underlying/root causes", and count among them features such as poverty, unemployment, illiteracy, discrimination, and political/economic marginalization.[148]"

In the context of the MENA region, "push factors" which have been identified as contributing to the radicalization process include economic deprivation, perceived corruption, and political and institutional dysfunction.[149]

Radical movements are taking advantage of economic hardship and the profound failure of governments to improve living conditions. Therefore, these movements started to provide varieties of public services such as helping the poor and providing in-kind support to local Hospitals and schools. On the other hand, some extremist imams began to act as a kind of life coach, and in some areas, these imams provide a place of residence to the needy students, which help them to spread the Salafist and Takfirist ideologies. Among some of the most indigent population opinion, the representatives of these Islamic entities began to have more credibility than the official institutions.[150] The mobilization of FTF in MENA appears to be a challenge for the jurisdictions overseeing regions affected by conflict, and where borders are not fully controlled.

Along with these "push factors", individual-level drivers called "pull factors" also contributed to the radicalization process. "Pull factors" are the perceived positive characteristics and benefits of an extremist organization that "pull" vulnerable individuals to join. These include the attractiveness of the group's ideology, the

148 Understanding Drivers of Violent Extremism: The Case of al-Shabab and Somali Youth – *Combating Terrorism Center at West Point*. (2020). Retrieved 7 September 2020, from https://ctc.usma.edu/understanding-drivers-of-violent-extremism-the-case-of-al-shabab-and-somali-youth/.

149 Ibid.

150- "How the Islamic State Rose, Fell and Could rise Again in the Maghreb" *International Crisis Group, 24 July 2017.*

promise of strong bonds of brotherhood and sense of belonging, the opportunity to build one's reputation, prospects of fame or glory, and other socialization benefits. Research on FTF who travelled to Iraq and the Syrian Arab Republic to join ISIL (Da'esh) suggest a multitude of "pull" factors which may operate in any number of combinations.[151] As regards the "pull" factors, the use of the Internet played an essential role in the process of radicalization. Whether used to disseminate extremist messaging or facilitate networking, web-based platforms and activities have served as drivers or force multipliers of radicalization in the MENA region.

Case study: Tunis

In 2015, the United Nations Working Group on the use of mercenaries had expressed its concern on the large exportation of FTF travelling from Tunis to Iraq and the Syrian Arab Republic.[152] One of the "push factors" identified was reinforced after the democratic transition following the Tunisian Revolution in 2010-2011. Prior to the uprising, individuals in Tunis were affected by the economic stagnation, food inflation, and high level of unemployment, and the uprising had failed to improve many of these conditions. Another crucial "push factor" is the social alienation of conservative groups like the Salafists grew further as they attempted unsuccessfully to create an Islamic state in Tunis[153], especially after the end of Ben Ali's secular regime which suppressed religious freedoms.

Tunis witnessed an increase in numbers of radical groups and terrorist attacks after the Arab Spring in 2011[154]. Suicide attacks, mass shootings, and ambushes on police and army were due to the exploitation of terrorist and violent extremist groups of weak spots and gaps during and after the democratic transition. The "pull factors" were financial temptations offered by terrorist and violent extremist groups which varied between $3,000 and $10,000 per recruit[155], the propaganda of caliphate, and recruitments and exploitations under the umbrella of humanitarian work[156].

Estimated figures of returnees and profiles

As ISIL (Da'esh) lost control of its territory, there were warnings that home countries

151- El-Said, Barrett, "Enhancing the Understanding of the Foreign Terrorist Fighters Phenomenon in Syria" (see footnote 14).

152- OHCHR, "Foreign fighters: Urgent measures needed to stop flow from Tunisia", Tunis/Geneva, July 2015, https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=16223&LangID=E.

153- G. Fahmi, "The Future of Political Salafism in Egypt and Tunisia", Malcolm H. Kerr Carnegie Middle East Center, November 2015, https://carnegie-mec.org/2015/11/16/future-of-political-salafism-in-egypt-and-tunisia-pub-61871.

154- Friedrich-Ebert-Stiftung, "The Rise of Religious Radicalism in the Arab World: Significance, Implications and Counter-Strategies", Amman, 2015.

155 OHCHR, "Foreign fighters: Urgent measures needed to stop flow from Tunisia", Tunis/Geneva, July 2015, https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=16223&LangID=E.

156 Quek, N., & Alkaff, S. (2019), "Analysis of the Tunisian Foreign Terrorist Fighters Phenomenon", Counter Terrorist Trends and Analyses, 11(5), 1-5. Retrieved October 22, 2020, from https://www.jstor.org/stable/26631539.

should prepare for a flood of FTF returnees. However, the number of returnees, if still worrisome, has been much smaller than anticipated.[157] Estimates indicate that 30% of FTF have returned home or moved to a third state.[158] As of November 2017, based on figures from 79 countries, the UN Analytical Support and Sanctions Monitoring Team estimated that nearly 7,000 FTF had died on the battlefield and further 14,900 had left the conflict zones. Of this latter group, only 36 per cent (5,395) were currently imprisoned, while 46 per cent (6,837) had returned home without entering the criminal justice system. FTF training and experience, for instance, handling weapons and explosives, but also their contacts make them exceptionally dangerous to the region.[159]

Most significantly, the fate of a large proportion of the ISIL FTF contingent remains unknown: there is a large discrepancy between the total number of FTF and those recorded as having been killed or detained or having returned or relocated.[160]

The following table lists the returnee rates from Iraq and the Syrian Arab Republic to countries with the highest number of FTF:

Jurisdictions	Total number of returnees from Syria and Iraq
Algeria	116
Egypt	600
Jordan	300
Kuwait	6
Lebanon	14
Libya	84
Morocco	308
Saudi Arabia	762
Sudan	5
Tunis	970
Total	**3439**

Source**:** J. Cook and G. Vale, "From Daesh to 'Diaspora' II: The Challenges Posed by Women and Minors After the Fall of the Caliphate", International Centre for the Study of Radiclisation, Vol.12,

157 Eric Schmitt, "ISIS Fighters Are Not Flooding Back Home to Wreak Havoc as Feared", *The New York Times*, 22 October 2017.

158 Mehra, "Foreign Terrorist Fighters: Trends, Dynamics and Policy" (see footnote 38); see also EUROPOL, TE-SAT 2019 (see footnote 139).

159 TE-SAT 2019 (see footnote 139).

160 CTED Trends Report: The Challenge Of Returning And Relocating Foreign Terrorist Fighters: Research Perspectives". 2020.https://www.un.org/sc/ctc/news/document/cted-trends-report-challenge-returning-relocating-foreign-terrorist-fighters-research-perspectives/.

Iss. 6. July 2019; Cook, Joana, and Gina Vale. "From Daesh to 'Diaspora' II: The Challenges Posed by Women and Minors After the Fall of the Caliphate." CTC Sentinel 12.6 (2019): 30-45.

The motivations for FTF to return are diverse. Some may experience disillusionment with violent extremist ideologies or life in territories controlled by terrorist organizations. Others may return to seek reunion with their families or better socio-economic conditions. A minority may also be bent on carrying out an attack on home soil. In the context of ISIL (Da'esh), the Soufan Center has formulated five broad categories for the classification of returning FTF, each presenting a different level of risk[161].

Category	Description
1. Returnees who left early or after only a short stay and were never particularly integrated with ISIL (Da'esh)	They are believed to retain little sympathy for ISIL (Da'esh) and may not have even travelled with the immediate intention of engaging in terrorist activities.
2. Returnees who stayed longer but did not agree with everything that ISIL (Da'esh) was doing.	As the caliphate began to lose attraction, became more violent towards co-religionists and suffered from increasing internal disagreement, some FTF began to develop doubts over ISIL (Da'esh)'s leadership, tactics, or strategy. These doubts, however, do not necessarily mean that the same returnees do not support terrorist aims, such as the establishment of a caliphate.
3. Returnees who had no qualms about their role or ISIL (Da'esh) tactics and strategy but decided to move on.	For some FTF, fighting for ISIL (Da'esh), gave them a sense of adventure and heroism. The concern here is that participating in ISIL (Da'esh)'s violent tactics is an extreme form of adventure, and the same FTF may seek even more extreme stimulus on return.

161 Barrett, "Beyond the Caliphate: Foreign Fighters and the Threat of Returnees" (see footnote 48).

4. Returnees who were fully committed to ISIL (Da'esh) but forced out by circumstances, such as the loss of territory, or were captured and sent to their home countries.	They are still fully committed to ISIL (Da'esh)'s cause and may attempt to further terrorist purposes by forming cells, recruiting sympathizers, mounting attacks, and fashioning themselves as charismatic veterans.
5. Returnees who were sent abroad by ISIL (Da'esh) to fight for the caliphate elsewhere.	From the earliest days of its formation in 2014, ISIL (Da'esh) developed and maintained a cell of foreign fighters that could plan and carry out attacks abroad. Strictly speaking, these terrorists are not so many returnees, but ought to be treated as fighters dispatched to operate outside the caliphate. Still, they will look the same as FTF returnees, use the same routes, and likely join with others who have left the caliphate. They will also be the most determined of FTF.

Source: Richard Barrett, "Beyond the Caliphate: Foreign Fighters and the Threat of Returnees", The Soufan Center, October 2017.

An additional caveat is that foreign fighters who travelled to Iraq and the Syrian Arab Republic for terrorist purposes should be distinguished from those who did not. In this regard, there is a significant number of returnees who departed from the Syrian Arab Republic before ISIL (Da'esh) established itself as a "caliphate" in 2014. Unlike FTF, most of these "first wave" returnees had different motivations for travelling abroad, such as taking up arms against the Syrian regime or providing humanitarian assistance.[162] While taking up arms abroad may be criminal under the national laws of the fighter's home country, applying counter-terror approaches may prove ineffective in such circumstances.

In any case, it is hard to predict how any returnee may react overtime to their experience abroad, or to their reception at home. Even if they are subject to close psychological and police assessment, circumstances may lead them to seek violent solutions to their problems again, especially if they return to the same conditions that they left.[163]

Likelihood of terrorist attacks from returning FTF

Political discourse on FTF returnees has largely centred on the security risk they may pose. It is not infrequently suggested ISIL (Da'esh) will mobilize returnees to attack targets in their home countries as part of its new focus on global brand preservation. FTF returnees are thought to be particularly dangerous, in no small part due to the

possibility of continuing radicalization and the combat experience they may have acquired during their time in conflict zones. For instance, the perpetrators of the 2015 Paris attacks where, in part, Belgian and French nationals who received training from ISIL (Da'esh) in the Syrian Arab Republic.[164]

Returnees may also maintain networks which they formed with other terrorists during their time abroad.[165] This is problematic since networks allow terrorists to coalesce resources for large scale attacks and provide opportunities for ISIL (Da'esh) core to instruct overseas operatives. Empirical research appears to affirm the value of networks to overseas terrorist operations – a common indicator across terrorist plots within MENA countries is the existence of operational connectivity between ISIL (Da'esh) and the perpetrators. A study of 510 ISIL attacks perpetrated outside the Syrian Arab Republic and Iraq up to 31 October 2017 found that FTF had participated in more than 25 per cent of the attacks, including 87 attacks conducted by FTF outside of their country of origin.[166] In addition to their direct involvement in terrorist attacks or plots, FTF have also been central to the development of a new type of terrorist modus operandi: attacks directed from Tall Afar by "virtual planners" who use secure communications to remotely guide attackers (often single perpetrators) and play a key role in the conceptualization, target selection, timing and execution of attacks.[167]

However, the security threat posed by FTF returnees must not be overestimated. According to EUROPOL, the attacks in the EU have been primarily committed by homegrown terrorists who did not travel abroad to join terrorist groups.[168] Most of these homegrown terrorists were instructed by a terrorist organization, typically through virtual channels. Notable attacks by homegrown terrorists include those on the Berlin Christmas market in 2016 and the London bridge in 2017. These terrorists were able to cause significant casualties without relying on firearms and despite having no combat experience.

The majority of FTF returnees would have no intention to plot terrorist attacks upon their return. A study undertaken by the European Parliamentary Research Service has concluded that "very few concrete cases of 'foreign fighters' returning to conduct attacks in Europe have been observed."[169] In this regard, the profiles of FTF returnees

---

164 "Paris attacks: Who was Abdelhamid Abaaoud?", *BBC News,* 19 November 2015.

165 Daniel L. Byman, "What happens when Arab foreign fighters in Iraq and Syria go home?", *Brookings Institution*, 7 May 2015.

166 Radicalization Awareness Network, "Responses to returnees: Foreign terrorist fighters and their families" (see footnote 17).

167 CTED Trends Report: The Challenge of Returning and Relocating Foreign Terrorist Fighters: Research Perspectives". 2020. https://www.un.org/sc/ctc/news/document/cted-trends-report-challenge-returning-relocating-foreign-terrorist-fighters-research-perspectives.

168 TE-SAT 2018 (see footnote 120).

169 Amandine Scherrer ed., "The return of foreign fighters to EU soil: Ex-post evaluation", European Parliamentary Research Service, May 2018.

are heterogeneous. Not all of them travelled to the conflict zones with the intention of engaging in terrorist violence. Some returnees, especially women and younger children, may not have received training in violent combat or committed violent crimes. On return, some have disengaged entirely from any association with violent extremism. Reports of former FTF actively contributing to efforts to prevent violent extremism exist too.[170] It would consequently be inappropriate to treat all FTF returnees as would-be attackers.

The threat of attacks being carried out by FTF can consequently be classified as high-impact and low-probability.[171] Research reveals that only 18% of attacks carried out in the "West" between June 2014 and June 2017 were by known FTF. However, the attacks conducted by returnees also tend to be among the most lethal, with an average of 35 deaths per attack.[172] From this perspective, the public perception of returnees as a threat must be distinguished from the threat of returnees plotting attacks or engaging in terrorist activities.

As of January 2019, the UN Analytical Support and Sanctions Monitoring Team has assessed the threat of FTF plotting attacks in MENA as "substantial threat".[173] There are several factors which may contribute to this assessment. First, the increase in the number of ISIL returnees in the region.[174] Second, the attacks increasingly resort to hit-and-run operations out of several points of concentration within the region such as in Iraq, Libya and Sinai[175] Third, among domestic groups with extremist views, available evidence suggests they created an organized network structure and tend to be managed by different ideological and political beliefs.[176] The recent domestic terrorist attacks in MENA appears to bear out the UN Analytical Support and Sanctions Monitoring Team's analysis. Since 2011, jurisdictions of MENA have witnessed an immense increase in the numbers of terrorist attacks in the region conducted by FTF returnees and ISIL local affiliates.

By the end of 2017, around 596 Moroccan FTF (which represents 35.8% of the official Moroccan FTF estimate) were killed either committing suicide attacks or in the different battles and coalition airstrikes in both Syria and Iraq.[177] Around 213 returnees from Morocco which only represents 12.8% of the total number of Moroccan FTF between 2011 and 2017 seem to have done so owing to disillusionment with the war and

---

170 Ibid.

171 Ibid.

172 Lorenzo Vidino, Francesco Marone, Eva Entenmann, "Fear thy neighbor: Radicalization and jihadist attacks in the West", *ICCT* (June 2017).

173 S/2019/50 (see footnote 140).

174 Ibid.

175 Ibid.

176 TE-SAT 2018 (see footnote 120).

177 Renard, Thomas. "Returnees in the Maghreb: Comparing policies on returning foreign terrorist fighters in Egypt, Morocco and Tunisia." *Egmont Paper* 107 (2019).

disheartenment with the infighting between jihadist groups[178]. The authorities appear to believe that few of these returnees pose an immediate security risk. Still, experts warn that "disillusionment with a terrorist group does not necessarily equate to distance from a violent ideology, nor disengagement from the 'jihadi' cause."[179] Authorities may, therefore, find value in assessing not just a returnee's attitude towards particular terrorist groups, but also their attitudes towards violence and extremist ideologies. For the authorities in MENA, a key challenge remains to be the deciphering and monitoring the intention of FTF returnees.

178 Richard Barrett, "Beyond the Caliphate: Foreign Fighters and the Threat of Returnees", *The Soufan Center*, October 2017.

179 Radicalisation Awareness Network, "Responses to returnees: Foreign terrorist fighters and their families" (see footnote 17).

Chapter 2

Foreign terrorist fighters: the international and regional legal frameworks

2.1 The international legal framework

Terrorism has been on the agenda of the international community since the 1930s. Over the past 60 years, a total of 19 international conventions and protocols have been adopted to address terrorism. These conventions deal with various thematic areas related to terrorism, such as the suppression of the financing of terrorism, transport-related (maritime and civil aviation) terrorism, nuclear and radiological terrorism, the taking of hostages, and the suppression of terrorist bombings. These instruments are complemented by the United Nations Security Council resolutions to prevent and counter terrorism. Collectively, these instruments create obligations for Member States under international law, which need to be reflected in national legislation, implemented and enforced[180] The implementation of these conventions, protocols and resolutions is informed by the guidance provided by the United Nations Global Counter-Terrorism Strategy along with United Nations General Assembly Resolutions.

Whereas the list of those legal instruments is extensive, the most relevant ones in terms of the investigation and adjudication of FTF-related offences in the international and MENA context are developed in this chapter.

A) United Nations Security Council Resolutions 1373 (2001), 2178 (2014) and 2396 (2017)

A number of Security Council resolutions has been adopted in order to meet the challenges of terrorism prevention and violent extremism, and the changing nature of the threat. Among these, resolution 1373 (2001) represents one of the most far-reaching. Subsequent resolutions should be interpreted and understood in light of resolutions adopted earlier. For instance, resolution 2178 (2014) builds upon the framework established by resolution 1373 (2001). Similarly, resolution 2396 (2017) builds on resolution 2178 (2014). In addition to these three key resolutions (1373, 2178 and 2396), several other Security Council resolutions exist within the counter-terrorism framework.

1. United Nations Security Council resolution 1373 (2001)

Agreed and adopted in the wake of the 11 September terrorist attacks in the United States,

180 For a current list of the international legal instruments to prevent terrorist acts see www.un.org/en/counterterrorism/legal-instruments.shtml.

resolution 1373 (2001)[181] provided the impetus for a series of international instruments targeting terrorism and violent extremism. Reaffirming its earlier unequivocal condemnation of these attacks,[182] the Security Council unanimously adopted sweeping legally binding measures requiring Member States to take a series of actions to counter, prevent and suppress terrorism. Arguably, one of the revolutionary aspects of resolution 1373 (2001) was the introduction of the obligation to criminalize not only terrorist acts themselves, but also preparatory acts such as the financing, planning, facilitation, or support of terrorist acts.

2. United Nations Security Council resolution 2178 (2014)

By September 2014, a pattern of individuals travelling abroad to join terrorist entities including ISIL, al-Nusrah Front and entities associated with Al-Qaida, had grown into such a concern that the Security Council adopted resolution 2178 (2014).[183] The resolution specifically addressed such individuals and defined the term "foreign terrorist fighters" as "Individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning or preparation, or participating in terrorist acts, or the providing or receiving of terrorist training, including in connection with armedconflict."[184]

Furthermore, resolution 2178 (2014) called upon Member States to enhance their criminal justice responses to FTF by introducing measures to detect, prevent and criminalize the travel of FTF and related activities. These measures can be broadly divided into three categories: criminal laws, sanctions and preventive measures. It is important to understand the distinct legal foundations of the three types of measures. Criminal offences have their foundations in criminal or penal codes; sanctions regimes are founded principally on the United Nations sanctions regimes but can also be based on national sanctions regimes; preventative measures are typically grounded in different types of laws that enable such measures to be used on a non-conviction basis, through an administrative procedure or a decision of the Executive, usually at the ministerial level.

Each of these measures serve distinct but overlapping functions. Criminal offences are primarily intended as post-facto punitive measures, although resolution 2178 (2014) also requires Member States to criminalize the attempt to travel abroad as an FTF, which serves a preventative function. In addition to the punitive aspect, a human rights and rule-of-law-based approach requires that following incarceration, policies of disengagement, rehabilitation, and reintegration should also be a priority of national

181 United Nations Security Council Resolution 1373 (2001) S/RES/1373.

182 United Nations Security Council Resolution 1368 (2001) S/RES/1368.

183 S/RES/2178 (see footnote 7, Chapter 1).

184 Ibid.

frameworks. Sanctions regimes suppress and debilitate the capacity of individual FTF and terrorist organizations that are listed under the sanctions lists. Unlike criminal laws or preventative measures that apply to all individuals falling within the jurisdiction of the Member State, the scope of sanctions regimes is limited to individuals and members of groups who have been explicitly placed on the sanctions lists. Preventative measures are self-explanatory in that their primary function is to prevent would-be FTF or terrorists from travelling or otherwise engaging in terrorism-related activities.

These measures may, in some instances, appear similar but are grounded in distinct legal foundations. For instance, travel restrictions may be applied to individuals who are suspected of travelling abroad as a preventative measure, or because they have been listed as a terrorist or FTF under the United Nations

sanctions regime. Examples of these three measures can be found in Security Council resolution 2178 (2014), as summarized in the table below:

Table (1) UN Security Council resolution 2178 (2014) - Overview of criminal justice measures

Criminal offences	
Resolution para.	Text
6(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."
6(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."

6(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."
Sanctions	
Resolution para.	Text
20	"Foreign terrorist fighters and those who finance or otherwise facilitate their travel and subsequent activities may be eligible for inclusion on the Al-Qaida Sanctions List maintained by the Committee pursuant to resolutions 1267 (1999) and 1989 (2011) where they participate in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, or on behalf of, or in support of, Al-Qaida, supplying, selling or transferring arms and related material to, or recruiting for, or otherwise supporting acts or activities of Al-Qaida or any cell, affiliate, splinter group or derivative thereof, and calls upon States to propose such foreign terrorist fighters and those who facilitate or finance their travel and subsequent activities for possible designation."
Preventative measures	
Resolution para.	Text
8	"Without prejudice to entry or transit necessary in the furtherance of a judicial process, including in furtherance of such a process related to arrest or detention of a foreign terrorist fighter, Member States shall prevent the entry into or transit through their territories of any individual about whom that State has credible information that provides reasonable grounds to believe that he or she is seeking entry into or transit through their territory for the purpose of participating in the acts described in paragraph 6, including any acts or activities indicating that an individual, group, undertaking or entity is associated with Al-Qaida, as set out in paragraph 2 of resolution 2161 (2014), provided that nothing in this paragraph shall oblige any State to deny entry or require the departure from its territories of its own nationals or permanent residents."

- **Criminal Offences**

Resolution 2178 (2014) requires Member States to establish serious offences under their national laws to criminalize activities relating to the travel of FTF. These offences cover the following three aspects:

- travel or attempted travel of FTF;
- financing the travel of FTF; and
- organizing or facilitating (including recruitment) the travel of FTF.

A number of key terms and phrases used in the resolution and other international instruments are left to the individual Member States to define, in a manner that gives full consideration to human rights, due process, and privacy concerns.

- **Sanctions**

Resolution 2178 (2014) makes it clear that individual FTF may be designated and listed under the United Nations sanctions regime concerning "ISIL (Da'esh), Al-Qaida, and associated individuals, groups, undertakings and entities" established pursuant to Security Council resolutions 1267 (1999), 1989 (2011) and 2253 (2015). Designation of individuals and entities for sanctions under this regime is decided by the Sanctions Committee upon the submissions of Member States. In addition to the United Nations sanctions regime, resolution 1373 (2001) requires Member States to establish national sanctions

regimes. Individuals subject to national sanctions regimes are designated by governments on their own initiative or following review of a request made by the government of another Member State.

Sanctions typically employ one or more of three measures: travel bans, asset freezing, and arms embargos. Travel bans are of particular importance for disrupting the travel of FTF into conflict zones. For sanctions to be effective and timely, national criminal justice agencies should review and ensure that their inter-agency collaboration is made possible and supported by national laws, regulations, and operating procedures. Law enforcement officials should be familiar with the listing and de-listing procedures applicable under the United Nations sanctions regime as well as the national terrorist sanctions regime within their respective jurisdictions.

- **Preventative measures**

Resolution 2178 (2014) requires Member States to prevent the entry into or transit through their territories of any individual when the State has "credible information that provides reasonable grounds to believe" that he or she is travelling for the purpose of participating in one of the criminal offences established under the resolution.

As per the text of the resolution, such travel preventative measures are triggered when the legal threshold of having "reasonable grounds to believe …" based on "credible information" is met. This language makes it clear that the threshold for implementing the mentioned preventative measures is below the criminal conviction standard of beyond reasonable doubt. In practical terms, this means Member States must establish legal and regulatory mechanisms to enable law enforcement actors to implement preventative measures through executive or administrative action that are not contingent on a criminal conviction. Each Member State must interpret the trigger threshold of having "reasonable grounds" in accordance with its own domestic laws.

The lower legal threshold that applies when utilizing preventative measures is reflective of its function, which is to prevent activities of FTF when law enforcement officials have sufficient information to be aware of their involvement in violent extremist or terrorist activity, even when there is insufficient evidence to prosecute and secure a conviction successfully.

3. United Nations Security Council resolution 2396 (2017)

In December 2017, the Security Council unanimously adopted resolution 2396 (2017).[185] While the subject focus of that resolution is on FTF, it is principally concerned with risks posed by FTF returning from conflict zones, in marked contrast with resolution 2178 (2014), which focused on FTF headed outbound. Resolution 2396 (2017) calls upon Member States to strengthen their efforts to stem the threat emanating from returning and relocating FTF and their family members, including women and children, through measures on border control, criminal justice, and informationsharing.

First, resolution 2396 (2017) urges Member States to strengthen measures to detect, investigate and prosecute returning FTF. As with previous resolutions, it underlines the need for cooperation and information sharing among Member States and with relevant organizations such as INTERPOL in the

detection of FTF. It also stresses the responsibility of Member States to share information and investigate individuals, even when suspects are foreign nationals.

Furthermore, Member States are called upon to develop and implement comprehensive risk assessments for returning and relocating FTF and their accompanying family members. Member States are expected to take appropriate actions, including consideration for tailored prosecution, rehabilitation, and reintegration strategies in compliance with domestic and international law. While emphasizing that Member States are obliged to bring to justice anyone who participated in terrorist acts, the resolution stresses the importance of assisting women or children associated with foreign terrorist fighters who might be victims of terrorism. In this regard, it encourages Member Stages

185 United Nations Security Council Resolution 2396 (2017) S/RES/2396.

to take women and children into special consideration when developing prosecution, rehabilitation, and reintegration strategies.

Finally, resolution 2396 (2017) requires Member States to develop and implement three types of administrative measures in the prevention and suppression of FTF travel:

- the collection of biometric data, which could include fingerprints, photographs and facial recognition;
- the establishment of Advance Passenger Information Systems (API), which require that airlines operating in a territory of a Member State provide to the competent national authorities basic information on passengers identity (such as name, date of birth, gender, or citizenship); and
- the capability to collect, process, and analyse Passenger Name Record (PNR) data, and ensure PNR data is used by and shared with all competent national authorities.

B) United Nations Global Counter-Terrorism Strategy

In addition to UN Security Council resolutions, the United Nations Global Counter-Terrorism Strategy provides a framework to address the FTF phenomenon. This strategy was adopted by the UN General Assembly on 8 September 2006[186] to provide an overarching framework for the response of all Member States to terrorism.

Even though the strategy is not legally binding to Member States – unlike Security Council resolutions adopted under Chapter VII of the Charter of the United Nations - it nonetheless represents a unique global instrument to enhance national, regional and international efforts to counter-terrorism. Through its adoption, all Member States have agreed for the very first time on a common strategic approach to fight terrorism, based on four main pillars:

- Pillar I: Addressing the conditions conducive to the spread of terrorism
- Pillar II: Preventing and combating terrorism
- Pillar III: Building States' capacity and strengthening the role of the United Nations
- Pillar IV: Ensuring human rights and the rule of law

The global strategy relies on both criminal justice and governance measures, with both approaches mutually reinforcing the other.

186 United Nations General Assembly Resolution 60/288 (2006) A/RES/60/288.

The criminal justice approach to prevent violent extremism and terrorism principally calls for Member States to establish and apply a range of criminal offences relating to violent extremism and terrorism. Criminal justice frameworks deal not only with acts of terrorism, but also the preparatory stages leading up to terrorism, including the recruitment of potential terrorists and incitement of terrorism. Under the international legal framework, Member States are required to implement obligations arising under the Security Council resolutions and other binding international conventions and protocols into their national laws.

The governance approach is principally used to prevent violent extremism by minimizing or eliminating the conditions conducive to violent extremism leading to terrorism. Deeply entrenched and inconspicuous socio-political issues that are considered to be root causes of violent extremism may not always be solved through a criminal justice approach. These causes are typically systemic rather than attributable to a particular individual or a group. These "non-criminal" aspects, which include inequality, perceptions of dissatisfaction, and social disenfranchisement, may serve as factors which ultimately "push" vulnerable individuals to engage with violent extremism and terrorism. As these issues are extremely deep-rooted, criminal justice frameworks that focus on criminal acts can only provide partial solutions. In these situations, good governance plays a crucial role in addressing the conditions conducive to the spread of terrorism. Examples include promoting moderation in religious education, implementing policies to support early identification of vulnerable individuals at risk of exposure to violent extremism, and providing dominant alternative narratives to counter the narratives of terrorist organizations.

Thus, the global framework seeks to eliminate the root causes of violent extremism and to implement robust criminal justice responses towards acts of terrorism and preparatory acts. These objectives are achieved through a web of strategies, policies, laws, institutions, as well as a range of operational capabilities. Each aspect is reliant upon the other elements for their effective functioning, and collectively espouse a holistic whole-of-government and whole-of-society approach to preventing and countering violent extremism and terrorism.

The United Nations Global Counter-Terrorism Strategy is reviewed and updated every two years by the UN General Assembly to reflect changing priorities. From 26 to 27 June 2018, the UN General Assembly held its sixth biennial review of the UN Global Counter-Terrorism Strategy. This review concluded in the adoption of General Assembly resolution 72/284[187] by consensus. Regarding the risks related to returning FTF, resolution 72/284 notably:

- called upon Member States to strengthen their cooperation at the international,

187 United Nations General Assembly Resolution 72/284 (2018) A/RES/72/284.

regional, sub-regional and bilateral levels to counter the threat posed by FTF, including through enhanced operational and timely information-sharing, logistical support and capacity-building activities;

- encouraged Member States to implement programmes on biometric data, Advance Passenger Information (API) Systems, and PNR data, as set out in UN Security Council resolution 2396 (2017); and
- called upon law enforcement and criminal justice authorities to better address the threat of returning FTF.

C) The 19 international instruments to prevent terrorist acts

Since 1963, the international community has elaborated 19 international legal instruments to prevent terrorist acts. Those instruments were developed under the auspices of the United Nations and the International Atomic Energy Agency (IAEA), and are open to participation by all Member States.

Although they are not specifically targeting FTF, they represent a major component of the international corpus juris against terrorism and provide an important framework for international cooperation in terrorist/ FTF cases. In this regard, many legally binding UN Security Council resolutions called upon Member States to become party to these instruments to fulfil the obligations that they impose.

Table (2) 19 International legal instruments to prevent terrorist acts

INSTRUMENTS REGARDING CIVIL AVIATION	
1.	1963 Convention on Offences and Certain Other Acts Committed on Board Aircraft
2.	1970 Convention for the Suppression of Unlawful Seizure of Aircraft
3.	1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation
4.	1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation
5.	2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation
6.	2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft

7.	2014 Protocol to Amend the Convention on Offences and Certain Acts Committed on Board Aircraft
INSTRUMENTS REGARDING THE PROTECTION OF INTERNATIONAL STAFF	
8.	1973 Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons
9.	1979 International Convention against the Taking of Hostages
INSTRUMENTS REGARDING THE NUCLEAR MATERIAL	
10.	1980 Convention on the Physical Protection of Nuclear Material
11.	2005 Amendments to the Convention on the Physical Protection of Nuclear Material
INSTRUMENTS REGARDING THE MARITIME NAVIGATION	
12.	1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation
13.	2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation
14.	1988 Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf
15.	2005 Protocol to the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms located on the Continental Shelf
INSTRUMENTS REGARDING EXPLOSIVE MATERIALS	
16.	1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection
17.	1997 International Convention for the Suppression of Terrorist Bombings
18.	1999 International Convention for the Suppression of the Financing of Terrorism
INSTRUMENTS REGARDING NUCLEAR TERRORISM	
19.	2005 International Convention for the Suppression of Acts of Nuclear Terrorism

D) International guiding principles

In addition to international legal obligations that Member States are required to perform, some international instruments set out recommendations and best practices that Member States are encouraged to adopt to strengthen their response to the FTF threat. In particular, three helpful references are:

- The Hague-Marrakech Memorandum on Good Practices for a More Effective Response to the FTF Phenomenon (2014) and its Addendum (2015).
- The Malta Principles for Reintegrating Returning Foreign Terrorist Fighters (2016).
- The Madrid Guiding Principles 2015 and its Addendum (2018).

1. The Hague - Marrakech Memorandum on Good Practices for a More Effective Response to the FTF phenomenon (2014) and its Addendum (2015)

The Hague-Marrakech Memorandum on Good Practices for a More Effective Response to the FTF phenomenon[188] is an initiative launched in 2014 by Morocco and the Netherlands within the framework of the Global Counter-Terrorism Forum (GCTF).[189] The aim of this initiative is to bring together practitioners and policymakers from a wide range of countries to share lessons learned, good practices and challenges in responding to the FTF threat.

The Memorandum identified 19 good practices to guide Governments in their policies to address the FTF threat. These goods practices focus on several aspects of the responses to the FTF threat, including:[190]

- Detecting and intervening against violent extremism (good practices n°1 to n°5);
  - *Good Practice #1 - Invest in the long-term cultivation of trusted relationships with communities susceptible to recruitment, considering the broader set of issues and concerns affecting the community.*
  - *Good Practice #2 – Develop a wide range of proactive, positive counter-narratives and alternative activities, offering non-violent, productive*

188 Global Counterterrorism Forum (GCTF), "The Hague-Marrakech Memorandum on good practices for a more effective response to the FTF phenomenon" (2014).

189 The GCTF is an informal, multilateral counter-terrorism Platform launched in 2011 to assist in the implementation of the UN Global Counter-Terrorism Strategy. The GCTF has six Working Groups, one of them is on Foreign Terrorist Fighters. The GCTF members from MENA are: Algeria, Egypt, Jordan, Morocco, Qatar, Saudi Arabia and United Arab Emirates.

190 Global Counterterrorism Forum (2014). "Foreign Terrorist Fighters" (FTF) Initiative The Hague - Marrakech Memorandum on Good Practices for a More Effective Response to the FTF Phenomenon.

alternatives to help those in need, as well as means to channel frustration, anger, and concerns without turning to violence.

- *Good Practice #3 – Bring together social media, analytic experts, and technology innovators to develop and produce compelling counter-narrative content.*
- *Good Practice #4 – Empower those who are best-placed to affect change, including youth, families, women, and civil society, to take ownership in the development and messaging of positive counter-narratives to the violent extremist agenda.*
- *Good Practice #5 - Prevent the identification of the FTF phenomenon or violent extremism with any religion, culture, ethnic group, nationality, or race.*

- Preventing, detecting and intervening against recruitment and facilitation (good practices n°6 to n°9);

  - *Good Practice #6 - Reach out to communities to develop awareness of the FTF threat and build resilience to violent extremist messages.*
  - *Good Practice #7 – Collect and fuse detailed information from government agencies, front line workers, communities, and social media to detect recruitment and facilitation while respecting the rule of law and human rights.*
  - *Good Practice #8 – Pool resources, share information, and collaborate with the private sector to curb online recruitment of FTFs.*
  - *Good Practice #9 - Adopt tailored and targeted approaches for CVE responses to radicalization and recruitment, based on the specific motivational factors and intended audience.*

- Detecting and intervening against travel and fighting (good practices n°10 to n°14); and

  - *Good Practice #10 - Increase the sharing of local public, law enforcement and intelligence information and analysis, and corresponding best practices, through bilateral relationships and multilateral fora to prevent FTF travel.*
  - *Good Practice #11 – Develop and implement appropriate legal regimes and administrative procedures to effectively prosecute and mitigate the risk posed by FTFs.*
  - *Good Practice #12 – Apply appropriate screening measures designed to disrupt FTF travel, with particular attention to air travel.*
  - *Good Practice #13 – Use all available tools to prevent the misuse of travel*

documents for FTF travel.

- *Good Practice #14 - Increase the capacity of States to prevent FTF travel across land borders and, more broadly, take appropriate measures to prevent FTF within their territory from planning or preparing for terrorist acts to be carried out at home or abroad.*

- Detecting and intervening upon return (good practices n°15 to n°19).

- *Good Practice #15 - Use as wide as possible a range of information sources to anticipate and detect returnees.*

- *Good Practice #16 – Build and use evidence-based, individual-level risk assessment frameworks for returnees, evaluate their condition and establish appropriate engagement approaches accordingly.*

- *Good Practice #17 – Strengthen investigations and prosecutions of FTFs, when appropriate, through improved information sharing and evidence gathering.*

- *Good Practice #18 – Prepare and exercise responses to the kinds of terrorist acts for which FTFs may have special skills.*

- *Good Practice #19 – Develop comprehensive reintegration programs for returning FTF.*

In 2015, an Addendum to this Memorandum[191] focusing on returning FTF was adopted. The Addendum provides seven recommendations,[192] including:

- The reinforcement of cooperation and information-sharing between law enforcement, intelligence, border control and public prosecution services;
- Access to relevant databases by law enforcement and border agencies; and
- The need to develop tailored approaches when dealing with returnees, taking into account "the risk the individual poses with respect to the commission of a terrorist attack; the gravity and seriousness of the crime; the available evidence; motivational factors; the age of the returnee; the support network of family and friends; the impact on victims; and the public interest."

---

191 GCTF, "Addendum to The Hague-Marrakech Memorandum on good practices for a more effective response to the FTF phenomenon, with a focus on Returning FTFs" (2015).

192 (1) "Ensure timely detection of, and intensify information sharing on returning FTFs within and between States." (2) "Use individual risk assessment tools that provide a basis for tailor - made interventions." (3) "Apply a case-by-case approach and address specific categories of returnees." (4) "Invest and develop a close partnership with local government and local communities to deal with returning FTFs." (5) "Engage and build sustainable partnerships with multi - disciplinary actors in the private sector and civil society organizations." (6) "Integrate rehabilitative measures within and beyond the criminal justice response." (7) "Consider using administrative procedures within a rule of law framework to effectively mitigate the risk posed by returning FTFs."

2. The Malta Principles for Reintegrating Returning Foreign Terrorist Fighters (2016)

The Malta Principles for Reintegrating Returning Foreign Terrorist Fighters[193] is a joint initiative between the Hedayah Research Centre and the International Institute for Justice and the Rule of Law (IIJ). This initiative proposed 22 principles to guide Member States in their policies and programmes on the reintegration of returning FTF. Some principles are worth highlighting here:

- **Principle #3**: "Conduct effective assessments to determine the best approach for reintegration program needs."

Principle #3 emphasizes that engagement with returnees should be individualized. Consequently, reintegration program "should be designed with individuals in mind, whether they serve FTF returning from active combat, their families, or those in a country's criminal justice system because they violated anti-terrorism laws."

A tailored response requires an understanding of an individual FTF's motivations and proper risk assessment frameworks. In some cases, it may be more appropriate to rely on other administrative measures such as reintegration programs, travel bans, surveillance, or restrictions on access to the internet or particular locations in place of criminal prosecution. Factors officials may consider in making this determination include the risk of the returnee participating in a terrorist attack; the gravity of the returnee's offence; the availability of evidence; motivational factors; the returnee's age; the support network of family and friends; the impact on victims; and the public interest. Further, it may also be appropriate to implement custodial care or hospitalization for returnees with mental health issues.

- **Principle #6**: "Law enforcement can play an instrumental role in successful reintegration efforts."

Principle #6 underlines the important role of law enforcement in rehabilitation efforts, noting that: "[l]aw enforcement officials could prepare a community engagement plan to help obtain trust and goodwill within communities and support partnerships with local leaders and organizations. Train and educate all enforcement officials and officers to understand and address the complexities of reintegration efforts. Train program staff and professionals to distinguish signs of radicalization, respond appropriately to potential extremist threats, and communicate with FTF, their families, and other individuals engaged in reintegration programs in constructive ways that avoid conflict. It is important to remove stigma, remain professional, and ensure an FTF has support from family and community and does not become unduly dependent on individual

193 Hedayah and The International Institute for Justice and the Rule of Law, "The Malta Principles for Reintegrating Returning Foreign Terrorist Fighters" (2016).

program staff members. Countries could explain programs to all involved by conducting training sessions or meetings. Respecting the rule of law and preventing human rights' violations remains a key consideration and should not be confined to detention centers."

- **Principle #7**: "Reintegration programs should use a broad range of cross-disciplinary experts, with close coordination among relevant officials."

Principle # 7 stresses that rehabilitation strategies should be multidisciplinary. Psychologists, social workers, religious scholars, aftercare experts, youth services, mental health services, and, in particular, family members and community representatives, all play a critical role in contributing to a successful rehabilitation program. In this regard, government institutions and civil society should work together to carefully plan, structure, and coordinate these efforts to maximize program effectiveness.

3. The Madrid Guiding Principles (2015) and its Addendum (2018)

The 2015 Madrid Guiding Principles constitute a practical tool for Member States. This instrument consolidates best practices for stemming the flow of FTF, in accordance with UN Security Council resolution 2178 (2014). The enumerated principles are the product of a UN Security Council Counter-Terrorism Committee (CTC) special meeting, hosted by the Government of Spain in Madrid on 27 and

28 July 2015, alongside a series of related technical sessions organized by the Counter-Terrorism Committee Executive Directorate (CTED).

The CTC special meeting was attended by Member States from every region of the world, including those most affected by the FTF threat. Relevant international and regional organizations, academia, and civil society representatives also participated. Over the course of the meeting, participants identified a set of 35 guiding principles. The final document was eventually adopted by the UN Security Council in December 2015(S/2015/939).[194]

The 35 guiding principles are grouped into three themes:

- "Detection of, intervention against and prevention of the incitement, recruitment and facilitation of foreign terrorist fighters" (guiding principles n°1 to n°14).
- "Prevention of travel by foreign terrorist fighters, including through operational measures, the use of advance passenger information and measures to strengthen border security" (guiding principles n°15 to n°21).
- "Criminalization, prosecution, including prosecution strategies for returnees, international cooperation and the rehabilitation and reintegration of returnees" (guiding principles n°22 to n°35).

194 S/2015/939 (see footnote 57, Chapter 1).

With the erosion of ISIL (Da'esh) so-called "caliphate", the attention of the Security Council shifted to the evolving threat posed by returning FTF. In its resolution 2396 (2017), the Security Council requested the CTC, with the support of the CTED, to review the 2015 Madrid Guiding Principles in light of the evolving threat posed by returning FTF, and other principal gaps that may hinder States' abilities to appropriately detect, interdict, and where possible, prosecute, rehabilitate and reintegrate FTF returnees and relocators and their families, as well as to continue to identify new good practices. Consequently, a further special meeting of the CTC held on 13 December 2018 in New York, led to the development of the 2018 Addendum to the 2015 Madrid Guiding Principles. The 2018 Addendum proffers 17 additional good practices to assist Member States in their efforts to respond to the evolving FTF phenomenon.[195]

The 17 additional guiding principles of the Addendum espouses the following areas for intervention:

- "Border security and information sharing" (guiding principle n°1 to n°3).
- "Preventing and countering incitement and recruitment to commit terrorist acts consistent with international law; countering violent extremism conducive to terrorism and terrorist narratives; risk assessments and intervention programmes" (guiding principles n°4 and n°5).
- "Judicial measures and international cooperation" (guiding principles n°6 to n°14).
- "Protecting critical infrastructure, vulnerable or soft targets and tourism sites" (guiding principles n°15 to n°17).

E) The role of civil society and local communities

The United Nations Secretary-General's Plan of Action on Preventing Violent Extremism (A/70/674)[196] emphasizes the need for Member States to "develop joint and participatory strategies, including with civil society and local communities, to prevent the emergence of violent extremism". This call to create solid partnerships with civil society so as to deliver a rounded counter-terror approach has been addressed on a number of occasions by the international community:

- The United Nations Security Council, through resolution 1624 (2005), highlighted "the importance of the role of the media, civil and religious society, the business community and educational institutions in fostering an environment that is not conducive to incitement of terrorism."

195 *2018 Addendum to the 2015 Madrid Guiding Principles*, 28 December 2018 (S/2018/1177).

196 *Plan of Action to Prevent Violent Extremism, Report of the Secretary General*, 24 December 2015 (A/70/674).

- Resolution 2129 (2013) emphasizes the need to enhance partnerships with "international, regional and subregional organizations, civil society, academia and other entities in conducting research and information-gathering, and identifying good practices" and "underscores the importance of engaging with development entities."
- Finally, resolution 2178 (2014) encouraged Member States to "engage relevant local communities and non-governmental actors in developing strategies" to counter violent extremism. This is the first time countering violent extremism is mentioned in a resolution adopted under Chapter VII of the United Nations Charter.

Therefore, it is crucial that Jurisdictions of MENA consider cooperation and collaboration with civil society organizations and allocate appropriate resources thereto when drafting their own national plans to prevent and counter violent extremism.

2.2 The regional framework

Not all extraterritorial obligations and recommendations dealing with counter-terrorism and the FTF phenomenon apply across the globe. Some of them are region-specific. Consequently, States which belong to a particular region must not only refer to international instruments, but also to regional ones. In the context of the MENA region, the Counter-terrorism legal framework developed by both the League of Arab States (LAS) and the Organization of Islamic Cooperation (OIC) are pertinent.

A) League of Arab States counter-terrorism legal instruments

The League of Arab States (LAS) was established on 22 March 1945 as an intergovernmental organization and has a membership of 22 Arab nations.[197] Its founding instrument is the Charter of the Arab League (adopted 22 March 1945) which provides that the Organization's overarching objectives include the strengthening of relations between its Member States, the coordination of their policies in order to enhance cooperation, and the safeguarding of their independence and sovereignty. Its principal organs are the Council, the permanent Committees, and the Secretariat general.

In terms of the normative significance of its outputs - predominantly resolutions and statements - the LAS has no mechanism with which to enforce compliance with its resolutions. Indeed, even the Charter states that decisions reached by a majority "shall bind only those [States] that accept them."[198] In doing so, and as reflected in other key instruments, the organization is founded on the prevalence of national sovereignty with limited ability to take collective action including in relation to its own Membership. In part, this is attributable to regional political, historical, religious and so forth complexities. Additionally, historically, levels of adoption and implementation with

agreed LAS outputs and measures have generally been low in practice.[199]

Counter-terrorism instruments

The phenomenon of terrorism and FTF are not new to the geographical regions represented by the Organization's membership (the Middle East, Gulf and North Africa), though the form and source of such activities have varied. In response to the accompanying threats and needs for increased regional cooperation, an agreement was reached on the Arab Strategy to Combat terrorism (1997). The following year, LAS adopted its primary, binding, instrument against terrorism, the Arab Convention for the Suppression of Terrorism (adopted 22 April 1998, entered into force 7 May 1999).

The Convention is fairly broad, ranging in terms of the scope of topics that it includes. Compared with most other regional instruments, with the exception of the Organisation of Islamic Cooperation, it has a number of distinguishing features. One is that its underpinning principles include not only international law, but also "the tenets of the Islamic Sharia" (Preamble).

Another feature of the Convention is the "Criminal Justice Responses to Terrorism"[200] in relation to differing regional approaches to defining terrorism - is that it "[a]ffirm[s] the right of peoples to combat foreign occupation and aggression by whatever means, including armed struggle, in order to liberate their territories and secure their right to self-determination". Under this provision, persons engaged in these armed struggles shall not be deemed to have committed criminal offences under the Convention (article 2(a)).

There are a number of other features of the Convention which raise issues when considered from the perspective of the rule of law, international human rights and international humanitarian law obligations of individual Member States, and related normative standards. The drafting of the Convention is very broad, (e.g., in the definition of terrorism (Article 2), the concepts of "threat" and "violence" are not defined), and there is no reference within the Convention's text to international human rights law; instead reference is made only to the national law of the Convention's States parties - not all of whom are parties to applicable international human rights treaties - as well as the Convention itself. Indeed, concern has been expressed by some commentators about the potential effect which the implementation of the Convention within the national legal structures of Member States would have in relation to efforts to promote and strengthen domestic human rights reforms at a national level. Finally, it is noted that the Convention does not expressly affirm the international legal framework underpinning

199 Ibid.

200 «Counter-Terrorism Module 4». 2020. *UNODC*. https://www.unodc.org/e4j/en/terrorism/module-4/index.html.

the UN Global Counter-Terrorism Strategy, and its principles or goals. [201]

The principal activities of the League of Arab Statues include the convening of summits and issuing of recommendations to its Membership. For example, during the 26th Arab League Summit, held in Egypt in 2015, to discuss significant regional crises, including terrorism-related issues, a number of recommendations were adopted, including for the creation of a joint Arab military force to deal with challenges posed by extremist terrorist groups and FTF. Reflecting the inherent limitations of soft law resolutions, statements and so forth, it would seem that this recommendation has not been implemented to date.[202]

The Arab Convention for The Suppression of Terrorism 1998

Article 1:

1. **Terrorism:**

   "Any act or threat of violence, whatever its motives or purposes, that occurs in the advancement of an individual or collective criminal agenda and seeking to sow panic among people, causing fear by harming them, or placing their lives, liberty or security in danger, or seeking to cause damage to the environment or to public or private installations or property or to occupying or seizing them, or seeking to jeopardize a national resources."

2. **Terrorist offence:**

   "Any offence or attempted offence committed in furtherance of a terrorist objective in any of the Contracting States, or against their nationals, property or interests, that is punishable by their domestic law. The offences stipulated in the following conventions, except where conventions have not been ratified by the Contracting States or where offences have been excluded by their legislation, shall also be regarded as terrorist offences:

   a. The Tokyo Convention on Offences and Certain Other Acts Committed on Board Aircraft, of 14 September 1963;

   b. The Hague Convention for the Suppression of Unlawful Seizure of Aircraft, of 16 December 1970;

   c. The Montreal Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, of 23 September 1971, and the Protocol thereto of 10 May 1984;

201 "Counter-Terrorism Module 3". 2020. *UNODC*. https://www.unodc.org/e4j/en/terrorism/module-3/index.html.

202 Sheira, Omar, and Muhammed Ammash (2015). " Arab League Summit Report." *Global Political Trends Center Istanbul Kultur University*, April, no. 10.

d. The Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, of 14 December 1973;

e. The International Convention against the Taking of Hostages, of 17 December 1979;

f. The provisions of the United Nations Convention on the Law of the Sea, of 1982, relating to piracy on the high seas.

Article 2:

a. "All cases of struggle by whatever means, including armed struggle, against foreign occupation and aggression for liberation and self-determination, in accordance with the principles of international law, shall not be regarded as an offence. This provision shall not apply to any act prejudicing the territorial integrity of any Arab State."

Article 8:

"For purposes of the extradition of offenders under this Convention, no account shall be taken of any difference there may be in the domestic legislation of Contracting States in the legal designation of the offence as a felony or a misdemeanor or in the penalty assigned to it, provided that it is punishable under the laws of both States by deprivation of liberty for a period of at least one year or more."

Human rights instruments and mechanisms

No references are made to human rights in the Charter of the Arab League 1945 upon which the Organization is founded. This is unsurprising since the first international treaty to make such references was the United Nations Charter, which was adopted after the Charter of the Arab League. In subsequent instruments, indirect references to respecting international human rights standards were sometimes made by implication through commitments to respect the principles of the United Nations Charter.[203]

In 1968, the Council of the League created the Arabic Commission of Human Rights with promotion and educational mandate regarding human rights issues. Whilst its creation was an encouraging development for the furtherance of human rights within the region, its impact and influence are significantly constrained by the absence of any enforcement mechanism such as those exercisable by the Inter-American Commission

203 Almakky, Rawa Ghazy. The league of Arab states and the protection of human rights: a legal analysis. Diss. *Brunel University London*, 2015.

on Human Rights (IACommHR).[204]

Further evolution was the adoption by the Council of the League of Arab States of the Arab Charter on Human Rights on 15 September 1994 (never ratified by any of the Member States). Although the Charter guaranteed many important human rights and added some regional variations of its own, it failed to recognize many other rights and safeguards guaranteed in international human rights standards. The drafting of its provisions on substantive rights was also incomplete compared with the international human rights law treaty obligations ratified by many LAS Member States. For example, the Charter includes a prohibition on torture as "treatment" but does not clearly prohibit torture as "punishment", including corporal punishment. For these and other reasons, there was a significant concern, especially among non-governmental organizations, about the effect which the Charter would have on efforts to promote and strengthen internationally agreed human rights and humanitarian law instruments and normative standards within Member States.

In response to such criticisms and concerns, a revised Arab Charter on Human Rights was adopted on 22 May 2004, which entered into force on 15 March 2008.[205] Some elements of the Charter remained the same, such as the reaffirmation of the 1948 Universal Declaration on Human Rights and the 1990 Cairo Declaration on Human Rights in Islam (adopted 5 August 1990), which were controversial in relation to the 1994 Charter. The text of some important provisions remained unchanged, such as article 8(1) that "No one shall be subjected to physical or psychological torture or cruel, degrading, humiliating or inhuman treatment"[206], which once again omitted any reference to "punishment"; and the text of article 5 on the right to life remained very brief. Other provisions though, such as article 4 derogations, were more reflective of existing international human rights standards.

While both Charters provide for the provision of periodic reports from States parties to an expert Committee, they do not provide any mechanism for individual or State petitions to this Committee alleging violations of the Charter's provisions, nor any powers for monitoring or enforcing compliance by Member States.[207]

There has, however, been some progress towards the creation of an Arab Court on Human Rights, based in Bahrain, to address some of these gaps in enforcement mechanisms.[208] The Court's statute was approved by the Ministerial Council of the League of Arab

---

204 Resolution No. 2/06. On Guantanamo Bay Precautionary Measures . 28 July 2006.

205 "OHCHR Arab Charter on Human Rights". 2020. OHCHR. https://www.ohchr.org/EN/Issues/RuleOfLaw/CompilationDemocracy/Pages/ArabCharter.aspx.

206 Ibid.

207 Human Rights Watch (2012). " Civil Society Denounces Adoption of Flawed Human Rights Declaration: AHRD falls far below international standards." 19 November.

208 "Plan to establish Arab Court of Human Rights in final stage." Arab News (Saudi Arabia). 23 February 2016.

States on 7 September 2014, and during 2016 further revisions were being made to its text.[209] Some reservations have been expressed regarding the human rights compliance of the proposed Court, including the inability of victims to have direct recourse to the Court (only States parties, and NGOs that are both accredited in a State party and are specifically permitted to do so by that State, can bring cases before the Court), and regarding ensuring proper guarantees of the Courts and judicial independence and impartiality. There are, however, still many hurdles to be crossed before the planned Court comes into effect and operation. An ongoing attempt at creating an Islamic International Court of Justice - a concept first agreed in 1987 by the then Members of the Organization of Islamic Conference - has as not yet come into being.

The Revised Arab Charter on Human Rights 2004

Article 5:

1. "Every human being has the inherent right to life."
2. "This right shall be protected by law. No one shall be arbitrarily deprived of his life."

Article 8:

1. "No one shall be subjected to physical or psychological torture or to cruel, degrading, humiliating or inhuman treatment."

B) Organization of Islamic Cooperation

The Organization of Islamic Cooperation (OIC) was created in 1969. It is the second-largest inter-governmental organization after the United Nations with a membership of 57 States, including the State of Palestine, spread across four continents.[210] The OIC aims to safeguard and protect the interests of the Muslim world, in particular through strengthening solidarity and cooperation among its Member States.

Of its organs, the three of primary relevance for the OIC are the Islamic Summit (composed of Heads of State and Government), Council of Foreign Ministers, and the Independent Permanent Human Rights Commission. The most influential outputs, both politically and legally, are those of the Islamic Summit and Council of Foreign Ministers, which adopt numerous declarations, resolutions and communiqués, including on terrorism-related issues (particularly as political, and sometimes legal, resolutions).[211] Although these outputs are generally non-binding on the Members, they

209 Ibid.

210 Organisation of Islamic Cooperation (OIC) (2016(a)). **The OIC-2025 Programme of Action** . OIC/SUM-13/2016/POA-Final.

211 "OIC to Revisit Convention on Combating International Terrorism." 8 May 2016.

are nevertheless politically and diplomatically important and form an important part of the Organization's body of law.

The constitutional instrument of the OIC is its Charter. The original one was adopted during the Conference of Foreign Ministers, held in Jeddah from 29 February to 4 March 1972, but was subsequently revised and updated in 2008 during its Eleventh Islamic Summit held in Dakar on 13-14 March 2008 (changing its name from 'Organization of Islamic Conference', which suggested a looser confederation of States, to 'Organization of Islamic Cooperation'). As with the LAS, one of its distinguishing features is that it is underpinned by Islamic as well as international law principles.

Counter-terrorism instruments

The OIC has been actively engaged in terrorism-related matters throughout is existence, with many of its State Members having experienced different forms of terrorism. Among the identified priorities in the Organization's strategic programme, the OIC-2025 Programme of Action[212], are peace and security, counterterrorism, as well as human rights and good governance.

Its first key instrument was the adoption of the OIC Code of Conduct on Terrorism 1994.[213] Although the Code was political rather than legally binding in nature, it influenced the subsequent drafting of the Convention of the Organization of the Islamic Conference on Combating International Terrorism in 1999 (adopted 1 July 1999, entered into force 7 November 2002), which is the Organization's primary instrument against terrorism.

The Convention has a number of notable features. One is its article 2(a) exemption from the scope of the Convention's provisions of those engaged in what it considers to be legitimate armed self-determination struggles (as with the League of Arab States Convention). This is an important provision since the OIC, through Malaysia in 2005 and since has referred to this approach to defining terrorism in the context of ongoing efforts to agree on a universal definition of terrorism in the context of the draft Comprehensive Convention.

In terms of its influence, although the Convention technically came into effect on 7 November 2002, the broadness of some of its provisions risks hampering its effectiveness as a substantive instrument. Moreover, its effectiveness is affected by a low level of uptake and ratification from within its membership, requiring only seven of its total membership to ratify it in order to come into effect, although several more have become States parties since. Nevertheless, the Convention is an important legal source, including in terms of articulating the Organization's agreed institutional approach to

212 OIC to Revisit Convention on Combating International Terrorism." 8 May 2016.

213 Organisation of Islamic Cooperation (OIC) (1994). OIC Code of Conduct on Terrorism 1994 . 22 and ICFM. Res 43/22-P.

counter-terrorism and developing regional terrorism-related norms.

In recognition of these and other challenges that have been encountered in relation to the 1999 Convention, the Organization announced in 2016 its consideration of a proposal for additional protocols as well as updates to the provisions of the 1999 Convention to strengthen existing levels of cooperation. This would also better reflect new trends in terrorism such as cyber terrorism, terrorist financing, transboundary terrorist networks, and to underline the importance of respecting human rights in counter-terrorism responses.[214]

Organization of Islamic Cooperation Charter 2008

Article 1:

18. "To cooperate in combating terrorism in all its forms and manifestations, organized crime, illicit drug trafficking, corruption, money laundering and human trafficking;"

Organization of Islamic Cooperation, Programme of Action 2016

2.2 Counter-terrorism, Extremism, Violent Extremism, Radicalization, Sectarianism, & Islamophobia

2.2.1 Establish counter-terrorism partnerships with a view to strengthening international efforts to combat all aspects of terrorism and strengthen cooperation with States and international and regional organizations.

2.2.2 Revisit the Convention on Combating Terrorism adopted in 1999 to lay down proper mechanisms to counter the new trends of terrorism.

2.2.3 Formulate a new paradigm for inter-religious, inter-sectarian and intra-sectarian tolerance for promotion of understanding and moderation through dialogue and encourage initiatives of King Abdullah bin Abdelaziz Center for Interreligious and Intercultural Dialogue in this regard.

2.2.4 Combat Islamophobia, intolerance and discrimination against Muslims.

2.2.5 Encourage youth forums and programs to infuse values and combat extremism and all types of social evils.

2.2.6 Improve the utilization of ICT for countering the misuse of Cyberspace in terrorist acts and recruiting for terrorism purposes.

2.2.7 Counter the misuse of cyberspace for terrorism purposes, including recruitment and financing, and for cyber espionage campaigns by illegal organizations.

---

214 " OIC to Revisit Convention on Combating International Terrorism." 8 May 2016.

Human rights instruments and mechanisms

The OIC has been engaged in a number of human rights-related activities for some time, including in pursuit of its goal of promoting solidarity founded on shared Islamic values.

One of its principal instruments is the 1990 Cairo Declaration on Human Rights in Islam. Although not a legally binding instrument, it has proven to be influential, including within the context of the Organization's institutional human rights discussions, with the Declaration being affirmed regularly within the text of many of its resolutions as well as human rights-related treaty texts. An important lingering concern, however, is that the provisions of the Cairo Declaration may not fully reflect internationally agreed human rights standards, including the international treaty obligations of OIC Member States which have ratified international human rights conventions.[215]

A notable milestone towards better reflecting the underpinning legal principles of the United Nations Global Counter-Terrorism Strategy was the adoption of the revised Organization of Islamic Cooperation Charter 2008.[216] Its key objectives and underpinning principles include "to promote human rights and fundamental freedoms, good governance, the rule of law, democracy and accountability in Member States in accordance with their constitutional and legal systems" (Preamble); and "to uphold the objectives and principles of the present Charter, the Charter of the United Nations and international law as well as international humanitarian law while strictly adhering to the principle of non-interference in matters which are essentially within the domestic jurisdiction of any State."

Another significant development was the creation in 2008 of the Independent Permanent Commission on Human Rights, as an organ of the OIC, to "promote the civil, political, social and economic rights enshrined in the organization's covenants and declarations and in universally agreed human rights instruments, in conformity with Islamic values."[217] The Commission was formally launched with the adoption of its Statute by the 38th Session of the Council of Foreign Ministers held in Astana, Kazakhstan, on 28-30 June 2011. Its primary functions include promoting and advising upon human rights standards and principles, pursuing human rights agendas, capacity-building and educational activities, as well as technical legislative assistance to Member States. Notably, its approach is to undertake such activities "in conformity with the universally recognized human rights norms and standards and with the added value of Islamic principles of justice and equality". In terms of its key outputs, these largely take the form of reports.

---

215 Human Rights Watch (2012). " Civil Society Denounces Adoption of Flawed Human Rights Declaration: AHRD falls far below international standards." 19 November 2012.

216 Organisation of Islamic Cooperation (OIC) (2008). **Charter of the Organisation of Islamic Cooperation** .

217 Ibid.

As with a number of other regional human rights mechanisms, however, the Commission does not benefit from any systematic monitoring mechanisms, such as the periodic submission of Member States' reports, has no ability to receive and adjudicate on individual or States petitions regarding alleged human rights violations, and has no powers of enforcement.

Although article 14 of the 2008 Charter also predicted the imminent introduction of the International Islamic Court of Justice, first conceived by Kuwait in 1987, it has still not yet been possible to secure the necessary levels of political consensus to finalize the Statute and bring it into force, upon which the Court's existence is dependent. In any event, the Court will be concerned with inter-state disputes rather than individual complaints.

Chapter 3

Online investigation of offences related to foreign terrorist fighters

Training on online investigations and the collection of computer-based evidence has been identified as a priority in the investigation and prosecution of FTF during UNODC's assessment missions and training activities in MENA. Computers, mobile phones and the Internet are rapidly becoming one of the key features of modern terrorism investigations. Each can be used in the commission of a crime, can contain evidence of a crime, and can even be targets of crime.

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

- UNODC/CTED/IAP Practical Guide for Requesting Electronic Evidence Across Borders (January 2019);
- UNODC Train-the-trainer Module on Requesting Electronic Evidence Across Borders (to be published in 2020);
- UNODC publication: "The use of the Internet for Terrorist Purposes" (September 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" (4 November 2015);
- The United Kingdom Association of Chief Police Officers publication: "Good Practice Guide for Digital Evidence=" (March 2012);
- The United States Department of Justice publication "Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition" (2012).

All of the above-mentioned documents are available online and are referenced when relied on in the text.

The trend towards increased dependency on communication and data networks, storage of information within the cyber-domain, alongside a lack of robust mutual consent between countries on the effective control of operations in that domain, now presents new challenges to law enforcement and prosecutorial authorities in combating the threat posed by terrorism. Terrorists, being resourceful, creative and flexible, have been among the first groups to exploit these new technologies for criminal purposes.

Crimes involving electronic evidence present unique challenges for the law-makers,

investigators, prosecutors and judges entrusted to respond appropriately both domestically and at the level of international cooperation. Alarmingly, incidents of transnational crimes, enabled by globalization and technological advancement, are increasing. Once suspects are apprehended nearly all prosecutions depend, at least in part, on the use of electronic evidence, including location data, social media postings, text and email messages and records of cell phone calls. Moreover, almost all transnational cases involving terrorist activities, money-laundering, drug trafficking, human trafficking and migrant smuggling require evidence held in the servers of Internet Service Providers (ISPs).

The scale and volume of these crimes, the technical complexity of identifying the perpetrators, and where identified, the challenges of bringing them to justice remain issues of critical and urgent concern to the law enforcement community.

Further complicating matters in cases involving electronic evidence, there are also important variations between countries with regard to legal frameworks, internal procedures, government departments involved, capacity, practice and experience, as well as differences in the practices and level of cooperation of ISPs when receiving data requests from law enforcement. Given the volume and time-sensitive nature of these cases, real-time cross-border cooperation is essential in effectively preserving and collecting the electronic evidence necessary for criminal investigations and prosecutions, with due respect for human rights and the rule of law and in accordance with applicable standards of international law.

These issues are further exacerbated by the time-sensitive nature of electronic evidence, differences between legal systems, the clash of bureaucracies, the protection of sovereignty and, many times, the incapacity of law enforcement and nations to work together to overcome their differences.

In 2014, Charles Lister, a terrorism expert at the Brookings Institution, 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."[218]

In truth, the digital revolution is redefining all aspects of society, and crime is no exception. Criminals, including terrorists, exploit technology more and more in planning and committing offences. This means authorities need to increasingly rely

218 Sam Jones, "Jihad by social media", *Financial Times,* 28 March 2014.

on e-evidence for convictions. In the United Kingdom, for instance, the evidence used in court has included Skype conversations, photographs of training camps, as well as photographs taken in the Syrian Arab Republic on a mobile phone.[219]

At the apogee of ISIL (Da'esh) in Iraq and the Syrian Arab Republic, the spread of radicalization on social media was a serious cause for concern. Reports suggest that in 2015, the group controlled around 90,000 Twitter accounts targeting and recruiting young people into a war where hashtags became the new weapons.[220] Social media has empowered ISIL recruiting, helping the group draw at least 30,000 foreign fighters, from some 100 countries to the battlefields of Syria and Iraq. It has aided the seeding of new franchises in places ranging from Libya and Afghanistan to Nigeria and Bangladesh. ISIL spread a huge panic online. Immaculately staged photos, filtered through Instagram, had a strong impact to spread the fear. Armies of Twitter bots twisted small, one-sided skirmishes into significant battlefield victories. Hashtags were created and pushed (and others hijacked) to shape and hype the story.[221]

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 reported by a number of news outlets that ISIL (Da'esh) has released a manual, entitled "How to Tweet Safely Without Giving out Your Location to NSA", which purports to explain how to avoid surveillance.[222] Other examples of how technologically-competent Islamist terrorists have become include a number of applications developed by terrorists themselves, such as:[223]

- **"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"** (Security if the Mujahid) - an encryption software (released in December 2013) developed by the al-Fajr Technical Committee, a mainstream Al-Qaida organization. This software was accompanied by a

219 EUROPOL, "European Union Terrorism Situation and Trend Report 2015" (TE-SAT) (2015).

220 J.M. Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and describing the population of ISIS Supporters on Twitter", Analysis Paper No. 20 (Washington, D.C., Brookings Institution, March 2015).

221 Singer, Emerson. 2020. "War Goes Viral". *The Atlantic*.

222 Pierluigi Paganini, "Covert Communication Techniques Used by Next Gen High Tech Terrorists", Security Affairs, 12 May 2016.

223 Ibid.

28 pages instruction manual on encryption.

- **"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 distributor of the application 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.

Aside from propagandistic uses, these applications mainly serve to facilitate secure communications, thus making it increasingly difficult for authorities to monitor and disrupt terrorism-related activities.

Alongside these bespoke applications, there are also many proprietary software options and online techniques available to terrorists to facilitate online security. Applications such as Telegram and WhatsApp spring to mind. Studies have indicated communications through "normal" channels (email etc.) using secret encoding techniques such as steganography, and hidden watermarking may also remain options.[224]

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, inter alia, being a member of ISIL (Da'esh) and terrorist training. The convict had set up an online self-help guide for terrorists with techniques on encryption and ways to avoid detection from police and security services. He had also published instructional videos on how to secure sensitive data and remain anonymous online.[225] Some of the software include:

- **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.

---

224 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 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.

225 Bill Goodwin, "IS supporter Samata Ullah branded a 'new and dangerous breed of terrorist", *Computer Weekly*, 29 April 2017; see also "'Cufflink terrorist' Samata Ullah jailed for eight years", *BBC News,* 2 May 2017.

- **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, which is a web browser that is often referred to along with 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.[226]

ISIL (Da'esh) sympathizers continue to invest in resources promoting open source tools which ensure the anonymity of communication on sites (including some on the Darknet) in order to safeguard those accessing online terrorist propaganda.[227]

These matters become even more critical due to Covid-19. As the virus spread globally, new terrorist threats emerged. Far-right networks are reported to be preparing to take advantage of the possibility of social disorder. Groups affiliated with the Islamic State in Iraq and the Levant/Da'esh (ISIL) continue to use media platforms such as Telegram to incite the commission of offences by supporters in countries distracted by Covid-19, framing the pandemic as a divine reinforcement of their struggles.

3.1 Online investigations

The capability to effectively carry out online investigations is increasingly 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. It 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 "world wide 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: "Uniform Resource Locator" (URL); "Hypertext Transfer Protocol" (HTTP); and "Hypertext Markup Language" (HTML).

227 TE-SAT 2018, p.31 (see footnote 120, Chapter 1); see also EUROPOL, "Internet Organised Crime Threat Assessment (IOCTA) 2018" (2018), p.13.

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 connected device. This scheme is commonly referred to as the IP address, which can be compared to something like a postal code or a phone number. It allows a person to address a package and drop it in the system. Delivery of the package is guaranteed by the other part of the communication protocol, known as the "Transmission Control Protocol" (TCP). TCP is one of the main protocols in TCP/IP networks. Whereas the IP deals only with packets of data, the TCP enables two hosts to establish a connection and exchange streams of data. TCP not only guarantees delivery of data but also that the data packets will be delivered in the same order in which they were sent.

An IP address identifies a device and its location anywhere in the world. There are two versions of an IP address: "IPv4" and "IPv6".

"IPv4" was created in 1983 and used a 32-bit address scheme, allowing for the possibility of over 4 billion addresses. But the massive growth of the Internet and the number of connected devices means 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. At the time of writing, both IPv4 and IPv6 are operating simultaneously. In order to handle the problem of potential exhaustion of addresses, ISP assigns dynamic IPv4 addresses. This means that an IP address probably changes periodically - likely each time there is a connection to a different network. Devices that go offline relinquish their IP addresses so that they can be used by others. Basically, you rent but do not own your IP address. This significantly slows down the depletion of IPv4 addresses.[228]

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[229] and separated by colons. An example IPv6 address could be: **3ffe:1900:4545:3:200:f8ff:fe21:67cf**.

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

---

228 Paul Bischoff, "IPV6 vs IPV4: what are they, what's the difference, which is the most secure?", Comparitech, 11 January 2019.

229 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.

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 a static allocation:

- A static IP address is normally allocated, for instance, to a server providing a service such as a web page. Assigning a static (or permanent) address allows devices to return to that same location on the Internet.
- Dynamically assigned addresses are done through a process called "Dynamic Host Configuration Protocol" (DHCP). This protocol consists of 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.

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 is 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.

However, due to the finite number of IPv4 addresses, as discussed above, another technology employed by ISPs to address this shortage of IPv4 addresses could have serious implications for law enforcement investigations until the full availability of IPv6. "Carrier Grade Network Address Translation" (CGN) technologies are being used by IPS's to share one single IP address among multiple subscribers at the same time (several thousand). It has, therefore, potentially, become technically impossible for ISP's to comply with legal orders to identify individual subscribers. In a criminal investigation, an IP address is often the only information that can link the crime to an individual.[230]

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 six months, some for two months, and some for as little as 14 days. 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.

Gaining access to digital data, however, is not always straightforward as the data is often saved in another country. Within the European Union, new rules proposed by

230 For more information see: EUROPOL, "Are you sharing the same IP address as a criminal? Law enforcement call for the end of carrier grade NAT (CGN) to increase accountability online", press release, 17 October 2017.

the EU Commission are designed to speed up access to e-evidence saved in another Member State. These new rules would allow judicial authorities from one European Union country to directly request access to e-evidence from a service provider in another European Union country. This would fast-track the access request as there would be no need to go through the authorities in the other Member State.[٢٣١]

At the same time, police and judicial authorities may have easier access to cloud data in the United States as the EU Commission intends to negotiate with the United States Government on participation in the United States "Clarifying Lawful Overseas Use of Data"(CLOUD)Act2018.[232]

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.
- **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 across jurisdictions.
- **Open-source intelligence gathering (OSINT)** - this includes general research on the Internet. Such information is available to anyone sans the need for a surveillance authority, a subpoena or warrant.

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". In these circumstances, investigators should refer to their respective legislation for the appropriate authority to continue.

The investigator should always ensure that they are using an anonymous, stand-alone

231 Council of the European Union, "Better access to e-evidence to fight crime", available at: https://www.consilium.europa.eu/en/policies/e-evidence/.

232 Matthias Monroy, "European Commission wants to facilitate access to servers in the third states", 05 February 2019, available at: https://digit.site36.net/2019/02/05/european-commission-wants-to-facilitate-access-to-servers-in-third-states/'; Aravind Swaminathan et al. "The CLOUD Act, Explained", Orrick, 06 April 2018, available at: https://www.orrick.com/Insights/2018/04/The-CLOUD-Act-Explained.

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. A VPN user thus benefits 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 a 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."[233] TOR is 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 to the Internet.

It is highly desirable that investigators tasked with open-source investigations 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, thus hampering any future investigations.

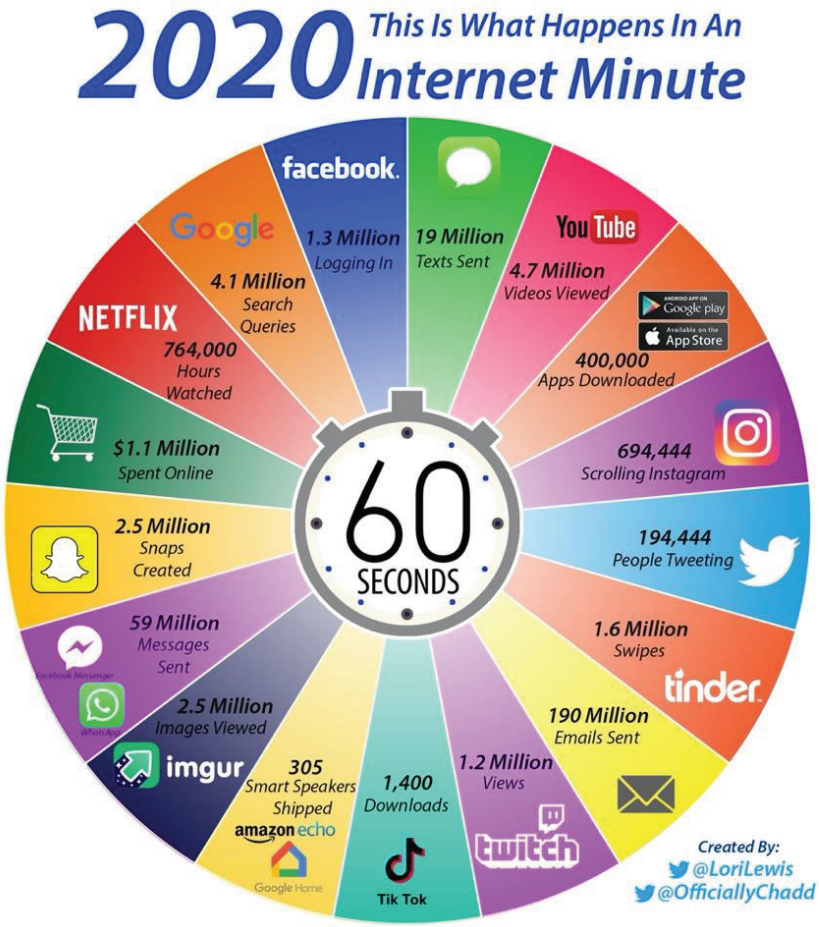
---

233 Johnathan D. Glater, "Privacy for People Who Don't Show Their Navels", *New York Times,* 25 January 2006.

Social media

Social media applications can be powerful tools for monitoring events and/or people for intelligence purposes. It should be stressed that 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 open-source intelligence should be treated with care. In practice, corroboration of OSINT is always desirable before executive action is considered.

The illustration below gives some idea of the challenges faced by investigators in terms of the volume of information available on social media alone. The figures show activity for one minute on the Internet.[234]



The use of the internet and social media for terrorism purposes should not be underestimated.

To give some idea of the scale of the challenge, 194,444 tweets in one minute equates to around 2.8 million tweets per day.

234 Lori Lewis, "Infographic: What Happens in an Internet Minute 2020", All Access, 10 March 2020.

To scale some of the above numbers to a monthly basis, there would be:

56,940,000,000 Facebook logins

179,580,000,000 Google searches

2,584,200,000,000 Facebook Messenger and WhatsApp messages sent, and

8,322,000,000,000 emails sent

Online Tools

There are other online search tools that are available to the investigator. These tools are 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.[235]
- **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.[236]
- **Research Clinic** - a free resource featuring internet research links, training, and apps in support of open source intelligence.[237]
- **OSINT Framework** - offers a flow-chart to help focus the gathering of information from free tools or resources.[238]
- **The Open Source Intelligence Tools and Resources Handbook 2018 -** offers a comprehensive list of tools to help investigators explore social media information.[239]

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"[240] and

---

235 For more information see the website of Intel Techniques, available at: https://inteltechniques.com/; N.B. There is also the possibility to pay a fee to gain fuller access to OSINT tools and training.

236 For more information see the website of NetBootCamp, available at: https://netbootcamp.org/osinttools/.

237 For more information see the website of Research Clinic, available at: http://researchclinic.net/.

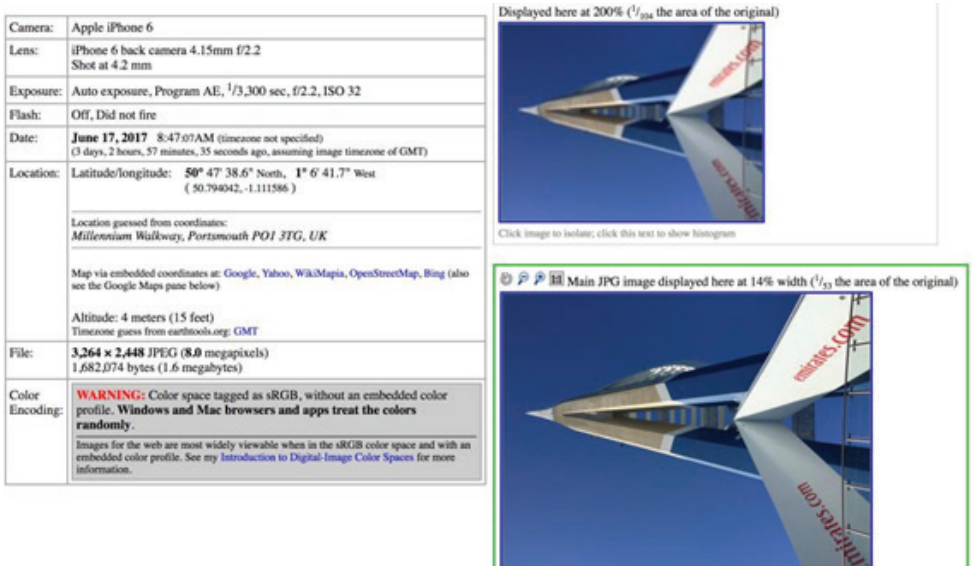
238 For more information see the website of OSINT Framework, available at: https://osintframework.com/.

239 Aleksandra Bielska et al, "Open source intelligence tools and resources handbook", I-intelligence (2018), available at: https://www.i-intelligence.eu/wp-content/uploads/2018/06/OSINT_Handbook_June-2018_Final.pdf.

240- For more information see the website of SocialMention, available at: http://www.socialmention.com/#.

"CheckUserNames"[241] 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 enable identification of where a picture was taken by looking inside its "Exchangeable Image File Format" (EXIF) data.[242] An example of how EXIF data is displayed using freely available online software is shown below:



Camera:	Apple iPhone 6
Lens:	iPhone 6 back camera 4.15mm f/2.2 Shot at 4.2 mm
Exposure:	Auto exposure, Program AE, 1/3,300 sec, f/2.2, ISO 32
Flash:	Off, Did not fire
Date:	**June 17, 2017** 8:47:07AM (timezone not specified) (3 days, 2 hours, 57 minutes, 35 seconds ago, assuming image timezone of GMT)
Location:	Latitude/longitude: **50°** 47' 38.6" North, **1°** 6' 41.7" West (50.794042, -1.111586) Location guessed from coordinates: *Millennium Walkway, Portsmouth PO1 3TG, UK* Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 4 meters (15 feet) Timezone guess from earthtools.org: GMT
File:	**3,264 × 2,448** JPEG (**8.0** megapixels) 1,682,074 bytes (1.6 megabytes)
Color Encoding:	WARNING: Color space tagged as sRGB, without an embedded color profile. **Windows and Mac browsers and apps treat the colors randomly.** Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

Note: EXIF information is deleted from photographs uploaded to Facebook but is often preserved on Twitter and Photobucket.

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 the name of the site and subject's name/nickname).
>
> Example - if you were to type into google the following:
>
> site: twitter.com "United Nations" says: "worldradioday"
>
> This will return a list of tweets from the United Nations official twitter site regarding World Radio Day

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

241 For more information see the website of CheckUserNames, available at: https://checkusernames.com/.

242 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.

places where they spend time. This a good source of additional leads and a chance to apply other investigative techniques. There are many social media platforms other than the more well-known names such as Facebook, Twitter or Instagram, some of them perhaps more obscure than others, but nevertheless worthy of consideration in open source intelligence gathering. The website "Social Media List" provides the top 200 networks, worldwide and is regularly updated.[243]

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 MENA jurisdictions vis-à-vis Internet use by June 2020 is set out in the table below[244]:

Jurisdiction	Internet usage/penetration (% of the population)	Facebook Users
Egypt	49,231,493/ 48.1 %	42,400,000
Iraq	21,276,000 / 52.9 %	22,030,000
Jordan	8,700,000 / 85.3%	5,755,000
Morocco	23,739,581 / 64.3 %	18,330,000
Saudi Arabia	31,856,652/ 91.5%	23,720,000
Tunisia	7,898,534/ 66.8 %	7,445,000
World	4,585,578,718/ 58.8 %	2,224,726,721

Privacy

Facebook enables users to choose their own privacy settings and who can see specific

243 For more information see the website of Social Media List, available at: https://socialmedialist.org/social-media-apps.html

244 See "Internet World Stats - Usage and Population Statistics", available at: https://www.internetworldstats.com/; Facebook penetration statistics were last updated in June 2020 (site accessed 11 June 2020).

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 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.

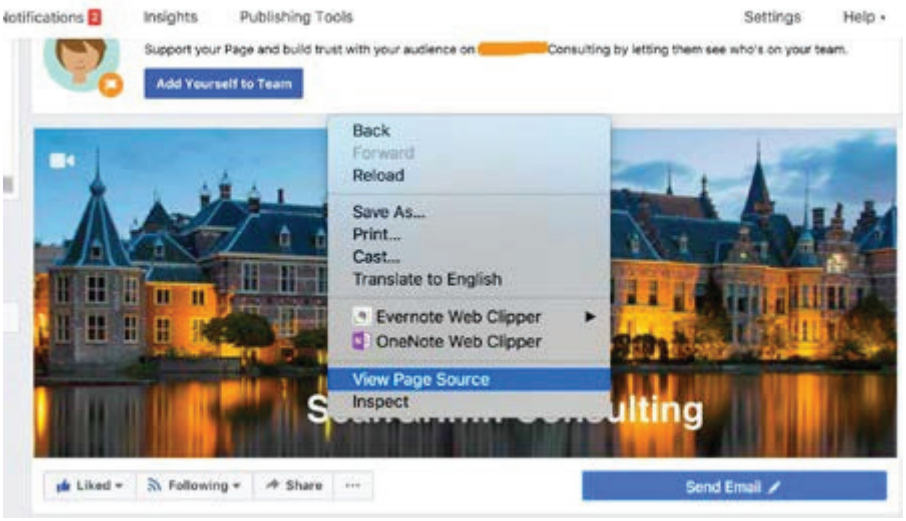
Facebook Graph searching

Following recent adverse publicity and data protection issues, Facebook has disabled the Graph search facility, making it more difficult to freely search for users of the site when only an email or telephone number is known.

However, using Facebook's own search engine, various pieces of information can be found. For example, people can access a list of publicly viewable photographs that 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 lives near Edinburgh, one can type "People named 'William' who live near Edinburgh, Scotland" in the Facebook search bar. There are also a number of other terms that may be used to trace a person, including:

- 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 proxies such as family members. Each person and every page on Facebook have 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 Facebook 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 HQ site:facebook.com

Images

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.[245]
- "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.[246]

Facebook itself provides guidelines for law enforcement officers on its website entitled "Information for law enforcement authorities". These guidelines outline procedures for investigators who may be seeking records from the website.[247]

Twitter

A 2014 investigation in the UK ("Operation Road") led to the first British conviction related to fighting in the Syrian Arab Republic. The subject of the investigation, Mashudur Choudhury, is reported to have been very active on Twitter, posting in the region 10,000 tweets (messages) and having 3,000 accounts listed as "followers".

Twitter is an online social networking service (micro-blog) that enables users to send and read short messages called "tweets". Registered users can read and post tweets, while those who are not registered can only read them. Users access Twitter through the website interface, SMS, or mobile device app. In 2020 Twitter had more than 262 million international users. Roughly 42% of Twitter users are on the platform daily.[248]

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.

Social media represents a powerful instrument in terrorist propaganda efforts, as demonstrated by a report in 2015 in which it was estimated that there were approximately 46,000 Twitter accounts operating on behalf of ISIL (Da'esh).[249]

245- See website of Tineye, available at: https://www.tineye.com/.

246- See website of Google images; available at: https://images.google.com/.

247- Facebook, "Information for law enforcement authorities"; Operational Guidelines. https://www.facebook.com/safety/groups/law/guidelines/

248- Omnicore, "Twitter by the Numbers: Stats, Demographics and Fun Facts", 15 June 2020, available at: https://www.omnicoreagency.com/twitter-statistics/.

249- Berger and Morgan, "The ISIS Twitter Census: Defining and describing the population of ISIS Supporters on Twitter" (see footnote 201).

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.
- **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,[250] many of which are provided therein a template for ease of use.

250 See "Twitter's Advanced Search", available at: https://twitter.com/search-advanced?lang=en-gb&lang=en-gb&lang=en-gb .

Basically, Twitter could be seen as an Internet version of mobile telephone SMS texts. Researching such a potentially vast number of messages and connections can seem a daunting task. The company (Twitter) does provide guidelines for investigators on procedures for seeking records.[251]

There are a number of free to use online tools available to assist investigations, including, for example:

- **Geosocial Footprint -** Enter a user name into the search box to see the location(s) from where the previous 200 tweets were posted.[252]
- **TweetBeaver -** provides useful, free Twitter analytics and allows investigators to search and download timelines and identify friends, followers, and Twitter IDs. Allows results to be downloaded into Excel files to assist further analysis.[253]

One useful tool for downloading and analysing the mass of data available on Twitter is **NodeXL**, which is simple but very thorough. 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 chosen period.

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**.[254]

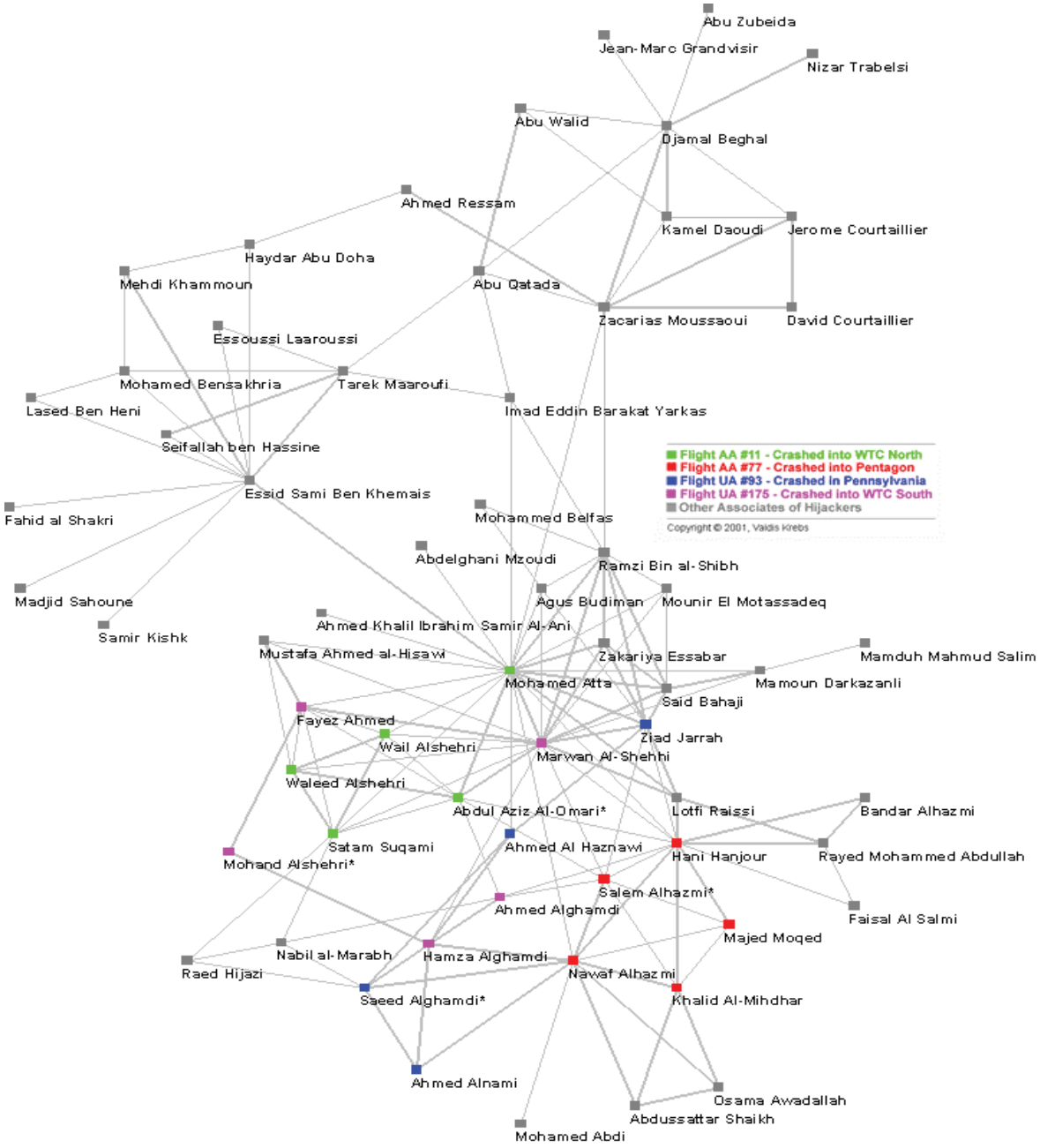
Alongside the analytical tools already discussed, there is also the possibility to use this mass data to map a social network ("Social Network Analysis" or SNA). SNA provides a visualization of a network and, through a series of algorithms, works out a particular person's place in his or her network. 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 directly reach?	In networks of music collaborations: How many people has this musician collaborated with?
Betweenness	How likely is this person to be the most direct route between two people in the network?	In networks of spies: Who is the spy though whom most of the confidential information is likely to flow?
Closeness	How quickly can this person reach everyone in the network?	In networks 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 networks 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 E. 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).[255]

His results come remarkably close to the actual position within the network for each of the hijackers.

255- Valdis E. Krebs, "Uncloaking Terrorist Networks", *First Monday,* vol. 7, No. 4 (1 April 2002).



All nodes within two steps/degrees of original suspects

What evidence to collect?

Reflecting on the 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; and information stored on computers, computer systems, thumb drives, flash drives, CDs, tapes and other digital media.[256]

- **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.[257]

- **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.[258]

Stored e-evidence	
Basic subscriber information (BSI)	The name of the subscriber/user and may include how long the subscriber has used that specific service and the Internet protocol (IP) address of the first login
Traffic data (non-content data)	• Metadata, which relates to the provision of services and includes data relative to the connection, traffic or location of the communication (for example IP or MAC addresses) • Access logs, which record the time and date an individual has accessed a service, and the IP address from which the service was accessed • Transaction logs, which identify products or services an individual has obtained from a provider or a third party (e.g., purchase of cloud storage space)
Content data	The body or text of an email, message, blog or post, videos, images, sound stored in a digital format (other than subscriber or metadata)[a]
Real-time collection of e-evidence	
Traffic data	Interception of who a subject is contacting and where from – for example static and dynamic IP addresses
Content data	Interception of the body or text of an email, message, blog or post, videos, images, sound stored in a digital format (other than subscriber or metadata)

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN page 43.

Categories of electronic evidence[259]

259- UNODC-CTED-IAP Practical Guide for Requesting Electronic Evidence Across Borders, United Nations, January 2019, page vii.

The raw message format of an email showing stored e-evidence[260]

In all instances, the investigation and prosecution of cases involving digital evidence require specialized 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 the domain 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 (IANA), where searches can be carried out by region through the Regional Internet Registries.[261]

Secondly, each site has a "WHOIS" function that allows investigators to identify

260 Ibid. page viii.

IP registration information.[262] 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 in fact behind the device to which the 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. Other online tools for tracing and investigating IP addresses include Network Tools[263] and Robtex.[264]

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). Alternatively, 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.[265] There are many tools freely available to assist, including:

i. HT Tracks;[266]

ii. Wget;[267]

iii. Wayback Machine - a website archive site;[268]

iv. Scrapbook - a "plug in" for Google Chrome and Firefox browsers.

Once a website has been captured or collected, an investigator will have access to a 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. An investigator can 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

---

262 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).

263 See website of Network Tools, available at: https://network-tools.com/.

264 See website of Robtex, available at: https://www.robtex.com/.

265 ACPO, "Good Practice Guide for Computer-Based Electronic Evidence" (see footnote 238).

266 See HT Tracks website, available at: http://www.httrack.com/.

267 GNU, "GNU Wget 1.20 Manual", 30 November 2018.

268 See Wayback Machine website, available at: https://archive.org/web/.

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[269] and a 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.[270]

For example, imagine that a person who is known to have been in the Syrian Arab Republic 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 the Syrian Arab Republic. The Facebook website would have left a cookie on the suspect's mobile phone (unless 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 the Syrian Arab Republic, possibly providing useful intelligence leads for further development.

Internet logs

Computer documents, emails, SMSs and instant messages, transactions, images and the Internet history 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

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

270 See "What are cookies?", available at: http://www.whatarecookies.com/.

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. 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).[271]

Encryption and anonymizing techniques employed in connection with other forms of the 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 and enforcement capabilities. Close coordination with local law enforcement may, therefore, be required to obtain key evidence for legal proceedings.[272] In such cases, competent national authorities should make use of the available tools for international cooperation, e.g. requesting Mutual Legal Assistance (MLA).[273]

Investigators should also consider referring to the UNODC document "Basic tips for investigators and prosecutors for requesting electronic/digital data/evidence from foreign jurisdictions"[274] which outlines a number of good practices. These practices include, 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 also be explored whether the formal requirements in the MLA procedures may be further differentiated depending on what data is requested (for example, whether it

---

271 See Hamstermap website, available at: http://www.hamstermap.com./.

272 UNODC, "The use of the Internet for Terrorist Purposes" (September 2012).

273 UNODC, "Manual on Mutual Legal Assistance and Extradition" (September 2012).

274 UNODC, *Basic tips for investigators and prosecutors for requesting electronic/digital data/evidence from foreign jurisdictions*, provided during 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.

is subscriber, traffic or content data).[275] 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.[276]

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

3.2 How to collect e-evidence?

The challenges facing law enforcement and prosecutors carrying out "digital" or online investigations are underlined in the European Union 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".[278]

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 practices in capturing ESI or Digital Evidence. Some of these good practices are listed below:

277 See International Association of Chiefs of Police (IACP), "Center for Social Media - Tools and Tutorials".

278 Council of the European Union, "Collecting E-evidence in the digital age - the way forward" (see footnote 255).

- Devices, peripherals and other materials may be collected once a crime scene has been secured, and 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.
- The mouse may be moved (without pressing buttons or moving the wheel) to determine if something is on the screen.[279]

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

279 ACPO, "Good Practice Guide for Computer-Based Electronic Evidence" (see footnote 238), p. 8.

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.

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 data forensics

Evidence handling is one of the most important aspects of 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").[280] However, this crucial piece of evidence 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.[281] 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.

---

280 See James Steele, Kevin O'Shea, Richard Brittson, Anthony Reyes, "Cybercrime Crime Investigations", Chapter 5: "Incident Response: Live Forensic and Investigations" (2011), available at: http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Incident-Response-Live-Forensics-and-Investigations.pdf.

281 ACPO, "Good Practice Guide for Computer-Based Electronic Evidence" (see footnote 238).

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.[282]

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.

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

282 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; for more information see https://www.webopedia.com/TERM/D/driver.html.

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 as possible. The investigator should consider including chargers for a variety of devices in their kit to facilitate this. Also, if 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 an "airplane" mode in order to disable Wi-Fi, Bluetooth or other communication systems. If the mobile device is switched on but locked, plugging it into 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,[283] or the 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 the 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. A 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.[284]

3.3 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:

Undercover activity 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

283 Aravind Swaminathan et al. "The CLOUD Act, Explained" (see footnote 213).

284 ACPO, "Good Practice Guide for Computer-Based Electronic Evidence" (see footnote 238), p. 13.

period of time by an undercover employee.[285]

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.[286]

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.[287]

Policies, procedures, and even legislation on the use of special investigative techniques differ from jurisdiction to jurisdiction, but there are several 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.
- Establish an evaluative process for these requests at the command level. Every request should be analysed to determine the investigatory purpose and the need for an undercover investigation.
- Maintain a record of all submitted requests, both approved and disapproved,

285 United States of America, Office of the Attorney General, *Guidelines on Federal Bureau of Investigation Undercover Operations* (Washington, D.C., 13

286 The United Kingdom, Home Office, *Covert Human Intelligence Sources - Revised Code of Practice*, (London, August 2018).

287 ACPO, "Good Practice Guide for Computer-Based Electronic Evidence" (see footnote 238), p. 13.

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.[288]

- The Chief of Police or deputy should establish protocols for documenting and recording investigations activity andcommunications.

- Ensure investigators are trained in how to set the 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.[289]

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

289 Michael D. Silva, "Undercover Online: Why Your Agency Needs a Social Network Investigations Policy", The Police Chief Magazine.

Annexes

List of international legal instruments related to terrorism and FTF

1. Instruments regarding civil aviation

1963 Convention on Offences and Certain Other Acts Committed on Board Aircraft

1970 Convention for the Suppression of Unlawful Seizure of Aircraft

1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation

1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation

2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation

2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft

2014 Protocol to Amend the Convention on Offences and Certain Acts Committed on Board Aircraft

2. Instruments regarding the protection of international staff

1973 Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons

1979 International Convention against the Taking of Hostages

3. Instruments regarding the nuclear material

1980 Convention on the Physical Protection of Nuclear Material

2005 Amendments to the Convention on the Physical Protection of Nuclear Material

4. Instruments regarding the maritime navigation

1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation

2005 Protocol to the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms located on the Continental Shelf

5. **Instruments regarding explosive materials**

1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection

1997 International Convention for the Suppression of Terrorist Bombings

1999 International Convention for the Suppression of the Financing of Terrorism

6. **Instruments regarding nuclear terrorism**

2005 International Convention for the Suppression of Acts of Nuclear Terrorism

7. **Relevant Security Council Resolutions**

Security Council resolution 1373 of 28 September 2001

Security Council resolution 2170 of 15 August 2014

Security Council resolution 2178 of 24 September 2014

Security Council resolution 2396 of 21 December 2017

8. **International Guiding Principles**

The Hague Marrakech Memorandum on Good Practices for a More Effective Response to the FTF Phenomenon (2014) and its Addendum (2015)

The Malta Principles for Reintegrating Returning Foreign Terrorist Fighters (2016)

The Madrid Guiding Principles 2015 and its Addendum (2018)

List of regional legal instruments related to terrorism and FTF

1. **League of Arab States**

The Arab Convention for The Suppression of Terrorism 1998

The Revised Arab Charter on Human Rights 2004

2. **Organization of Islamic Cooperation**

Organization of Islamic Cooperation Charter 2008

Organization of Islamic Cooperation, Programme of Action 2016

UNODC

United Nations Office on Drugs and Crime