UNODC
United Nations Office on Drugs and Crime

Foreign Terrorist Fighters

Manual for Judicial Training Institutes South-Eastern Europe

Updated Edition 2019

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

UNITED NATIONS OFFICE ON DRUGS AND CRIME
Vienna

Foreign Terrorist Fighters

Manual for Judicial Training Institutes South-Eastern Europe

Updated Edition
2019

UNITED NATIONS
Vienna, 2019

This handbook is a technical tool that has been developed for training purposes to support crime prevention and criminal justice practitioners in South-Eastern Europe.

This publication has not been formally edited.

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

Contents

Abbreviations

AQI	Al-Qaida in Iraq
CDCT	Council of Europe Committee on Counter-Terrorism
CGN	Carrier Grade Network Address Translation
CHIS	covert human intelligence source
CII	covert Internet investigator
CODEXTER	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 Counterterrorism Forum
GIMF	Global Islamic Media Front
GPS	Global Positioning System
HTML	Hypertext Markup Language
HTS	Hayat Tahrir al-Sham
HTTP	Hypertext Transfer Protocol
IACP	International Association of Chiefs of Police
IAEA	International Atomic Energy Agency
IANA	International Assigned Number Authority
IAP	International Association of Prosecutors
IIJ	International Institute for Justice and the Rule of Law
IP	Internet Protocol
ISP	Internet service provider
MILF	Moro Islamic Liberation Front
MLA	Mutual Legal Assistance

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
SEE	South-Eastern Europe
SIM	subscriber identity module
SNA	social network analysis
TCP	Transmission Control Protocol
TOR	The Onion Router
UNODC	United Nations Office on Drugs and Crime
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	virtual private network

Introduction

This updated edition of the UNODC publication "Foreign Terrorist Fighters. Manual for Judicial Training Institutes. South-Eastern Europe", which was issued in 2017, aims to reflect recent developments in the world, especially in South-Eastern Europe (SEE), related to foreign terrorist fighters (FTFs), and provide crime prevention and criminal justice practitioners in the region with the updated knowledge and skills to address new FTF-related challenges.[1]

Chapter 1 is expanded to elaborate on the FTF phenomenon and its evolution at the global and regional levels. It includes a section covering the developments in SEE and sections on the general FTF-related trends which largely draw upon earlier UNODC publications, such as "Investigation, Prosecution and Adjudication of Foreign Terrorist Cases for South and South-East Asia" (2018). Chapter 2 is updated to include details of the recent global and regional legal documents on countering and preventing terrorism with a focus on FTFs related aspects. For example, this chapter features Security Council resolution 2396 (2017), which addresses the risks posed by returning FTFs. The original publication covered only the earlier Security Council resolution 2178 (2014), which discussed FTFs' travel abroad to join terrorist groups. The updated chapter 3 responds to the requests from the SEE crime prevention and criminal justice practitioners to equip them with the updated information and tools for online investigations in terrorism cases. It provides examples of online search tools that are available to investigators for open source intelligence gathering (OSINT).

The original version of the manual was part of a UNODC project, launched in 2016, which covered Albania, Bosnia and Herzegovina, Montenegro, North Macedonia and Serbia, as well as Kosovo.[2] The project addressed the complex and interrelated challenges posed by FTFs to the criminal justice systems in the region. The UNODC project built upon continuous cooperation with counterparts from the region towards an effective and a sustainable legal regime against FTFs, founded in the rule of law, due process, and human rights. In the course of the project, the UNODC team visited and interviewed judges, prosecutors and managers and trainers of judicial institutes in the region. The work culminated in the production of the FTF training manual to be utilized by judges and/or prosecutors and incorporated into existing training courses delivered by national training institutes. Published in 2017, the manual attracted the attention of policymakers and practitioners concerned with the challenge of FTFs

[1] United Nations Office on Drugs and Crime, "Foreign Terrorist Fighters", Manual for Judicial Training Institutes South-East Europe, September 2017.

[2] All references to Kosovo in the present document should be understood to be in the context of the United Nations Security Council resolution 1244 (1999).

phenomenon.[3] It addressed the extent, structure and dynamics of the FTF phenomenon, the elements of FTF-related offences and investigations of FTF offences with special regard to online and financial investigations. The Government of the United States of America provided funding for the project, including the publication of the manual.

"Foreign Terrorist Fighters. Manual for Judicial Training Institutes. South-Eastern Europe / Updated Edition 2019" aims to preserve its relevance as a tool to be utilized by judges and prosecutors and incorporated into existing training courses delivered by national training institutes in the region. This updated edition is funded by the European Union.

[3] The webstory announcing the launch of the publication was the most visited webpage of UNODC in 2017.

I. 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.[4] 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.[5]

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 differing meanings of 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".*[6]

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 "FTFs", traces back to 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.[7]

A month later, on 24 September 2014, Security Council resolution 2178 (2014) was adopted to specifically tackle "the acute and growing threat posed by foreign terrorist

[4] David Malet, Foreign Fighters: *Transnational Identity in Civil Conflicts*, (Oxford, Oxford University Press, 2015). David Malet, "What does the evidence tell us about the impact of foreign fighters on home-grown radicalization", debate on 6 July 2015, available at https://www.radicalisationresearch.org/debate/malet-foreign-fighters-home-grown-radicalization/.

[5] Sebastiaan Faber, "Spain's Foreign Fighters", *Foreign Affairs* (September/October 2016).

[6] Geneva Academy of International Humanitarian Law and Human Rights, "Foreign Fighters under International Law", *Academy Briefing No. 7* (October 2014).

[7] United Nations, "Security Council Adopts resolution 2170 (2014) Condemning Gross, Widespread Abuse of Human Rights by Extremist Groups in Iraq, Syria", 15 August 2014, SC/11520.

fighters". The resolution emphasized the urgency of tackling the issue of FTFs, in particular those who had been recruited by and had joined ISIL (Da'esh), the al-Nusrah Front and "derivatives" of Al-Qaida.[8] Resolution 2178 (2014) also provided a helpful definition of FTFs:

> "[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*".[9]

In December 2017, the Security Council adopted resolution 2396 (2017) to reaffirm the definition of FTFs and call upon Member States to tackle the threat posed by FTFs returning or relocating from conflict zones.[10]

The definition adopted by the Security Council contains several elements, which should be highlighted. First, the 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.

Second, the Security Council definition applies regardless of whether the FTFs 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.[11]

Finally, FTFs also differ from mercenaries, who fight abroad on behalf of Governments or privately financed entities[12] and are "*motivated to take part in the hostilities essentially by the desire for private gain*".[13] Nevertheless, where financial and political or ideological interests significantly overlap, such individuals may fall within the scope of the definition of FTFs.

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 FTFs. A common conclusion emerged that there was no standardized profile of FTFs.

[8] Security Council resolution 2178 (2014) S/RES/2178.

[9] Ibid.

[10] 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.

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

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

[13] 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 wide 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.[14] While a large percentage of FTFs are young, economically disadvantaged males from socially or politically marginalized backgrounds,[15] there are many others with affluent backgrounds and well-educated. A report published by USAID states that, "some are school dropouts, others have graduate qualifications … some FTFs are itinerant workers, but others have successful professional careers as doctors, teachers, engineers and public servants."[16] Many FTFs have troubled pasts, but others would have enjoyed great prospects had they not subscribed to terrorist causes. Not all FTFs are pious, either. Furthermore, while some have criminal records (often for petty crime), 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.[17] 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 associations played a role in influencing prospective fighters. The average recruitment age dropped, with FTFs 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 FTFs or existing members of terror groups, but many travel without any prior contact with the terrorist organizations they seek to fight for. Others are groomed and facilitated in their travels by recruiters working online, including by FTFs who have already gone to the Syrian Arab Republic and subsequently encouraged their friends and acquaintances to do the same.

The June 2017 report from the European Union Radicalisation Awareness Network (EU-RAN) states: "… *[ISIL (Da'esh)] recruitment focuses on grooming techniques that exploit identity confusion and focus on persuasion, emotional manipulation and total obedience … recruiters identify individual psychological weaknesses and skilfully exploit these through online and offline techniques*".[18]

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

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

[15] 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).

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

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

[18] Radicalisation Awareness Network, "Responses to returnees: Foreign terrorist fighters and their families" (July 2017).

there is no online contact, the Internet enables potential recruits to view terrorist propaganda and discover terrorist narratives about the conflict, thus reinforcing decisions.[19] In a recent report by the United Nations Counter-Terrorism Executive Directorate (CTED) on the implementation of Security Council resolution 2178 (2014) in States affected by FTFs, the 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.[20]

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 a number of 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, while reinforcing the idea that Muslims should be living in a place where sharia is the supreme law guiding both political and 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 FTFs 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.[21]

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.[22] 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].[23]

---

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

[20] 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).

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

[22] Rebecca Gould, "The Islamic State's Perversion of Hijra", Project Syndicate, 11 August 2015.

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

- *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.[24]
- *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).[25] These prophesies 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 and Christians. Many FTFs viewed this as their chance to take part in the "battle to end all battles",[26] 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.[27]

While religion and ideology are typically treated as the main reason for enlisting, many FTFs recruited in both Europe and Asia were also attracted by the "thrill factor" and excitement of fighting in a foreign conflict.[28]

A common motivation cited in interviews of FTFs 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".[29] ISIL (Da'esh) propaganda, by contrast, offered an attractive

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

[25] Ibid.

[26] 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).

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

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

[29] 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).

message of belonging, purpose, brotherhood, adventure and respect.[30] Stated another way, FTFs could be categorized into four primary types:[31] "*The Revenge Seeker*": the frustrated and angry FTF seeks an outlet to discharge these emotions towards 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.

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

Case study: United Kingdom

Anjem Choudary, 49, was convicted in 2016 of inviting support for ISIL (Da'esh). Since 1999, he had been an organizer of extremist groups, giving speeches at public gatherings that were attended by impressionable young men, some of whom subsequently became radicalized and travelled abroad as FTFs or went on to commit terrorist acts in the United Kingdom. Choudary, a former solicitor, was always careful to stay within the boundaries of the law without crossing the criminal threshold in his speeches. However, he was judged to have crossed that line after posting speeches on YouTube propounding the caliphate established by ISIL (Da'esh) and asserting that for true Muslims, "*obedience to the caliph [al-Baghdadi] is an obligation*". Choudary was sentenced to imprisonment for five years and six months.[32]

Case study: 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.[33]

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

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

[32] Vikram Dodd, "Anjem Choudary jailed for five-and-a-half years for urging support of Isis", *The Guardian*, 6 September 2016.

[33] "Dutch court convicts nine for terror offences", *BBC News*, 10 December 2015.

1.3 Women and children

About one in five of those who have travelled to the Syrian Arab Republic from Europe is female, with even greater numbers of females making the journey from Asia, the Gulf States and North Africa.[34] 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, including children and grandparents, have migrated through a desire for a better life in ISIL (Da'esh)-held territory. 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.[35] There are many similar examples.

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 are 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*".[36] 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.[37]

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.[38] 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 undertake include teaching or nursing. However, one of the most important roles women 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 FTFs

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

[35] John Simpson, "All 12 of us are here: Luton family announce arrival in Isis held Syria", *The Times*, 4 July 2015.

[36] "From the battle of Al-Ahzab to the war of coalitions", Dabiq, Issue 11, available at https://clarionproject.org/docs/Issue%2011%20-%20From%20the%20battle%20of%20Al-Ahzab%20to%20the%20war%20of%20coalitions.pdf.

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

[38] 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).

encourage them to migrate, and facilitate their travel.[39] Whichever role they partake in, women FTFs 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.[40] In 2015, Jones issued a series of threatening messages on Twitter. Among other things, she called on Muslim women to launch terrorist attacks in the United Kingdom during Ramadan.[41] In June 2016, Jones was killed in a United States 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.[42]

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 FTFs for terrorism on the basis of their day-to-day support for their husbands. Other States do not consider such actions to be criminal in the absence of additional evidence of terrorist conduct.

Case study: 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 three years.[43]

While the conventional view is that women are less likely than men to engage in terrorist conduct, returning females still constitute a considerable risk. Researchers have found that women who join terrorist groups tend to be motivated by ideology. They

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

[40] 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).

[41] Alexandra Sims, "Sally Jones: Isis recruiter 'issues series of terror threats against UK cities' over Twitter", *The Independent*, 25 May 2016.

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

[43] 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.

see themselves as "part of a social movement" and are dedicated to the cause they believe in.[44] Transnational marriages bring the potential for future international collaboration among extremists.

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 FTFs 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 membership of ISIL (Da'esh).[45]

The average age of FTFs from the Western Balkans in the Syrian Arab Republic and Iraq is 31 for males and 30 for females. When compared to other areas of Europe, more women (36 per cent among Bosnians and 27 per cent among Kosovars, which is almost double the European average), joined men travelling to the Syrian Arab republic and Iraq. Compared to the European average, women and children (non-combatants) make up far greater (up to 55 per cent) of the Western Balkan people that travelled to the Syrian Arab Republic and Iraq.[46]

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.[47] Those born in conflict zones risk statelessness in cases where both parents are killed or imprisoned. Mothers may also try to claim the nationality of the father for their children.[48]

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.

---

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

[45] Rachel Roberts, "German teenage 'Isis bride' could face death penalty in Iraq", *The Independent*, 18 September 2017.

[46] 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.

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

[48] 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.

Boys as young as the age of nine, dubbed "cubs of the caliphate", have been trained to use weapons and taught to kill.[49] 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.[50] Classes included both militarization and indoctrination. Weapons and explosives training was coupled with religious instruction.[51] Once trained, children could perform support roles such as treating the wounded. Alternatively, they could act as spies, snipers and frontline fighters.[52] 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.[53] In 2016, a 12-year-old Indonesian boy who travelled to the Syrian Arab Republic to fight with ISIL (Da'esh) was reported killed in an airstrike.[54]

ISIL (Da'esh) is unique among terrorist groups in its brazen use of child soldiers, who were given a significant role in propaganda videos. Young boys, including the sons of FTFs, 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.[55]

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 to 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.[56] 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.[57] Not only have

[49] Richard Barrett, "Beyond the Caliphate: Foreign Fighters and the Threat of Returnees", The Soufan Center (October 2017).

[50] Ibid.

[51] 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.

[52] Ibid.

[53] 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).

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

[55] 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.

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

[57] Sidney Jones, presentation at UNODC Manila Workshop (November 2017).

children been taken to the conflict zones, large numbers were also born there to FTFs. 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."[58]

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."[59]

The mujahidin war in Afghanistan in the 1980s was the first modern conflict to see high levels of foreign fighter 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.[60] 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.[61] Yunos

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

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

[60] Maria Galperin Donnelly, Thomas M. Sanderson and Zack Fellman, "Foreign Fighters in History", Center for Strategic and International Studies, (Washington, D.C.), available at: http://foreignfighters.csis.org/history_foreign_fighter_project.pdf.

[61] 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).

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.[62] He is reported to have received military training in Afghanistan in the 1990s.[63]

- *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.[64]
- *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.[65]

The attacks of 11 September 2001 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.[66]

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 FTFs responded to Al-Qaida's rallying calls and joined local Sunni militants. These FTFs 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.[67]

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. FTFs volunteered to carry out most suicide bombings.[68] 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

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

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

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

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

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

[67] Ibid.

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

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[69] that soon became bolstered by an 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". 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 FTFs, but also lone women and families.

While the eyes of the world are on Iraq and the Syrian Arab Republic, FTFs 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 are unique.

1.5 Global situation

At its peak, about 10 million people were living in territory 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

[69] "Guide to the Syrian rebels", *BBC News*, 13 December 2013.

[70] "Islamic State and the crisis in Iraq and Syria in maps", *BBC News*, 28 March 2018. See also "Isis leader calls on Muslims to 'build Islamic state'", *BBC News* (1 July 2014).

[71] Noor Zahid, "Afghan Officials See Foreign Fighters Playing Key Role in Helmand Fighting", *Voice of America*, 14 August 2016.

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

[73] Daniel L. Byman, "What's beyond the defeat of ISIS?", Brookings Institution, 27 September 2016.

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 43,000 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) 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 (Libya, Yemen, Egypt-Sinai 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 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 fewer 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 Syrian Arab Republic and western Iraq. The Governments of Iraq and the Syrian Arab Republic both declared victory

---

[74] Paul Cruickshank, "A View from The CT Foxhole: Lisa Monaco, Former Assistant to President Barack Obama for Homeland Security and Counterterrorism", CTC Sentinel West Point, Volume 10, Issue 9 (October 2017). See also Radicalisation Awareness Network, "Responses to returnees: Foreign terrorist fighters and their families" (see footnote 17), stating that there are "42,000+ foreign terrorist fighters from 120+ countries".

[75] Schmid, "Foreign (Terrorist) Fighter Estimates: Conceptual and Data Issues" (see footnote 58).

[76] Daveed Gartenstein-Ross, "How Many Fighters Does the Islamic State Really Have?" War on the Rocks, 9 February 2015.

[77] Brett McGurk, *Letter to D-ISIS Coalition Partners on the Progress of the Past Year*, United States Department of State, Remarks of the Special Presidential Envoy for the Global Coalition to Defeat ISIS, (Washington, D.C., U.S. Department of State, 29 December 2017).

[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.

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. First, 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] Second, 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 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)

[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.

[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.

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]

What has happened to the fighters?

Research indicates that an estimated 14,910 FTFs have already left Iraq and the Syrian Arab Republic,[94] 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 killed or captured.[95] However, reports suggest considerable numbers were still able to evade death or capture. These FTFs could have left under the cover of civilian evacuations from cities such as Raqqa and subsequently used established people-smuggling routes to cross the border into Turkey.[96]

The FTFs currently in Iraq and the Syrian Arab Republic may have no option but to stay and fight. FTFs were overrepresented in the final battles for Mosul and Raqqa. Many are currently being tried in Iraqi courts[97] or in the custody of the Syrian Democratic Forces (SDF). Some, according to the Coalition, are moving into areas controlled by the Syrian Government.[98]

> "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."[99]

Not all FTFs 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 FTFs 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.[100]

For FTFs 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 FTFs in their ranks. A movement of escaping fighters

---

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

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

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

[96] Hannah Lucinda Smith, "Surge of Isis fighters set to hit mainland Europe, Turkey warns", *The Times*, 5 December 2017.

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

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

[99] 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.

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

to these ISIL (Da'esh) provinces has already been reported.[101] Other terrorist groups affiliated with ISIL (Da'esh), such as in the Philippines, may also welcome FTFs from the Syrian campaign.

The large flow of refugees and asylum seekers from conflict zones raises the risk that FTFs will try to use the refugee system or migrant-trafficking routes, either to escape prosecution[102] 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.[103] 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.[104] 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.[105]

Al-Qaida

While fear of an attack by ISIL (Da'esh) is the highest-ranked concern of the public and of Governments globally,[106] the threat of other terrorist organizations should not be forgotten. In particular, Al-Qaida seeks to make a comeback. Al-Qaida is making plans towards its "*strategic objective … to incite the umma to undertake a global jihad to defend Muslims*", and will seek to fill any vacuum left by ISIL (Da'esh).[107]

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 officials as the Khorasan Group – was to coordinate with the Yemen-based Al-Qaida in the Arabian Peninsula to sneak explosives onto civil aviation.[108] 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.[109]

---

[101] 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.

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

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

[104] "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.

[105] 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.

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

[107] 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.

[108] "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).

[109] "What is the Khorasan Group?" (see footnote 107).

Al-Qaida continues to be a significant worldwide threat, with its regional offshoots conducting mass-casualty attacks.[110] 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.[111] In an attempt to expand its sphere of influence, in 2017, Al-Qaida announced a new affiliate in Jammu and Kashmir.[112] As it has done historically, the organization continues to recruit and utilize the services of FTFs. 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 home lands. Outside of the Western countries, he urges Muslims to rise up against "tyranny".[113]

In the Syrian Arab Republic, 20 per cent of FTFs are estimated to have gone to militant groups other than ISIL (Da'esh),[114] 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*",[115] 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*".[116] In 2017, it announced an alliance with four smaller factions to form Hayat Tahrir al-Sham (HTS), or Liberation of the Levant Organization.[117]

Many analysts view the Jabhat Fateh al-Sham element of the alliance "*as a covert Al-Qaida affiliate*",[118] 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 occupy the "*largest Al-Qaida safe haven since 9/11*"[119] in Idlib province in the north of the Syrian Arab Republic. Standing to profit both politically and militarily from any

[110] 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).

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

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

[113] 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).

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

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

[116] Ibid.

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

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

[119] 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.

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.[120] The number of FTFs that remain with HTS is unknown. If HTS starts to suffer losses, these FTFs may also seek to return home.

1.6 Regional situation in South-Eastern Europe

According to Europol's 2018 report on the terrorist threat in the European Union,[121] one of the main threats to the jurisdictions of South-Eastern Europe (SEE) is FTFs returning to their country of origin. It is estimated that around 1000 persons from SEE have travelled to Iraq and the Syrian Arab Republic between the end of 2012 and 2017 (women and children constituted almost 35 per cent of this group), and around 300 have already returned.[122]

Most FTF contingents came from Kosovo, Bosnia and Herzegovina, Albania and North Macedonia, and those areas are now particularly exposed to the threats posed by returnees. Although the region has not suffered from any attack conducted by returning combatants, returnees raise serious security concerns, not only to SEE but also to the rest of Europe. Some FTFs from SEE hold dual citizenship and/or have links to diaspora communities across the continent.

Furthermore, according to the Organized Crime Threat Assessment (OCTA) SEE 2018 conducted by the Southeast European Law Enforcement Center (SELEC), terrorism "remains a serious threat" in the region and appears primarily linked not only to the returning FTFs, but also to individuals who self-radicalize and may commit lone-wolf attacks.[123] Two such deadly attacks were carried out in Bosnia and Herzegovina in 2015. In addition, in November 2016, security forces in Albania and Kosovo thwarted an attempted attack targeting the Israeli national soccer team during a World Cup match in Shkodër, northern Albania's second-largest city.

Historic perspective of the FTF phenomenon

The recent influx of foreign fighters to Iraq and the Syrian Arab Republic is not a new phenomenon in SEE. In the 1990s, the post-Cold War fragmentation of the Socialist Federal Republic of Yugoslavia proved to be a magnet for foreign fighters. Thus, SEE was among the active suppliers of ISIL (Da'esh) warriors, and there were previous waves of demand for the warriors from the region. It is estimated that up to 5,000 foreign fighters, mainly drawn from veterans of the Afghan war, participated in the civil war in Bosnia Herzegovina (1992–1995). There, they formed a unit of the Bosnian Army known

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

[121] Europol, "European Union Terrorism Situation and Trend Report 2018" (TE-SAT) (2018).

[122] Vlado Azinović, "Regional Report: Understanding Violent Extremism in the Western Balkans", Extremism Research Forum, British Council, June 2018.

[123] Southeast European Law Enforcement Center, Organized Crime Assessment for Southeast Europe 2018 (SELEC OCTA 2018).

as "El Mujahedin".[124] Some of the same foreign fighters also returned to take up arms in the 1998 Kosovo War.[125] In both conflicts, some individuals and groups sought to exploit ethno-religious distinctions to promulgate violent extremist ideologies.

At the onset of the civil war in the Syrian Arab Republic, volunteers from SEE felt obliged to join the conflict to help their "fellow Muslims" in need. Most of the fighters from SEE 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 SEE to the conflict zones presents a unique challenge for the region. The geographical proximity of SEE to Turkey facilitated travels between the two areas. From Turkey, individuals seeking to join ISIL (Da'esh) could cross the Syrian border with the help of operatives.[126] Flows between SEE and the Syrian Arab Republic reached their peak in 2013 and early 2014, when 70 per cent of the SEE contingent regularly travelled back and forth.[127]

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 FTFs 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.[128] Furthermore, it became harder for FTFs 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.

The following table lists persons (adult men and women, as well as children) from the six jurisdictions of SEE who are reported to have travelled to Iraq and the Syrian Arab Republic from 2012 to 2017.[129]

Jurisdiction	Total adults	Men	Women	Children
Albania	109	96	13	31
Bosnia and Herzegovina	240	177	63	57
Kosovo	303	255	48	95
Montenegro	23	18	5	4
North Macedonia	154	140	14	No data

[124] Malet, *Foreign Fighters: Transnational Identity in Civil Conflicts* (see footnote 3).

[125] Aida Ćorović, "Radicalization in Serbia: The Youth of Sandžak between a Hammer and an Anvil", in Vlado Azinović ed., "Between Salvation and Terror: Radicalization and the Foreign Fighter Phenomenon in the Western Balkans", Atlantic Initiative (2017).

[126] Ibid.

[127] Azinović, "Regional Report: Understanding Violent Extremism in the Western Balkans" (see footnote 121).

[128] Ibid.

[129] Ibid.

Serbia	49	37	12	10
Total	**878**	**723**	**155**	**197**

Source: Vlado Azinović, "Regional Report: Understanding Violent Extremism in the Western Balkans", *British Council*, June 2018.

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 Belgium, both Bosnia and Herzegovina and Kosovo appear to have a higher rate of citizen engagement in the fighting in Iraq and the Syrian Arab Republic. In fact, the population of Belgium is around 11,370,000 and there have been approximately 498 Belgian foreign fighters, or 44 FTFs per one million inhabitants. The populations of Bosnia and Herzegovina and Kosovo are around 3,530,000 and 1,780,000 respectively, and they have contributed some 240 and 303 citizens (men and women) to the foreign fighter contingent to Iraq and the Syrian Arab Republic. This makes the rate of foreign fighters from Bosnia and Herzegovina around 68 per one million inhabitants, and from Kosovo 170 per one million inhabitants. This is much higher than the Belgian number, which is cited as the highest in the European Union.[130]

Patterns of radicalization and recruitment

Radicalization and recruitment efforts by violent extremist groups pose a significant long-term challenge to the security of SEE. The Islamic tradition among Muslim communities in the region is generally oriented towards the Hanafi school of thought within Sunni Islam. Hanafi interpretations and practices are different from more conservative counterparts in the Arabian Peninsula. This, however, has not prevented some actors from exploiting socio-economic disenfranchisement, lack of trust in state institutions, and other internal factors to promulgate 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 SEE. 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/economical marginalization. In the context of SEE, "push factors" which have been identified as contributing to the radicalization process include economic deprivation, perceived corruption, and political and institutional dysfunction.[131]

> "Taking advantage of economic hardship and the profound failure of governments to improve living conditions, radical Islamic movements also began to provide public services ranging from helping the poor to supporting hospitals and schools. Meanwhile radical imams began to provide something akin to life coaching, and

[130] Ibid.

[131] Ibid.

> in some towns, dormitories opened to provide accommodation to poor students and spread Salafist and Takfirist ideas. In the eyes of certain segments of the impoverished populations of the Balkans, the representatives of these Islamic organizations began to have more credibility than government institution."[132]

Mobilization of FTFs in SEE appears to be more successful in jurisdictions where Muslim populations are a relative minority. This may be explained by the possibility of relative minorities being more amenable to narratives of Muslim persecution and victimhood.[133]

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 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 FTFs 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.[134] 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 South-Eastern Europe.

Case study: Kosovo

Kosovo presents an interesting case study for the drivers of radicalization. On the "push" side, social alienation, especially among young individuals between the ages of 18 and 25, has been pointed to as one of the most significant risk factors of violent extremism. In particular, the capital, Pristina, has been identified as a locus for at-risk communities.[135] Contrary to popular belief, there does not appear to be a correlation between certain measures of education (school attendance, literacy rates, and access to educational resources) and the likelihood of radicalization.[136] Instead, contributing factors which have been identified include the individual's immediate socio-economic conditions, structural issues such as the level of unemployment, and a sense of detachment from the mainstream social fabric.

On the other hand, "pull factors" are largely facilitated by organized cells which, through an assiduous exploitation of political ideology and religious beliefs, target individuals for radicalization. These cells typically seek to promulgate narratives of Muslim victimhood, and these narratives may have particular resonance in Kosovo in light of fresh

[132] Predrag Petrović, "Islamic radicalism in the Balkans", European Union Institute for Security Studies, June 2016.

[133] Ibid.

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

[135] Shpend Kursani, "Kosovo Report", Extremism Research Forum, British Council, April 2018.

[136] Ibid.

memories of the Yugoslav Wars.[137] As with other areas in South-Eastern Europe, another "pull factor" is the existence of Middle Eastern charities seeking to disseminate religious ideologies which sanction violence under the veneer of humanitarian work.[138]

Estimated figures of returnees and profiles

As ISIL (Da'esh) lost control of its territory, there were warnings that home countries should prepare for a flood of FTF returnees. However, the number of returnees, if still worrisome, has been much smaller than anticipated.[139] Estimates indicate that 30 per cent of FTFs have returned home or moved to a third state.[140] In the context of SEE, as of January 2019, the United Nations Analytical Support and Sanctions Monitoring Team estimated that around 300 of the nearly 1,000 FTFs have already returned, while 100 are reported as killed.[141] FTFs training and experience, for instance, handling weapons and explosives, but also their contacts make them exceptionally dangerous.[142]

Europol, in its 2019 report on the terrorist threat in the European Union, indicates that the Western Balkans and European Union countries such as Bulgaria, Hungary and Romania, were used as transit countries. Whereas the pressure of migrant flows towards the European Union stabilized in 2018, the continued use of smuggling routes, including through Western Balkan countries, remained a matter of concern from a counter-terrorism perspective.[143]

The following table lists the number of adult returnees from Iraq and the Syrian Arab Republic to South-Eastern Europe from 2012 to 2017:

Jurisdiction	Adults who have returned from the Syrian Arab Republic and Iraq
Albania	40
Bosnia and Herzegovina	50
Kosovo	130
Montenegro	9
North Macedonia	80
Serbia	10
Total	**319**

Source: Vlado Azinović, "Regional Report: Understanding Violent Extremism in the Western Balkans", *British Council*, June 2018

[137] Asya Metodieva, "Why do Foreign Fighters Join Islamic State? The case of Kosovo", Strategic Update, LSE IDEAS, December 2018.

[138] Ibid.

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

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

[141] *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*, 15 January 2019 (S/2019/50).

[142] TE-SAT 2019 (see footnote 139).

[143] Ibid.

The motivations for FTFs 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 FTFs, each presenting a different level of risk.[144]

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 FTFs 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 FTFs, 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 FTFs may seek even more extreme stimulus on return.
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 much 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 FTFs.

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

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

regard, there is a significant number of European returnees who departed from the Syrian Arab Republic before ISIL (Da'esh) established itself as a "caliphate" in 2014. Unlike FTFs, 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.[145] 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 over time 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.

Likelihood of terrorist attacks from returning FTFs

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. FTFs 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.[146]

Returnees may also maintain networks which they formed with other terrorists during their time abroad.[147] 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 Europe is the existence of operational connectivity between ISIL (Da'esh) and the perpetrators. Of the 42 terrorist attacks against the "West" between 2014 and 2016, 38 involved some connection between ISIL (Da'esh) and the perpetrators.[148]

However, the security threat posed by FTF returnees must not be overestimated. According to Europol, the attacks in the European Union have been primarily committed by homegrown terrorists who did not travel abroad to join terrorist groups.[149] 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 London Bridge in 2017. These terrorists were

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

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

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

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

[149] TE-SAT 2018 (see footnote 120).

able to cause significant casualties without relying on firearms and despite having no combat experience. Thus, in the context of Kosovo, the Kosovar Center for Security Studies had noted, "fresh terrorist sympathizers carry more potential and capabilities to undertake terrorist attacks compared to foreign fighters who returned from Syria and Iraq."[150]

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."[151] In this regard, the profiles of FTF returnees are heterogenous. 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 have not received training in violent combat or committed violent crimes. On return, some have disengaged entirely from any association with violent extremism. Reports of former FTFs actively contributing to efforts to prevent violent extremism exist too.[152] It would consequently be inappropriate to treat all FTF returnees as would-be attackers.

The threat of attacks being carried out by FTFs can consequently be classified as high-impact and low-probability.[153] Research reveals that only 18 per cent of attacks carried out in the "West" between June 2014 and June 2017 were by known FTFs. However, the attacks conducted by returnees also tend to be among the most lethal, with an average of 35 deaths per attack.[154] 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 United Nations Analytical Support and Sanctions Monitoring Team has assessed the threat of FTFs plotting attacks in SEE as "medium to low".[155] There are several factors which may contribute to this assessment. First, it is generally believed terrorist groups will find more propagandistic value in attacking Western European targets over South-Eastern European ones.[156] Second, the death of major ISIL (Da'esh) figures in the region, such as Almir Daci from Albania and Ines Midzic from Bosnia and Herzegovina, has left a leadership vacuum for their supporters in the region.[157] Third, among domestic groups with extremist views, available evidence suggests they lack an organized network structure and tend to be factionalized by different religious

[150] Skender Perteshi, "Beyond the Triggers: New Threats of Violent Extremism in Kosovo", Kosovar Centre for Security Studies (KCSS), August 2018.

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

[152] Ibid.

[153] Ibid.

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

[155] S/2019/50 (see footnote 140).

[156] Ebi Spahiu, "Returning IS Fighters in the Balkans: Beyond the Immediate Security Threat", The Jamestown Foundation, 18 May 2018.

[157] Ibid.

and ideological beliefs.[158] The recent history of domestic terrorist attacks in SEE appears to bear out the United Nations Analytical Support and Sanctions Monitoring Team's analysis. Since 2012, jurisdictions of SEE have witnessed only two isolated lone-actor attacks in Bosnia and Herzegovina (both in 2015) aimed at police and armed forces.

Nevertheless, the risk of terrorist attacks still exists. In 2016–2017, the authorities in Kosovo reported four terrorist plots, all of which were foiled.[159] Furthermore, the possibility of a major terrorist attack in the region became apparent in November 2016, when security forces in Albania and Kosovo thwarted an attempted attack targeting the Israeli national soccer team during a World Cup qualifying match in Shkodër, northern Albania's second largest city. The plot was reportedly coordinated by Lavdrim Muhaxheri and Ridvan Haqifi, Kosovo Albanian ISIL (Da'esh) leaders who were operating in Iraq and the Syrian Arab Republic until their deaths in 2017. In total, 19 people were arrested across Albania, North Macedonia, and Kosovo. The operation was an example of strong collaboration between regional intelligence agencies and international partners.[160]

Between 250 and 300 returnees from SEE who left ISIL (Da'esh) between 2014 and 2015 seem to have done so owing to disillusionment with the war and disheartenment with the infighting between jihadist groups.[161] 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*."[162] 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 SEE, a key challenge remains to be the deciphering and monitoring the intention of FTF returnees.

[158] TE-SAT 2018 (see footnote 120).

[159] Arife Muji, "Reintegration of returning foreign fighters: what approach best suits Kosovo?", KCSS, April 2017.

[160] Perteshi, "Beyond the Triggers: New Threats of Violent Extremism in Kosovo" (see footnote 149).

[Die] Morina, "Lavdrim Muhaxheri, ISIS Warrior, Remains Threat to Kosovo", *Balkan Insight*, 18 November 2016.

[161] Spahiu, "Returning IS Fighters in the Balkans: Beyond the Immediate Security Threat" (see footnote 155).

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

II. 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 50 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 protection of international staff. These instruments are complemented by the Security Council resolutions to prevent and counter terrorism. Collectively, these instruments create obligations for Member States under international law, whereby Member States must implement these obligations under their national laws.[163] The implementation of these conventions, protocols and resolutions is informed by the guidance provided by the United Nations Global Counter-Terrorism Strategy along with 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 European context are developed in this chapter.

A. Security Council resolutions 1373 (2001), 2178 (2014) and 2396 (2017)

A number of Security Council resolutions have 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. Security Council resolution 1373 (2001)

Agreed and adopted in the wake of the 11 September terrorist attacks in the United States, resolution 1373 (2001)[164] provided the impetus for a series of international

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

[164] Security Council resolution 1373 (2001) S/RES/1373.

instruments targeting terrorism and violent extremism. Reaffirming its earlier unequivocal condemnation of these attacks,[165] 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. 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).[166] 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 armed conflict.*"[167]

Furthermore, resolution 2178 (2014) called upon Member States to enhance their criminal justice responses to FTFs by introducing measures to detect, prevent and criminalize the travel of FTFs and related activities. These measures can be broadly divided into three categories: criminal laws, sanctions and preventative 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 frameworks. Sanctions regimes suppress and debilitate the capacity of individual FTFs 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 FTFs or ter-

[165] Security Council resolution 1368 (2001) S/RES/1368.

[166] S/RES/2178 (see footnote 7, chapter 1).

[167] Ibid.

rorists 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. 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 FTFs. These offences cover the following three aspects:

- travel or attempted travel of FTFs
- financing the travel of FTFs
- organizing or facilitating (including recruitment) the travel of FTFs

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 FTFs 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 embargoes. Travel bans are of particular importance for disrupting the travel of FTFs 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 FTFs 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 successfully prosecute and secure a conviction.

Security Council resolution 2396 (2017)

In December 2017, the Security Council unanimously adopted resolution 2396 (2017).[168] While the subject focus of that resolution is on FTFs, it is principally concerned with risks posed by FTFs returning from conflict zones, in marked contrast with resolution 2178 (2014), which focused on FTFs headed outbound. Resolution 2396 (2017) calls upon Member States to strengthen their efforts to stem the threat emanating from returning and relocating FTFs 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 FTFs. 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 FTFs. It also stresses the responsibility of Member States to share information and investigate individuals, even when suspects are foreign nationals.

[168] Security Council resolution 2396 (2017) S/RES/2396.

Furthermore, Member States are called upon to develop and implement comprehensive risk assessments for returning and relocating FTFs 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 FTFs, who may be victims of terrorism. In this regard, it encourages Member Stages 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 are used by and shared with all competent national authorities.

B. United Nations Global Counter-Terrorism Strategy

In addition to Security Council resolutions, the United Nations Global Counter-Terrorism Strategy provides a framework to address the FTF phenomenon. This strategy was adopted by the General Assembly on 8 September 2006[169] 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

[169] General Assembly resolution 60/288 (2006) A/RES/60/288.

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

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 key 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 General Assembly to reflect changing priorities. From 26 to 27 June 2018, the General Assembly held its sixth biennial review of the United Nations Global Counter-Terrorism Strategy. This review concluded in the adoption of General Assembly resolution 72/284[170] by consensus. Regarding the risks related to returning FTFs, resolution 72/284 notably:

[170] General Assembly resolution 72/284 (2018) A/RES/72/284.

- Called upon Member States to strengthen their cooperation at the international, regional, sub-regional and bilateral levels to counter the threat posed by FTFs, 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 Security Council resolution 2396 (2017); and
- Called upon law enforcement and criminal justice authorities to better address the threat of returning FTFs.

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 FTFs, they represent a major component of the international *corpus juris* against terrorism and provide an important framework for international cooperation in terrorist/FTFs cases. In this regard, many legally binding 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 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 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

C. 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[171] is an initiative launched in 2014 by Morocco and the

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

Netherlands within the framework of the Global Counterterrorism Forum (GCTF).[172] 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 good practices focus on several aspects of the responses to the FTF threat, including:

- Detecting and intervening against violent extremism (good practices no.1 to no.5)
- Preventing, detecting and intervening against recruitment and facilitation (good practices no.6 to no.9)
- Detecting and intervening against travel and fighting (good practices no.10 to no.14)
- Detecting and intervening upon return (good practices no.15 to no.19)

In 2015, an Addendum to this Memorandum[173] focusing on returning FTFs was adopted. The Addendum provides 7 recommendations,[174] 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
- 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.*"

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

The Malta Principles for Reintegrating Returning Foreign Terrorist Fighters[175] 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

[172] The GCTF is an informal, multilateral counter-terrorism platform launched in 2011 to assist in the implementation of the United Nations Global Counter-Terrorism Strategy. The GCTF has six Working Groups, of which one concerns Foreign Terrorist Fighters.

[173] 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).

[174] (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."

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

Member States in their policies and programmes on the reintegration of returning FTFs. Some principles are worth highlighting here:

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

Principle 3 emphasizes that engagement with returnees should be individualized. Consequently, reintegration programmes "*should be designed with individuals in mind, whether they serve FTFs 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 programmes, 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 programme staff and professionals to distinguish signs of radicalization, respond appropriately to potential extremist threats, and communicate with FTFs, their families, and other individuals engaged in reintegration programmes 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 programme staff members. Countries could explain programmes 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 centres.*"

Principle 7: *"Reintegration programmes 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 programme. In this regard, government institutions and civil society should work together to carefully plan, structure, and coordinate these efforts to maximize programme 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 FTFs, in accordance with Security Council resolution 2178 (2014). The enumerated principles are the product of a 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 Security Council in December 2015 (S/2015/939).[176]

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 no.1 to no.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 no.15 to no.21)
- "*Criminalization, prosecution, including prosecution strategies for returnees, international cooperation and the rehabilitation and reintegration of returnees*" (guiding principles no.22 to no.35)

With the erosion of the ISIL (Da'esh) so-called "caliphate", the attention of the Security Council shifted to the evolving threat posed by returning FTFs. 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 FTFs, 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.[177]

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

- "*Border security and information sharing*" (guiding principle no.1 to no.3)

[176] S/2015/939 (see footnote 57, chapter 1).

[177] *2018 Addendum to the 2015 Madrid Guiding Principles*, 28 December 2018 (S/2018/1177).

- "*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 no.4 and no.5)
- "*Judicial measures and international cooperation*" (guiding principles no.6 to no.14)
- "*Protecting critical infrastructure, vulnerable or soft targets and tourism sites*" (guiding principles no.15 to no.17)

E. The role of civil society and local communities

The Secretary-General's Plan of Action on Preventing Violent Extremism (A/70/674)[178] 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 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."
- 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 SEE 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 SEE, the legal framework developed by both the Council of Europe and the European Union are pertinent.

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

B. Council of Europe counter-terrorism legal instruments

The Council of Europe was founded in 1949, currently has 47 Member States, and is the oldest intergovernmental organization in Europe. The organization principally aims to promote and uphold human rights, parliamentary democracy and the rule of law. It is located in Strasbourg (France) and should not be confused with the separate (though closely connected) system of the European Union, which has its political arm based in Brussels (Belgium).

The Council of Europe has developed key legal standards to prevent and suppress acts of terrorism. Its principal counter-terrorism framework treaty is the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol. The Council of Europe Committee on Counter-Terrorism (CDCT) (formerly called the Committee of Experts on Terrorism (CODEXTER))[179] is the key coordinating body for Council of Europe activities to combat terrorism. CDCT's primary objectives are to oversee and ensure the successful implementation of relevant Council of Europe legal instruments in the counter-terrorism field, and in particular, the Convention on the Prevention of Terrorism and its Additional Protocol.

1. The Convention on the Prevention of Terrorism (2005) CETS No. 196

Following the September 2001 attacks in the United States, the Council of Europe formed a working group to review its counter-terrorism legislation and began work on the Convention on the Prevention of Terrorism in 2003. After a number of meetings, the CODEXTER drafted the Council of Europe Convention on the Prevention of Terrorism, which was adopted on 16 May 2005 in Warsaw (Poland) and entered into force on 1 June 2007.[180]

This Convention does not define new terrorist offences in addition to those included in the existing conventions against terrorism. However, it creates three new offences which may lead to terrorist offences as defined in those conventions. These new offences are: "*public provocation to commit a terrorist offence*" (article 5); "*recruitment for terrorism*" (article 6); and "*training for terrorism*" (article 7). They are coupled with a provision on accessory (ancillary) offences (article 9) providing for the criminalization of complicity (such as aiding and abetting) in the commission of all of the three aforementioned offences. In addition, attempts to commit an offence are criminalized under articles 6 and 7 (recruitment and training).[181]

One of the characteristics of the new crimes introduced by the Convention is that conviction does not require the actual commitment of a terrorist offence within the

[179] The Committee of Experts on Terrorism (CODEXTER) was an intergovernmental body coordinating the Council of Europe's action against terrorism. It drafted the Council of Europe Convention on the Prevention of Terrorism and a number of important soft law instruments. In 2018, the CODEXTER became the Council of Europe Counter-Terrorism Committee (CDCT).

[180] Council of Europe, Council of Europe Convention on the Prevention of Terrorism, *Council of Europe Treaty Series No. 196* (16 May 2005).

[181] Council of Europe, Explanatory Report to the Council of Europe Convention on the Prevention of Terrorism, *Council of Europe Treaty Series No. 196* (16 May 2005), paras. 32 and 33.

meaning of article 1 (i.e., any of the offences within the scope of and as defined in one of the international treaties against terrorism listed in the appendix). This is explicitly stated in Convention article 8, which is itself based on an equivalent provision in the International Convention for the Suppression of the Financing of Terrorism. The place where such an offence is committed is also irrelevant for the purposes of establishing the commission of any of the offences set forth in articles 5 to 7 and 9. In addition, these offences must be committed unlawfully and intentionally, as is explicitly stated in each article:[182]

Article 5 – Public provocation to commit a terrorist offence:

(1) "For the purposes of this Convention, 'public provocation to commit a terrorist offence' means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed."

(2) "Each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law."

Article 6 – Recruitment for terrorism:

(1) "For the purposes of this Convention, 'recruitment for terrorism' means to solicit another person to commit or participate in the commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group."

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

Article 7 – Training for terrorism:

(1) "For the purposes of this Convention, "training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence, knowing that the skills provided are intended to be used for this purpose."

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

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

Article 9 – Ancillary offences:

"Each Party shall adopt such measures as may be necessary to establish as a criminal offence under its domestic law:

a) Participating as an accomplice in an offence as set forth in Articles 5 to 7 of this Convention;

b) Organizing or directing others to commit an offence as set forth in Articles 5 to 7 of this Convention;

c) Contributing to the commission of one or more offences as set forth in Articles 5 to 7 of this Convention by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either:

i. be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of an offence as set forth in Articles 5 to 7 of this Convention; or

ii. be made in the knowledge of the intention of the group to commit an offence as set forth in Articles 5 to 7 of this Convention."

(1) "Each Party shall also adopt such measures as may be necessary to establish as a criminal offence under, and in accordance with, its domestic law the attempt to commit an offence as set forth in Articles 6 and 7 of this Convention."

2. *Additional Protocol to the Council of Europe Convention on Prevention of Terrorism (2015) CETS No. 217*

Following the unanimous adoption by the Security Council of resolution 2178 (2014), in which the Security Council called on Member States to take a series of measures aimed at preventing and curbing the flow of FTF to conflict zones, CODEXTER proceeded to examine the issue of radicalization and FTFs. The result of these discussions eventually led to the drafting of the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (2015) CETS 196.[183]

The main objective of the Additional Protocol is to address criminal law aspects of the phenomenon of FTFs and returnees. The Protocol, which opened for signature on 22 October 2015 in Riga and entered into force on 1 July 2017, requires Parties to criminalize taking part in an association or group for the purposes of terrorism, receiving terrorist training, travelling abroad for the purposes of terrorism, and financing or organizing travel for terrorist purposes. Following from the Additional Protocol, the

[183] Council of Europe, Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, *Council of Europe Treaty Series No. 217* (22 October 2015).

CDCT also oversees a network to facilitate the rapid exchange of relevant police information concerning terrorist fighters suspected of travelling to or from Member States.

The offences set forth in the Protocol, like those in the Convention, are mainly of a preparatory nature. These offences are: Participating in an association or group for the purpose of terrorism (article 2); Receiving training for terrorism (article 3); Travelling abroad for the purpose of terrorism (article 4); Funding travelling abroad for the purpose of terrorism (article 5); and Organizing or otherwise facilitating travelling abroad for the purpose of terrorism (article 6).[184]

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

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

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

Article 3 – Receiving training for terrorism:

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

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

Article 4 – Travelling abroad for the purpose of terrorism:

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

[184] For a more detailed account of the background to the Protocol see Council of Europe, Explanatory Report to the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, *Council of Europe Treaty Series No. 217* (22 October 2015), paras. 2-12.

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

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

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

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

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

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

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

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

In addition to criminal offences, parties to the Convention and its Additional Protocol are encouraged to take measures to foster national and international cooperation. Regarding national cooperation, Article 3 (2) of the Convention underlines that "*Each Party shall take such measures as may be necessary to improve and develop the co-operation among national authorities with a view to preventing terrorist offences and their negative effects*" by, among other things, "*exchanging information*"; "*improving the physical protection of persons and facilities", and "enhancing training and coordination plans for civil emergencies.*"

To strengthen international cooperation, parties to the Convention are encouraged to "assist and support each other with a view to enhancing their capacity to prevent the commission of terrorist offences, including through exchange of information and best practices, as well as through training and other joint efforts of a preventive character" (Article 4), "afford one another the greatest measure of assistance in connection with criminal investigations or criminal or extradition proceedings" (Article 17), and to extradite or submit the case without undue delay to its competent authorities for the purpose of prosecution (Article 18). Of a particular relevance to FTFs is Article 7 of the Additional Protocol, which requires each Party "to strengthen the timely exchange between Parties of any available relevant information concerning persons travelling abroad for the purpose of terrorism." For that purpose, each Party shall "designate a point of contact available on a 24-hour, seven-days-a-week basis."

3. The Council of Europe Counter-Terrorism Strategy for 2018–2022

In addition to developing legal standards to prevent and suppress acts of terrorism through criminal laws and other measures, the Council of Europe through the CDCT, works to help Member States fight terrorism more effectively by strengthening their national legislation and facilitating international cooperation.

In response to the evolving terrorist threat in Europe, the Committee of Ministers of the Council of Europe has tasked the CDCT to draw up the Council of Europe Counter-Terrorism Strategy for 2018–2022.[185] The Strategy is based on the Council of Europe legal framework and standards. It sets out a series of actions and tools to assist Member States which can be summarized as "the three P's" – "Prevention", "Prosecution", and "Protection":

- **Prevention:** preventing terrorism both through criminal law and law enforcement measures aimed at disrupting terrorist attacks or their preparation and through multifaceted longer-term measures aiming at preventing radicalization leading to terrorism, including countering recruitment, training, the dissemination of terrorist ideology and the financing of terrorism.
- **Prosecution:** ensuring that terrorist offences committed in Europe or abroad are investigated in the most efficient and quickest possible manner through effective judicial and international cooperation, including the principle of aut dedere aut iudicare,[186] and ensure that those responsible are brought to justice and answer for their acts, in compliance with human rights and the rule of law.
- **Protection:** protecting all persons present on the territories of the Member States against terrorism, providing for the security of the people and the protection of potential targets of terrorist attacks, including critical infrastructures and public spaces; providing assistance and offering support to victims of terrorism.

[185] Council of Europe CDCT, Council of Europe Counter-Terrorism Strategy (2018-2022), CM (2018)86-addfinal (4 July 2018).

[186] Legal principle requiring States to extradite or to prosecute a person sought by another State in order to avoid impunity for serious crimes.

In each of these three main strands, concrete activities to be undertaken by Member States in the framework of the Council of Europe in the period 2018–2022 have been identified to further improve Member States' ability to prevent and combat terrorism while respecting human rights, the rule of law, and democracy.

In addition, the Strategy indicates working methods as well as expected outcomes and outputs for every proposed activity. In order for the Strategy to remain a living instrument, it will be reviewed every 18 months, or as appropriate, with the possibility of adjustments under the guidance of Member States.

B. European Union counter-terrorism legal instruments

In addition to the Council of Europe, States which are members of or seeking accession to the European Union should also refer to the latter's instruments. Regardless of whether a State is a European Union Member State or not, there is value in taking guidance from the European Union's counter-terror instruments.

The European Union is a separate institution from the Council of Europe, but it is closely connected since all of its Member States are also Member States of the Council of Europe. The organization has a number of institutions. The ones which play the most significant role in relation to the development of counter-terrorism related laws and policies are the European Parliament, the European Council, and the European Commission. The European Parliament is the lawmaking body of the European Union. Parliament passes laws, together with the European Council, based on proposals of the European Commission. The primary role of the European Council is to set the organization's political agenda. It is essentially the European Union decision-making body rather than lawmaker. The European Commission, for its part, is the politically independent executive arm of the European Union. It draws up proposals for new European legislation and implements the decisions of the European Parliament and the European Council. Additionally, together with the Court of Justice, the Commission ensures that European Union law is properly applied in all Member States.[187]

Following the Madrid terrorist attack in March 2004, the European Union leaders also adopted a declaration[188] which established the position of a European Union Counter-Terrorism Coordinator. The Coordinator's principal roles include coordinating the work of the Council in combating terrorism; presenting policy recommendations and proposing priority areas for action to the Council; as well as facilitating international cooperation, including between the European Union and third countries.

While the European Union asserts that the primary responsibility in the fight against terrorism lies with Member States, it plays an important supporting role that helps respond to the cross-border nature of the threat. The European Union notably provides

[187] UNODC, Education for Justice (E4J) University Module Series: Counter-Terrorism, "Module 5: Regional Counter-Terrorism Approaches, European Region", July 2018.

[188] Council of the European Union, Declaration on combating terrorism, 7906/04 (29 March 2004).

an important framework to facilitate the coordination of national policies, information-sharing, and the determination of good practices. The issues of radicalization and FTFs have been regular items on the agenda of the Union institutions, which have in turn developed a comprehensive approach to tackle the issues of FTFs and home-grown terrorism.

1. The European Union Counter-Terrorism Strategy (2005)

The European Union's counter-terrorism responses are framed around the European Union Counter-Terrorism Strategy (EUCTS), adopted by the European Council in November 2005.[189] It commits the European Union to combating terrorism globally, while respecting human rights and allowing its citizens to live in an area of freedom, security, and justice. While influential, the EUCTS is technically non-binding. The Strategy is built around four main strands:

"Prevent" people from turning to terrorism by addressing the factors and root causes which can lead to radicalization and recruitment, in Europe and internationally.

Under this first pillar, and as part of the EUCTS, the Council adopted the "EU strategy for combating radicalization and recruitment to terrorism" in 2008. The text was revised in June 2014 in light of how terrorism in Europe evolved over the 21st century, notably the phenomena of lone-actor terrorism, returning foreign fighters, and the use of social media by terrorists.[190] While the bulk of measures to combat radicalization and recruitment exist at the national level, the revised European Union strategy contains joint standards and measures grouped under three key headings: disrupt the activities of individuals and networks that draw people into terrorism; ensure that voices of mainstream opinion prevail over those of extremism; and promote security, justice, democracy, and opportunities for all more vigorously. In December 2014, the Council adopted guidelines for the implementation of the revised strategy by Member States, which have been revised in 2017.[191]

In order to promote actions empowering communities and key groups that are engaged in the prevention of terrorist radicalization and recruitment, the European Commission established an European Union-wide Radicalization Awareness Network (EU-RAN). This network connects key groups (researchers, social workers, religious leaders, youth leaders, policemen etc.) involved in countering violent radicalization across the European Union.

[189] Council of the European Union, European Union counter-terrorism strategy, 14469/4/05 REV 4 (30 November 2005).

[190] Council of the European Union, Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism, 9956/14 (19 May 2014).

[191] Council of the European Union, Revised Guidelines for the EU Strategy Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism, 10855/17 (30 June 2017).

"Protect" citizens and infrastructure by reducing vulnerabilities against attacks.

The second pillar notably includes securing external borders, improving transport security, protecting strategic targets, and reducing the vulnerability of critical infrastructure.

For instance, under the second pillar, the European Council adopted on 27 April 2016 a Directive regulating the use of PNR data[192] for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. According to the European Union law, the Member States were required to put into force the laws, regulations, and administrative provisions necessary to comply with the Directive within two years of its adoption. In line with the directive, air carriers are obliged to provide Member States' authorities with the PNR data for flights entering or departing from the European Union. It also allows, but does not oblige, Member States to collect PNR data concerning selected intra-European Union flights.

Another concrete example falling under the protection pillar is the adoption by the European Commission in 2017 of the "Action Plan on the protection of public spaces".[193] This Action Plan aims to step up support for European Union countries' in reducing the vulnerability of public spaces.

Protective measures by the European Union also extend to acts preparatory to terrorism. Another key area of activity of the Union in the counter-terrorism field has been the fight against money-laundering and terrorist financing. In 2015, the European Parliament and the European Council adopted the Directive 2015/849, which established common rules on the prevention of money-laundering or terrorist financing through the European Union's financial system.[194]

Additionally, as part of its response against terrorism after the 9/11 attacks, the European Union established in December 2011 a list of persons, groups, and entities involved in terrorist acts. The list includes persons and groups active both within and outside the European Union. The list is reviewed by the Council regularly, at least every six months. Common position 2001/931/CFSP lays down the criteria for listing persons, groups and entities. It identifies the actions that constitute terrorist acts for these purposes and defines the restrictive measures to be applied. The Working Party on the implementation of Common Position 2001/931/CFSP on the application of specific measures to combat terrorism ("CP 931 Working Party") evaluates information relevant to listing

[192] Passenger name record (PNR) data is personal information provided by passengers and collected and held by air carriers. It includes information such as the name of the passenger, travel dates, itineraries, seats, baggage, contact details and means of payment. For more information see Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, *Official Journal of the European Union* L119/123 (4 May2016).

[193] European Commission, Action Plan to support the protection of public spaces, COM (2017) 612 final (18 October 2017).

[194] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, *Official Journal of the European Union* L 141/73 (5 June 2015).

and de-listing persons, groups, and entities involved in terrorism, before making recommendations to the Council. Listed persons are subjected to restrictive measures. These measures include the freezing of funds and other financial assets, as well as enhanced measures related to police and judicial cooperation in criminal matters.

"Pursue" and investigate terrorists across borders.

To achieve these goals, the strategy notably focuses on improving cooperation and information exchange between police and judicial authorities; impeding planning, travel, and communications; cutting off access to funding and materials; and bringing terrorists to justice, all while respecting human rights and international law.

For instance, as part of this third pillar, an action plan to strengthen the fight against terrorist financing has been adopted in 2016.[195]

"Respond" in a coordinated way by preparing for the management and minimization of the consequences of a terrorist attack.

The Strategy also aims to improve national capabilities to deal with the aftermath of a terrorist attack; the coordination of the post-crisis response; and the needs of victims. The main priorities in this area include developing European Union crisis coordination arrangements, developing risk assessments tools, and sharing best practices on assistance to victims of terrorism. A concrete example of ongoing work under this pillar is the creation of an European Union Centre of Expertise for Victims of Terrorism.[196]

Across the four pillars, a cross-cutting feature is the European Union's role in supporting international cooperation and national capabilities, even as the European Union recognizes that Member States have primary responsibility for combating terrorism. In particular, the European Union counter-terrorism strategy underlines the role of the European Union in:

- **"Strengthening national capabilities":** using best practices; sharing knowledge and experiences in order to improve national capabilities to prevent, protect against, pursue, and respond to terrorism, including through improved collection and analysis of information and intelligence.
- **"Facilitating European cooperation":** working together to share information securely between Member States and Institutions; establishing and evaluating mechanisms to facilitate cooperation, including police and judicial authorities, through legislation where necessary and appropriate.
- **"Developing collective capability":** ensuring European Union level capacity to understand and make collective policy responses to the terrorist threat; mak-

[195] European Commission, Action Plan for strengthening the fight against terrorist financing, COM(2016) 50 final (2 February 2016).

[196] European Commission, Commission decision of 31.1.2019 on the financing of the Pilot project "Setting up a EU Centre of Expertise for Victims of Terrorism" and the adoption of the work programme for 2018, C(2019) 636 final (31 January 2019).

ing best use of the capability of the Union bodies including Europol, Eurojust, FRONTEX, the MIC, and the SITCEN.

- **"Promoting international partnership":** working with others beyond the European Union, particularly the United Nations, other international organizations and key third countries, to deepen the international consensus, build capacity, and strengthen cooperation to counter terrorism. On 9 February 2015, in the wake of the Charlie Hebdo attacks, the European Union leaders stressed the need for the European Union to engage more with non-member countries on security issues and counter-terrorism. In this regard, the counter-terrorism agenda is present in the relations between the European Union and non-European Union countries in many forms, including through high-level political dialogues; the adoption of cooperation clauses and agreements; specific assistance; and capacity-building projects with strategic countries.

2. Directive (EU) 2017/541 on combating terrorism

In addition to non-binding instruments, such as the European Union Counter-Terrorism Strategy, Member States have several binding obligations under the regional legal framework of the European Union. Until March 2017, the foremost counter-terror obligations were articulated in the Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)[197] and amending decision 2008/919/JHA.[198] These decisions required Member States to take a series of actions, such as ensuring that definitions of terrorism – embedding criteria which have been agreed on among Member States – existed within their domestic law, and criminalizing certain acts associated with terrorism. These decisions defined particular terrorist offences and set down the rules for transposition in European Union Member States.

In March 2017, the Council adopted Directive (2017/541)[199] on combating terrorism. The Directive, which replaced the 2002 Framework, strengthens the European Union legal framework by reinforcing and widening the scope of existing legislation. For example, it criminalizes travel within, outside, or to the European Union for terrorist purposes. Of relevance are Articles 9 and 10, which concern travelling or facilitating travel for the purpose of terrorism.

The Directive provides its own definition of "terrorist offence" (defined in Article 3), which is different from the one proposed in the Council of Europe Convention. Even though both instruments criminalize similar activities, there is a slight possibility an act that is criminal under Directive 2017/541 may not be so under the Council of Europe Convention, and vice versa. As in the Council of Europe Convention on the Prevention

[197] Council of the European Union, Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA), *Official Journal of the European Union* L 164/3 (22 June 2002).

[198] Council of the European Union, Council Framework Decision of 28 November 2008 on combating terrorism (2008/919/JHA), *Official Journal of the European Union* L 330/21 (9 December 2008).

[199] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, *Official Journal of the European Union* L 88/6 (31 March 2017).

of Terrorism, these offences must be committed intentionally, as explicitly stated in each article:

Article 4 – Offences relating to a terrorist group

"Member States shall take the necessary measures to ensure that the following acts, when committed intentionally, are punishable as a criminal offence:

(a) directing a terrorist group;

(b) participating in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group."

Article 5 – Public provocation to commit a terrorist offence

"Member States shall take the necessary measures to ensure that the distribution, or otherwise making available by any means, whether online or offline, of a message to the public, with the intent to incite the commission of one of the offences listed in points *(a)* to (i) of Article 3(1), where such conduct, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed, is punishable as a criminal offence when committed intentionally."

Article 6 – Recruitment for terrorism

"Member States shall take the necessary measures to ensure that soliciting another person to commit or contribute to the commission of one of the offences listed in points *(a)* to (i) of Article 3(1), or in Article 4 is punishable as a criminal offence when committed intentionally."

Article 7 – Providing training for terrorism

"Member States shall take the necessary measures to ensure that providing instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques, for the purpose of committing, or contributing to the commission of, one of the offences listed in points *(a)* to (i) of Article 3(1), knowing that the skills provided are intended to be used for this purpose, is punishable as a criminal offence when committed intentionally."

Article 8 – Receiving training for terrorism

"Member States shall take the necessary measures to ensure that receiving instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques, for the purpose of committing, or contributing to the commission of, one of the offences listed in points *(a)* to (i) of Article 3(1) is punishable as a criminal offence when committed intentionally,"

Article 9 – Travelling for the purpose of terrorism

(1) "Each Member State shall take the necessary measures to ensure that travelling to a country other than that Member State for the purpose of committing, or contributing to the commission of, a terrorist offence as referred to in Article 3, for the purpose of the participation in the activities of a terrorist group with knowledge of the fact that such participation will contribute to the criminal activities of such a group as referred to in Article 4, or for the purpose of the providing or receiving of training for terrorism as referred to in Articles 7 and 8 is punishable as a criminal offence when committed intentionally."

(2) "Each Member State shall take the necessary measures to ensure that one of the following conducts is punishable as a criminal offence when committed intentionally:

(a) Travelling to that Member State for the purpose of committing, or contributing to the commission of, a terrorist offence as referred to in Article 3, for the purpose of the participation in the activities of a terrorist group with knowledge of the fact that such participation will contribute to the criminal activities of such a group as referred to in Article 4, or for the purpose of the providing or receiving of training for terrorism as referred to in Articles 7 and 8; or

(b) Preparatory acts undertaken by a person entering that Member State with the intention to commit, or contribute to the commission of, a terrorist offence as referred to in Article 3."

Article 10 – Organizing or otherwise facilitating travelling for the purpose of terrorism

"Member States shall take the necessary measures to ensure that any act of organization or facilitation that assists any person in travelling for the purpose of terrorism, as referred to in Article 9(1) and point *(a)* of Article 9(2), knowing that the assistance thus rendered is for that purpose is punishable as a criminal offence when committed intentionally."

Article 11 – Terrorist financing

(1) "Each Member State shall take the necessary measures to ensure that providing or collecting funds, by any means, directly or indirectly, with the intention that they be used, or in the knowledge that they are to be used, in full or in part, to commit, or to contribute to the commission of, any of the offences referred to in Articles 3 to 10 is punishable as a criminal offence when committed intentionally."

(2) "Where the terrorist financing referred to in paragraph 1 of this Article concerns any of the offences laid down in Articles 3, 4 and 9, it shall not be necessary that the funds be in fact used, in full or in part, to commit, or to contribute to the commission of, any of those offences, nor shall it be required that the offender knows for which specific offence or offences the funds are to be used."

Article 12 – Other offences related to terrorist activities

"Member States shall take the necessary measures to ensure that offences related to terrorist activities include the following intentional acts:

(a) aggravated theft with a view to committing one of the offences listed in Article 3;

(b) extortion with a view to committing one of the offences listed in Article 3;

(c) drawing up or using false administrative documents with a view to committing one of the offences listed in points *(a)* to (i) of Article 3(1), point *(b)* of Article 4, and Article 9."

III. 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 FTFs during UNODC assessment missions and training activities in SEE. Computers and the Internet are rapidly becoming one of the key features of modern terrorism investigations. Each can be used in the commission of crime, can contain evidence of crime, and can even be targets of crime.

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

- UNODC/CTED/IAP publication: "Practical Guide for Requesting Electronic Evidence Across Borders" (2018)
- 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 Electronic 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.

In 2014, Charles Lister, a terrorism expert at the Brookings Institute, said:

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

> profound. 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."[200]

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 on e-evidence for convictions. In the United Kingdom, for instance, 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.[201]

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.[202] Some jihadists from SEE were very influential on social media. One such jihadist is Lavdrim Muhaxheri, also known as "Abu Abdullah al Kosovo", a Kosovo Albanian IS leader and recruiter of FTFs who proclaimed himself as "commander of Albanians in Syria and Iraq". Apart from the borderless nature of the Internet, there is an important transnational dimension of extremist online content, in SEE in particular, owing to factors such as shared languages, key influencers, and diaspora links.[203]

Alongside other groups, ISIL (Da'esh) members have proven difficult to track due to their use of technological tools, such as encryption applications, social media platforms, and encrypted instant messaging platforms. It was recently reported by a number of news outlets that ISIL (Da'esh) has released a manual, entitled "How to Tweet Safely Without Giving out Your Location to NSA", which purports to explain how to avoid surveillance.[204] Other examples of how technologically competent Islamist terrorists have become include a number of applications developed by terrorists themselves, such as:[205]

- **"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.

[200] Sam Jones, "Jihad by social media", Financial Times, 28 March 2014.

[201] Europol, "European Union Terrorism Situation and Trend Report 2015" (TE-SAT) (2015).

[202] 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).

[203] Maura Conway, Sheelagh Brady, "A New Virtual Battlefield - How to Prevent Radicalisation in the Cyber Security Realm of the Western Balkans" (Sarajevo, Regional Cooperation Council, December 2018), p. 83.

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

[205] Ibid.

- **"Amn al-Mujahid"** (*Security of 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 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 applications distributor to change the URL (Uniform Resource Locator) where the application is hosted, in case any of their websites are taken down. This technique has also been used by cyber-criminals 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 terrorist-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.[206]

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.[207] Some of the software includes:

- **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.

[206] 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.

[207] 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.[208]

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.[209]

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 "worldwide web" (www), is an information space where documents and other resources can be accessed on the Internet. At the time of development of the "web", three specifications for web technologies were defined: "Uniform Resource Locator" (URL); "Hypertext Transfer Protocol" (HTTP); and "Hypertext Markup Language" (HTML).

The basis for Internet communication is a process of assigning an address to each device attached to the Internet. This address allows a device to connect and communicate with any other 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

[208] Retirely, "How terrorists communicate - Dark Web", available at: https://www.retire.ly/how-terrorists-communicate-dark-web/.

[209] TE-SAT 2018, p.31 (see footnote 120, chapter 1); see also Europol, "Internet Organised Crime Threat Assessment (IOCTA) 2018" (2018), p.13.

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 uses 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, "Internet Service Providers" (ISP) assign 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 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.[210]

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[211] 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.

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.

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

[211] 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.

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 thousands). 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 a crime to an individual.[212]

As there is no common data retention policy in place in Europe, and ISPs have the discretion to decide on data retention time frames, some ISPs retain data for 6 months, some for 2 months, and some for as little as 14 days. 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 the European Union 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.[213]

At the same time, police and judicial authorities may have easier access to cloud data in the United States as the European Union Commission intends to negotiate with the United States Government on participation in the United States "Clarifying Lawful Overseas Use of Data" (CLOUD) Act 2018.[214]

---

[212] 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.

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

[214] 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.

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 the 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 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*."[215] 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.

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.[216]

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

[216] Jeff Desjardins, "What Happens in an Internet Minute in 2018", Visual Capitalist, 14 May 2018.

To give some idea of the scale of the challenge, 481,000 tweets in one minute equates to over 5 million tweets per day. To scale some of the above numbers to a monthly basis, there would be:

42,033,600,000 Facebook logins
159,840,000,000 Google searches
1,641,600,000,000 WhatsApp messages sent, and
8,078,400,000,000 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.[217]
- **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.[218]
- **Research Clinic** – a free resource featuring internet research links, training, and apps in support of open source intelligence.[219]
- **OSINT Framework** – offers a flow-chart to help focus the gathering of information from free tools or resources.[220]
- **The Open Source Intelligence Tools and Resources Handbook 2018** – offers a comprehensive list of tools to help investigators explore social media information.[221]

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"[222] and "CheckUserNames"[223] 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

[217] 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.

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

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

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

[221] 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.

[222] For more information see the website of SocialMention, available at: http://www.socialmention.com/#.

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

looking inside its "Exchangeable Image File Format" (EXIF) data.[224] An example of how EXIF data is displayed using freely available online software, is shown below:

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 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 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.[225]

[224] 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.

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

Facebook

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

Additionally, users may join common-interest user groups organized by their workplace, school, or other characteristics, and categorize their friends into lists such as "People From Work" or "Close Friends". Facebook is the most popular social networking site in several English-speaking countries, including Canada, the United Kingdom, and the United States. In regional Internet markets, Facebook penetration is reported to be highest in North America, followed by Middle East-Africa, Latin America, Europe, and Asia-Pacific. Facebook penetration in the relevant SEE jurisdictions vis-à-vis Internet use by December 2017 is set out in the table below:[226]

Jurisdiction	Internet usage/penetration (% of population)	Facebook usage/penetration (% of population)
Albania	1,932,024 / 65.8%	1,400,000 / 47.7%
Bosnia and Herzegovina	2,828,846 / 80.7%	1,500,000 / 42.8%
Kosovo	1,523,373 / 80.4%	910,000 / 48.0%
Montenegro	439,624 / 69.9%	320,000 / 50.9%
North Macedonia	1,583,315 / 75.9%	1,000,000 / 48.0%
Serbia	6,325,816 / 72.2%	3,400,000 / 38.8%
Europe	704,833,752 / 85.2%	340,891,620 / 41.2%
World	4,159,440,684 / 54.5%	2,119,060,152 / 27.8%

Privacy

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

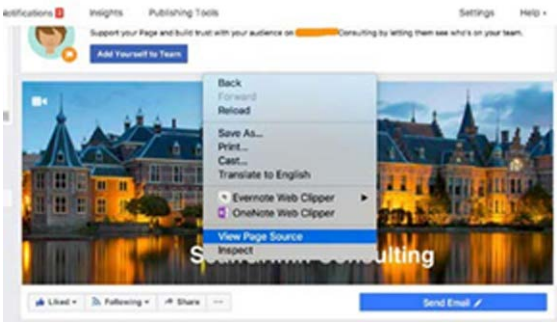
Following recent adverse publicity and data protection issues, Facebook has disabled the Graph search facility, making it more difficult to freely search for users of the site when only an email or telephone number is known.

[226] See "Internet World Stats - Usage and Population Statistics", available at: https://www.internetworldstats.com/europa2.htm; Facebook penetration statistics were last updated in December 2017 (site accessed 6 February 2019).

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 live 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.[227]
- **"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, such as Twitter accounts, blogs and personal websites.[228]

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.[229]

Twitter

A 2014 investigation in the United Kingdom ("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 of 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 2019 Twitter had more than 261 million international users. Roughly 46 per cent of Twitter users are on the platform daily.[230]

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.

[227] See website of Tineye, available at: https://www.tineye.com/.

[228] See website of Google images; available at: https://images.google.com/.

[229] Facebook, "Information for law enforcement authorities"; Operational Guidelines.

[230] Omnicore, "Twitter by the Numbers: Stats, Demographics and Fun Facts", 5 September 2019, available at: https://www.omnicoreagency.com/twitter-statistics/.

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).[231]

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. For example, type "near:NYC within:5mi" to return tweets sent within five miles of 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,[232] many of which are provided there in a template for ease of use.

---

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

[232] 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.[233]

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.[234]
- **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.[235]

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, namely 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.[236]

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", that is, how "central" to the group a person is in terms of influence, access, direct contact and as a go-between.

[233] Twitter, "Guidelines for Law Enforcement".

[234] See Geosocial Footprint website, available at: http://geosocialfootprint.com/.

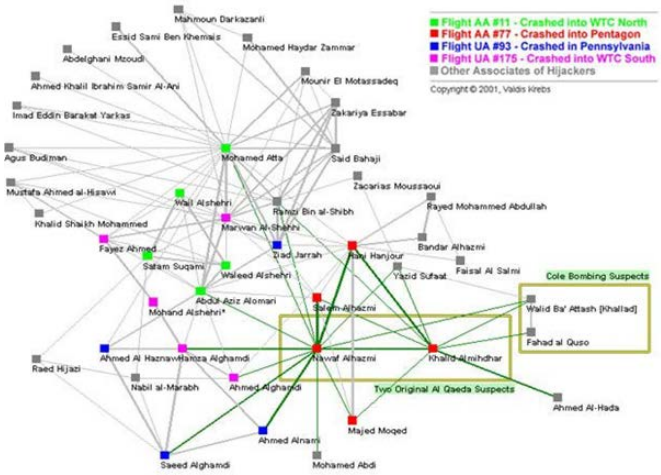
[235] See TweetBeaver website, available at: https://tweetbeaver.com/.

[236] See Paterva website, available at: https://www.paterva.com/community/community.php.

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).[237]

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



All nodes within two steps/degrees of original suspects

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

1. 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.[238]
- **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.[239]
- **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.[240]

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

When deciding on what ESI or digital evidence to collect, consideration should be given to the environment in which such information and evidence will be gathered through online investigation, or at a crime scene. As previously discussed, an initial phase in an investigation may include an amount of OSINT gathering. Throughout this

[238] United States, Department of Justice (DOJ) and Administrative Office of the U.S. Courts (AO) Joint Working Group on Electronic Technology in the Criminal Justice System (JETWG), *Recommendations for Electronically Stored Information (ESI)* Discovery Production in Federal Criminal Cases (Washington, D.C., February 2012), available at: https://www.fd.org/sites/default/files/Litigation%20Support/final-esi-protocol.pdf, p. 12.

[239] Association of Chief Police Officers (ACPO), "Good Practice Guide for Computer-Based Electronic Evidence" (2017), available at: https://www.datlabsdatarecovery.co.uk/wp-content/uploads/2017/10/ACPO-Guidelines.pdf, p.5.

[240] United States, Department of Justice (DOJ), Office of Justice Programs, *Electronic Crime Scene Investigation: A Guide for First Responders*, Second Edition (Washington, D.C., April 2008).

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 domain is a key part of any Internet investigation and there are many resources available on the Internet to assist with this process. First, 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.[241]

Second, each site has a "WHOIS" function that allows investigators to identify IP registration information.[242] 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[243] and Robtex.[244]

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.[245] There are many tools freely available to assist, including:

- HT Tracks[246]
- Wget[247]

[241] See Internet Assigned Numbers Authority (IANA) website, available at: http://www.iana.org/.

[242] 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).

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

[244] See website of Robtex, available at: https://www.robtex.com/.

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

[246] See HT Tracks website, available at: http://www.httrack.com/.

[247] GNU, "GNU Wget 1.20 Manual", 30 November 2018.

- Wayback Machine – a website archive site[248]
- 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 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 an 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[249] 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.[250]

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

[248] See Wayback Machine website, available at: https://archive.org/web/.

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

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

holders and for the original IP from where the account was registered. Also, mobile devices, laptops, and desktop computers use online-based backup systems, also known as the "cloud".

With regard to mobile devices, cloud-based systems can provide forensic investigators with access to text messages and pictures taken from a particular phone and keep an average of 1,000-1,500 (or even more) of the last text messages sent to and received from that phone. In addition, many mobile devices store information about the locations where the device may have travelled and provide an idea as to when exactly it had been there. To obtain this information, investigators can access an average of the last 200 cell locations accessed by a mobile device. Satellite navigation systems and satellite radios in cars can provide similar information. Photos taken with a GPS-enabled device contain file data that shows when and exactly where a photo was taken. 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).[251]

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.[252] In such cases, competent national authorities should make use of the available tools for international cooperation, such as requesting Mutual Legal Assistance (MLA).[253]

Investigators should also consider referring to the UNODC document "Basic tips for investigators and prosecutors for requesting electronic/digital data/evidence from foreign jurisdictions"[254] 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

[251] See Hamstermap website, available at: http://www.hamstermap.com./.

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

[253] UNODC, "Manual on Mutual Legal Assistance and Extradition" (September 2012).

[254] 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.

holder may learn of any preservation request (for instance if it is the policy of an ISP to notify their clients).

It could be also explored whether the formal requirements in the MLA procedures may be further differentiated depending on what data is requested (for example, whether it is subscriber, traffic or content data).[255] 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.[256]

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.[257] 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".[258]

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.

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

[256] Council of the European Union, "Collecting E-evidence in the digital age - the way forward", 13689/15 (4 November 2015).

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

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

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:

- Devices, peripherals and other materials may be collected once a crime scene has been secured and a legal authority is in place to seize evidence.
- Before recovering anything, first photograph or video the scene and all the components including the leads in situ. If no camera is available, draw a sketch plan of the system and label the ports and cables so that the system(s) may be reconstructed at a later date.
- Document any activity on the computer, components, or devices, again by taking a photograph and record any information that can be seen on the screen.
- Physical searches of suspects and the location of computers may reveal Personal Identification Numbers (PINs) and passwords.
- Recover associated chargers, cables, peripherals and manuals, along with thumb drives, cellular phones, external hard drives, and electronic photo frames etc.
- Many of these devices are examined using different tools and techniques, and this is most often carried out in specialized laboratories.
- To prevent the alteration of digital evidence during collection, document any activity on the computer, components, or devices by taking a photograph and recording any information on the screen.
- The mouse may be moved (without pressing buttons or moving the wheel) to determine if something is on the screen.[259]

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.

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

3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

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

Effectively, "live forensics" provides for the collection of digital evidence in an order that is based on the life expectancy of the evidence in question. Perhaps the most important evidence to be gathered in digital evidence collection today and for the foreseeable future exists only in the form of the volatile data contained within the computer's RAM ("Random Access Memory").[260] 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.[261] If a computer is on, using a computer forensic expert is highly recommended, as turning off the computer may result in the loss of evidence relating to criminal activity. However, if a computer is on but is running destructive software (formatting, deleting, removing or wiping information), power to the computer should be disconnected immediately to preserve whatever is left on the machine.

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

[260] 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.

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

- 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.[262] 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 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.

[262] 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.

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 in to a power source will (in most cases) force the device to synchronize with any cloud services running. This should maximize the amount of evidence potentially available in the cloud. However, capturing this evidence may pose some major challenges, as the target machine(s) may be cited outside of the concerned State's jurisdiction,[263] 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.[264]

3.3 Special investigative techniques and foreign terrorist fighters

Undercover operations online

Successful investigations against FTFs 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 period of time by an undercover employee.[265]

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)*;

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

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

[265] United States of America, Office of the Attorney General, Guidelines on Federal Bureau of Investigation Undercover Operations (Washington, D.C., 13 November 1992).

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.[266]

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.[267]

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, 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.

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

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

- 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.[268]
- The Chief of Police or deputy should establish protocols for documenting and recording investigations activity and communications.
- Ensure investigators are trained in how to set tone, pace, and subject matter of online conversations in addition to other entrapment considerations.

Regardless of which policy considerations are implemented, a social networking investigations policy and the use of fictitious profiles should generally mirror those relating to conventional undercover investigations.[269]

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

[269] 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 foreign terrorist fighters

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 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 maritime navigation

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

2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation

1988 Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf

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

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 foreign terrorist fighters

Council of Europe

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

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

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

Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, CETS No. 217 (2015)

European Union

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (2017)

Council Framework Decision of 28 November 2008 on combating terrorism (2002/475/JHA)

UNODC

United Nations Office on Drugs and Crime

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-3389, www.unodc.org

V.19-10338