UNODC
United Nations Office on Drugs and Crime

Investigation, Prosecution and Adjudication of Foreign Terrorist Fighter Cases for South and South-East Asia

Cover image: istockphoto.com/Lorado

UNITED NATIONS OFFICE ON DRUGS AND CRIME
Vienna

Investigation, Prosecution and Adjudication of Foreign Terrorist Fighter Cases for South and South-East Asia

UNITED NATIONS
Vienna, 2018

The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

This publication has not been formally edited.

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

Contents

Introduction

Foreign terrorist fighters (FTFs) have, over the past few years, constituted one of the major threats to international peace and security.

On 24 September 2014, the United Nations Security Council adopted resolution 2178 as a response to the increasing threat posed by FTFs, requiring Member States to implement criminal justice measures to effectively prevent, deter and criminalize the travel of FTFs and their related activities. While the resolution primarily targets individuals travelling to Iraq and the Syrian Arab Republic to join entities such as ISIL (Da'esh),[1] the Al-Nusrah Front and certain other cells or derivatives of Al-Qaida, the definition of FTFs is cast widely to include all "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".

Since the adoption of this resolution, there have been significant changes and developments in the landscape of the FTF phenomenon. As ISIL (Da'esh) loses ground in the Syrian Arab Republic and Iraq, Member States will be concerned as FTFs search for new battlegrounds. This is particularly the case in South and South-East Asia. For South and South-East Asian countries, the phenomenon of FTFs relates not only to a country's nationals travelling to and from Iraq and the Syrian Arab Republic, but also to those individuals who travel to perpetrate terrorist acts in neighbouring South and South-East Asian countries. This unique situation faced by South and South-East Asian countries has given rise to calls for greater regional and cross-regional cooperation to prevent and counter the threat of FTFs.

As such, it is imperative that national authorities review their current national criminal justice frameworks and strategies to prevent and counter the threat of FTFs, including returning and relocating FTFs and their families, in both regions. Responding to the identified needs of Member States in countering the threat of FTFs, the UNODC Terrorism Prevention Branch has published this training manual on the investigation, prosecution and adjudication of FTFs in South and South-East Asia. The training manual is intended to be used as an aide for practical training sessions for law enforcement officials and judicial officers. The training manual focuses on, among other aspects, the international and regional legal frameworks relevant to FTFs, with a focus on digital evidence, including online investigatory tools and techniques. The manual also includes an adult learning methodology.

[1] Hereinafter for ease of reference, the text uses "ISIL" to refer to ISIL (Da'esh), ISIS, IS or the Islamic State, and the "caliphate" to refer to its area of control. The authors take no position as to the legal or formal status of any group, territory or jurisdiction.

Chapter 1

Overview of foreign terrorist fighter topics

1.1 The foreign terrorist fighter phenomenon

Scope of the term “foreign terrorist fighter”

The concept of “foreign fighters” is not new. Over the past 250 years alone, nearly 100 civil wars have included the participation of fighters from abroad.[2] The Spanish Civil War (1936-1939) is a prime example, in which around 50,000 volunteers from more than 50 countries participated, representing both sides of the conflict.[3]

The term “foreign fighter” was first officially used in reference to fighters travelling from outside the conflict zone to fight for Al-Qaida in Afghanistan, and has become more and more commonly used since the terrorist-led insurgency started in Iraq in 2003. In the absence of a legal definition, several academics have presented differing meanings of the term.

One of the most widely accepted is that of 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”.[4]

Terrorists who travel internationally to commit attacks is not a new concept either, and has become an increasing phenomenon since global travel became easier in the twentieth century. The first notable appearance of the term “foreign terrorist fighters” was in United Nations Security Council resolution 2170, adopted in August 2014 in response to the then-escalating crisis in the Syrian Arab Republic and Iraq. Condemning the terrorist acts causing the deaths of civilians, the Security Council called upon Member States to “suppress the flow of foreign terrorist fighters” to violent extremist groups in the two countries.[5]

[2] David Malet, *Foreign Fighters: Transnational Identity in Civil Conflicts,* (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. At https://www.radicalisationresearch.org/debate/malet-foreign-fighters-home-grown-radicalization/.

[3] Sebastiaan Faber, “Spain’s Foreign Fighters”, *Foreign Affairs* (September/October 2016). At https://www.foreignaffairs.com/reviews/review-essay/spain-s-foreign-fighters.

[4] Geneva Academy of International Humanitarian Law and Human Rights, “Foreign Fighters under International Law”, *Academy Briefing No.* 7 (October 2014). At https://www.geneva-academy.ch/joomlatools-files/docman-files/Publications/Academy%20Briefings/Foreign%20Fighters_2015_WEB.pdf.

[5] United Nations, “Security Council Adopts resolution 2170 (2014) Condemning Gross, Widespread Abuse of Human Rights by Extremist Groups in Iraq, Syria” (15 August 2014). At https://www.un.org/press/en/2014/sc11520.doc.htm.

A month later, on 24 September 2014, United Nations Security Council resolution 2178 was adopted to specifically tackle "the acute and growing threat posed by foreign terrorist fighters". The resolution emphasized the urgency of tackling the issue of all FTFs, in particular those of ISIL (Da'esh), the Al-Nusrah Front and "derivatives" of Al-Qaida.[6]

The resolution provided a helpful definition of an FTF:

> 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".[7]

In December 2017, United Nations Security Council resolution 2396 reaffirmed the definition of FTFs, and called upon Member States to tackle the threat posed by FTFs returning or relocating from conflict zones.[8]

Scope of the definition

Significantly, the United Nations definition only applies to foreign fighters who travel for the purpose of "terrorist" activity. While they might be guilty of a crime in their home State by virtue of privately engaging in an armed conflict in another country, not all foreign fighters are terrorists and should not be treated as such. The United Nations definition applies regardless of whether the FTF is engaged in armed conflict. The International Committee of the Red Cross has warned of the "potentially adverse effects" of conflating armed conflict with terrorism, and erroneously designating all non-State armed groups as terrorists.[9] FTFs also differ from mercenaries, who fight abroad on behalf of governments or privately financed entities[10] and are "motivated to take part in the hostilities essentially by the desire for private gain".[11] However, where financial and political or ideological interests significantly overlap, they may fall within the scope of the definition of FTFs.

1.2 Evolution

"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".

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

[6] United Nations Security Council resolution 2178 (2014).

[7] Ibid.

[8] United Nations, "Security Council Urges Strengthening of Measures to Counter Threats Posed by Returning Foreign Terrorist Fighters, Adopting resolution 2396 (2017)" (21 December 2017). At https://www.un.org/press/en/2017/sc13138.doc.htm.

[9] International Committee of the Red Cross, "The applicability of IHL to terrorism and counterterrorism" (1 October 2015). At https://www.icrc.org/en/document/applicability-ihl-terrorism-and-counterterrorism.

[10] Charles Lister, "Returning Foreign Fighters: Criminalization or Reintegration?", Policy Briefing August 2015 (Brookings Doha Center, 2015). At https://www.brookings.edu/wp-content/uploads/2016/06/En-Fighters-Web.pdf.

[11] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 8 June 1977, Art. 47. The use of mercenaries is covered by other international, regional, and domestic laws.

The mujahidin war in Afghanistan in the 1980s was the first modern conflict to see high levels of foreign fighter participation. From that one conflict, a global fighter community was to be established 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.[12] 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 normal life but others, including fighters from South and South-East Asia, continued militant activities and were involved in the formation of terrorist organizations such as Jemaah Islamiyah and the Abu Sayyaf Group. 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.

During the 1990s, foreign fighters who had trained in Afghanistan joined with others to fight on behalf of the Muslim population in the civil war in Bosnia and Herzegovina (1992-1995). Estimates of the number range from up to 5,000, with recruits mainly drawn from the Middle East and backed by the Al-Qaida leadership. There, they formed a unit of the Bosnian army known as "El Mujahedin", with their leaders paid as officers.[13]

Smaller numbers were to fight from 1994 in Chechnya. Returning veterans from the Afghan campaign became separatist leaders in Chechnya and recruited experienced Afghan-Arab fighters, together with other Arabs from the Chechen diaspora community, to travel and fight with rebels seeking independence from Russia. Fighting for a vision of an Islamic State in the North Caucasus, the number of foreign fighters that took part is estimated at 500-700.[14]

As the twentieth century came to a close, a large core of foreign fighters remained in Afghanistan, where Al-Qaida provided training camps for fighters such as the hijackers of 11 September 2001. Examples of others 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.[15] Convicted for his role in a coordinated series of bomb attacks, including on public transport that killed 22 people and wounded scores of commuters in Metro Manila, on Rizal Day, in December 2000.[16] Reported to have received military training in Afghanistan in the 1990s.[17]
- 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. Also convicted of a plot, planned in the Philippines, to place bombs on passenger flights. Yousef fought in the mujahidin war in Afghanistan.[18]
- 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

[12] Maria Galperin Donnelly, Thomas M. Sanderson and Zack Fellman, "Foreign Fighters in History", Center for Strategic and International Studies. At http://foreignfighters.csis.org/history_foreign_fighter_project.pdf.

[13] David Malet, *Foreign Fighters: Transnational Identity in Civil Conflicts*, (Oxford University Press, 2015).

[14] "The radicalisation of the Chechen separatist movement - Myth or reality?", Prague Watchdog (16 May 2007). "The Rise and Fall of Foreign Fighters in Chechnya", Jamestown Foundation (31 January 2006). At https://jamestown.org/program/the-rise-and-fall-of-foreign-fighters-in-chechnya/.

[15] United States Department of the Treasury, "Snow Announces Designation of 10 Jemaah Islamiyah (JI) Terrorists", Press Release JS-700 (5 September 2003). At https://www.treasury.gov/press-center/press-releases/Pages/js700.aspx.

[16] Sandy Araneta, "Life terms for MILF Rizal Day bombers", *The Philippine Star* (24 January 2009). At http://www.philstar.com/headlines/433895/life-terms-milf-rizal-day-bombers.

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

[18] "Mastermind Gets Life For Bombing Of Trade Center", *The New York Times* (9 January 1998). At http://www.nytimes.com/1998/01/09/nyregion/mastermind-gets-life-for-bombing-of-trade-center.html.

2004, which caused the deaths of 245 people. He is said to have received explosives training in Afghanistan in 1999.[19]

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

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, amounting to 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.[21]

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 the majority of suicide bombings.[22] AQI began to lose power in 2006 following the death of its leader in an airstrike, and Sunni tribal leaders forming a new movement for the purpose of expelling the terrorist group. Many of AQI's leaders were killed or imprisoned, but the group continued to conduct attacks.

After the outbreak of civil war in the Syrian Arab Republic in 2011, one of AQI's commanders established an official Al-Qaida affiliate in the country, called the Al-Nusrah Front. At the same time, remnants of AQI sought to create a safe haven in Syria. Both initially were part of an estimated 1,000-person armed opposition group in the Syrian Arab Republic[23] 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 the Syrian Arab Republic and Iraq, 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".[24]

Despite its extreme use of violence, the persuasive use of propaganda by ISIL (portraying its military successes and the benefits of life under the caliphate) led to an unprecedented flow of

[19] "Dr Azahari the most dangerous terrorist", *The Star Online* (15 August 2003). At https://www.thestar.com.my/opinion/letters/2003/08/15/dr-azahari-the-most-dangerous-terrorist/.

[20] Maria Galperin Donnelly, Thomas M. Sanderson and Zack Fellman, "Foreign Fighters in History", Center for Strategic and International Studies. At http://foreignfighters.csis.org/history_foreign_fighter_project.pdf.

[21] Ibid.

[22] "Suicide Bombers in Iraq: The Strategy and Ideology of Martyrdom", United States Institute of Peace (July 23, 2007).

[23] "Guide to the Syrian rebels", BBC (13 December 2013). At http://www.bbc.com/news/world-middle-east-24403003.

[24] "Islamic State and the crisis in Iraq and Syria in maps", *BBC News* (21 December 2017). At http://www.bbc.com/news/world-middle-east-27838034. "Isis leader calls on Muslims to 'build Islamic state'", *BBC News* (1 July 2014). At http://www.bbc.com/news/world-middle-east-28116846.

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 the Syrian Arab Republic and Iraq, FTFs are also engaged in terrorist activity with other branches or affiliates of ISIL and Al-Qaida and with insurgent groups such as the Afghan Taliban.[25] Normally drawn from the same continent or from diaspora communities of the countries involved, they all potentially pose risks for the future. It is the numbers and multinational composition of those drawn to the Syrian conflict that is unique.

1.3 Global situation

At its peak, some 10 million people were living in territory under ISIL control in the Syrian Arab Republic and Iraq[26] and the flow of foreign fighters across the Turkish-Syrian border was as high as 2,000 per month.[27] By 2015 approximately 40,000 individuals from over 120 countries had travelled to Iraq and the Syrian Arab Republic as fighters.[28] An estimated 80 per cent of those migrated to join ISIL and live in the caliphate,[29] creating a combined force with local Syrians and Iraqis assessed at around 100,000 fighters.[30]

INTERPOL has 43,000 names in its ISIL database, including information collected from the battlefields in Iraq and the Syrian Arab Republic.

Source: Brett McGurk, "Letter to D-ISIS Coalition Partners on the Progress of the Past Year", remarks of the Special Presidential Envoy for the Global Coalition To Counter ISIS, United States Department of State (29 December 2017). At https://www.state.gov/s/seci/2017remarks/276806.htm.

As part of its overarching aim to build a global Islamic caliphate, ISIL has announced the establishment of a number of provinces outside of Iraq and the Syrian Arab Republic. Controlled by affiliated groups, these provinces are located in the Middle East (Libya, Yemen, Egypt—Sinai and Saudi Arabia) and beyond (North Caucasus, Algeria, Nigeria and on the Afghanistan/Pakistan border).[31] It is reported that more than 50 terrorist groups around the world have pledged allegiance to ISIL.[32]

[25] "Afghan Officials See Foreign Fighters Playing Key Role in Helmand Fighting", *Voice of America* (14 August 2016). At https://www.voanews.com/a/afghan-officials-see-foreign-fighter-playing-key-role-in-helmand-fighting/3463768.html.

[26] "Islamic State and the crisis in Iraq and Syria in maps", *BBC News* (21 December 2017). At http://www.bbc.com/news/world-middle-east-27838034.

[27] "What's beyond the defeat of ISIS?", Brookings Institution (27 September 2016). At https://www.brookings.edu/blog/markaz/2016/09/27/whats-beyond-the-defeat-of-isis/.

[28] 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). At https://ctc.usma.edu/posts/a-view-from-the-ct-foxhole-lisa-monaco-former-assistant-to-president-barack-obama-for-homeland-security-and-counterterrorism. See also "Responses to returnees: Foreign terrorist fighters and their families", Radicalisation Awareness Network (July 2017), stating that there are "42,000+ foreign terrorist fighters from 120+ countries". At https://ec.europa.eu/home-affairs/sites/homeaffairs/files/ran_br_a4_m10_en.pdf.

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

[30] "How Many Fighters Does the Islamic State Really Have?" University of Texas War on the Rocks (9 February 2015). At https://warontherocks.com/2015/02/how-many-fighters-does-the-islamic-state-really-have/.

[31] "Beyond Syria and Iraq - Examining Islamic State Provinces", The Washington Institute for Near East Policy (November 2016). At https://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus149_Bauer.pdf.

[32] Ibid.

The tightening of border controls—particularly by Turkey—after the passing of United Nations resolution 2178, combined with the worsening situation on the ground in the Syrian Arab Republic and Iraq, meant that by September 2016 the flow of fighters crossing the border from Turkey had dropped to an estimated 50 per month.[33]

By December 2017, ISIL had lost most of the land it held in Iraq, and was reduced to occupying only 7 per cent of Syrian territory (in December 2016 it had held almost 55 per cent).[34] 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.[35] The loss of seized oil fields also meant ISIL lost its main revenue streams.[36]

The Global Coalition to Defeat ISIL estimated there were less than 1,000 ISIL terrorists in the coalition's area of operations at the end of 2017,[37] with an unknown but heavily reduced number in eastern Syria and western Iraq. The governments of Iraq and the Syrian Arab Republic both declared victory over ISIL, but it continues to conduct attacks against military and civilian targets.[38] Despite major territorial losses, ISIL remains the "deadliest terrorist organization in the world".[39] 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 attacks can be placed in three categories. First, there are attacks conducted by "core" FTF operatives, who are trained by ISIL, based in and primarily active in Iraq and the Syrian Arab Republic.[40] Second, there are attacks where the person or group has not travelled to the conflict zone, but reaches out online and is coached virtually by an ISIL facilitator based in the Syrian Arab Republic/Iraq (often an FTF from their own country). Using encrypted messaging these facilitators both encourage and instruct the would-be attackers. Attacks conducted in this manner have been termed by some commentators as "remote-controlled attacks".[41] Finally, there are "Lone wolf attacks", where the person or group self-affiliates with ISIL but does not have any direct link with the group. These attacks have been referred to as "leaderless jihad".[42] Thirty-five such attacks were carried out across 16 countries in 2016, killing 172.[43] However, it is often difficult to correctly classify many attacks. Although contact with the ISIL is frequently suspected, tangible evidence may not be found.

[33] "What's beyond the defeat of ISIS?", Brookings Institution (27 September 2016. At https://www.brookings.edu/blog/markaz/2016/09/27/whats-beyond-the-defeat-of-isis/.

[34] OMRAN Center for Strategic Studies, http://omranstudies.org/. For an updated map of the areas controlled by ISIL, see https://isis.liveuamap.com/.

[35] For an updated map of the areas controlled by ISIL, see https://isis.liveuamap.com/.

[36] "End of ISIS Approaching as Caliphate Loses Money and Land", *Newsweek* (29 June 2017). At http://www.newsweek.com/islamic-state-wont-survive-fourth-year-after-territory-and-revenue-collapse-630018.

[37] "Less than 1,000 IS fighters remain in Iraq and Syria, coalition says", *Reuters* (27 December 2017). At https://www.reuters.com/article/us-mideast-crisis-islamic-state/
less-than-1000-is-fighters-remain-in-iraq-and-syria-coalition-says-idUSKBN1EL0QT.

[38] "Why Reports of ISIS' Demise Have Been Greatly Exaggerated", Omran Center for Strategic Studies (18 December 2017). At http://omranstudies.org/publications/articles/why-reports-of-isis%E2%80%99-demise-have-been-greatly-exaggerated.html.

[39] "Overview: Terrorism in 2016", University of Maryland Study of Terrorism and Responses to Terrorism. At https://www.start.umd.edu/pubs/START_GTD_OverviewTerrorism2016_August2017.pdf.

[40] Ibid.

[41] "Terror from afar: how ISIS inspires and directs attacks remotely", *CBC* (24 March 2017). At http://www.cbc.ca/radio/day6/episode-330-london-attacks-trump-and-russia-autism-on-sesame-street-kids-climate-change-lawsuit-and-more-1.4035186/terror-from-afar-how-isis-inspires-and-directs-attacks-remotely-1.4035188.

[42] Marc Sageman, "Leaderless Jihad - Terror Networks in the Twenty-First Century" (University of Pennsylvania Press, 2008). See also "Frustrated foreign fighters", Brookings Institution (13 July 2017). At https://www.brookings.edu/blog/order-from-chaos/2017/07/13/frustrated-foreign-fighters/.

[43] "Overview: Terrorism in 2016", University of Maryland Study of Terrorism and Responses to Terrorism. At https://www.start.umd.edu/pubs/START_GTD_OverviewTerrorism2016_August2017.pdf. "ISIS goes global: 143 attacks in 29 countries have killed 2,043", *CNN* (12 February 2018). At http://edition.cnn.com/2015/12/17/world/mapping-isis-attacks-around-the-world/index.html.

Case study: Australia

On 15 July 2017, two Lebanese brothers living in Australia attempted to place an improvised explosive device (IED) on an Etihad passenger flight out of Sydney on which a third brother was flying, with the intention of blowing up the airliner mid-air. The Australian Federal Police have stated that the men were acting under the direction of "a senior member of the Islamic State". According to Lebanon's Interior Minister, a fourth brother is a commander in ISIL in the Syrian Arab Republic.[a]

Police alleged that the IED was constructed by placing explosives within a meat grinder, packed in a piece of luggage. But, the attempt was abandoned because the luggage exceeded the airline's weight limit. The two accused were subsequently arrested and await trial in Sydney, on the charge of acting in preparation for, or planning, a terrorist act.[b]

[a] "Australia disrupts 'sophisticated' plot directed by the Islamic State", *Long War Journal* (4 August 2017). At https://www.longwarjournal.org/archives/2017/08/australia-disrupts-sophisticated-plot-directed-by-islamic-state.php.

[b] "Lebanon monitored Australia bomb plot suspects: minister", *Reuters* (21 August 2017). At https://www.reuters.com/article/us-lebanon-security-emirates-australia/lebanon-monitored-australia-bomb-plot-suspects-minister-idUSKCN1B11A0.

Use of the Internet

The use of the Internet to facilitate attacks is not a new tactic, and in many respects, follows Al-Qaida's example of recruiting and inspiring plots online. However, ISIL has exploited the Internet on an unprecedented scale through recruiting; plotting and executing attacks using encrypted chat networks; and deploying a powerful social media network enabling the dissemination of a constant stream of professionally produced propaganda. This propaganda claims every success as the actions of "soldiers of the caliphate" and inspires future attacks.[44] The material is honed to appeal to a new tech savvy generation of recruits, with short soundbites, glossy images and action videos, as opposed to some of the lengthy speeches previously produced by other groups.

> "In 2015, the Islamic State's official propagandists were at the height of their bloody influence, producing slick content from thirty-eight different media offices from West Africa to East Afghanistan. Come December 2017, though, and over three-quarters of these outlets have been almost totally silenced".
>
> *Source:* "Inside the collapse of Islamic State's propaganda machine", *Wired* (20 December 2017). At http://www.wired.co.uk/article/isis-islamic-state-propaganda-content-strategy.

[44] "How do we know ISIS is losing? Now it's asking women to fight", *Washington Post* (2 November 2017). At https://www.washingtonpost.com/news/posteverything/wp/2017/11/02/how-do-we-know-isis-is-losing-now-its-asking-women-to-fight-for-it/?utm_term=.b7cc1e919795.

As the group lost territory, ISIL reduced its media production and concentrated on logistics, instruction and incitement, rather than conventional recruitment and promotion of life under the caliphate. During this time, the group released bomb and poison making instructions, together with "theological coaching on why murdering civilians is permissible, and advising on encryption and information security."[45]

Should the group continue to lose territory, propaganda will be more important to ISIL than ever. Many commentators believe that it may initially retreat into a "virtual caliphate" from where it will attempt to inspire more lone wolf attacks in an effort to remain relevant.[46]

The future for ISIL

While the caliphate appears to be on the verge of extinction, the organization of ISIL is not. The threat it has created is multidimensional, constantly and rapidly evolving, establishing provinces in countries in South and South-East Asia[47] with the ultimate goal of establishing a new satellite State.

Branches of ISIL in its provinces are increasing in influence, such as in Yemen, where the group is reported to have doubled in size in 2017.[48] In Sinai and Afghanistan, increasingly lethal attacks are being carried out in the group's name, and ISIL fighters are redeploying in Libya.[49] In the Syrian Arab Republic and Iraq, ISIL 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."[50]

What has happened to the fighters?

Research indicates that an estimated 14,910 FTFs have already left the Syrian Arab Republic and Iraq,[51] many in the early stages of the conflict. The Global Coalition has stated that since the start of Coalition action in 2014, most ISIL fighters have been killed or captured.[52] However, reports suggest that considerable numbers were still able to evade death or capture, for example leaving under the cover of civilian evacuations from cities such as Raqqa, and then using established people smuggling routes to cross the border into Turkey.[53]

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, and many are currently being

[45] "Inside the collapse of Islamic State's propaganda machine", *Wired* (20 December 2017). At http://www.wired.co.uk/article/isis-islamic-state-propaganda-content-strategy.

[46] "ISIS will remain a threat in 2018, experts warn", *NBC* (27 December 2017). At https://www.nbcnews.com/storyline/isis-terror/isis-will-remain-threat-2018-experts-warn-n828146.

[47] "New Counterterrorism 'Heat Map' Shows ISIS Branches Spreading Worldwide", *NBC* (3 August 2016). At https://www.nbcnews.com/storyline/isis-terror/new-counterterrorism-heat-map-shows-isis-branches-spreading-worldwide-n621866.

[48] "Islamic State in Yemen has 'doubled in size' since 2016: Pentagon", *Wired* (21 December 2017). At http://www.wired.co.uk/article/isis-islamic-state-propaganda-content-strategy.

[49] "Isis regroups in Libya after defeats across Iraq and Syria" *The Times* (18 August 2017). At https://www.thetimes.co.uk/article/isis-regroups-in-libya-after-defeats-across-iraq-and-syria-ph0zvtrdp.

[50] "How real is the threat of returning IS fighters?", *BBC News* (23 October 2017). At http://www.bbc.co.uk/news/world-41679377.

[51] "Foreign Fighter 'Hot Potato'", Lawfare, (26 November 2017). At https://lawfareblog.com/foreign-fighter-hot-potato. See also Richard Barrett, "Beyond the Caliphate", The Soufan Center (October 2017). At http://thesoufancenter.org/research/beyond-caliphate/.

[52] "Less than 1,000 Islamic State fighters remain in Iraq and Syria, coalition says", *Reuters*, 27 December 2017. At https://uk.reuters.com/article/uk-mideast-crisis-islamic-state/less-than-1000-islamic-state-fighters-remain-in-iraq-and-syria-coalition-says-idUKKBN1EL0QL.

[53] "Surge of Isis fighters set to hit mainland Europe, Turkey warns", *The Times*, 5 December 2017. At https://www.thetimes.co.uk/article/surge-of-isis-fighters-set-to-hit-europe-turkey-warns-75tssb2kv.

tried in Iraqi courts,[54] or are in the custody of the Syrian Democratic Forces (SDF). Some, according to the Coalition, are moving into areas controlled by the Syrian government.[55]

> "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."
>
> *Source:* General Raymond Thomas, Head of United States. Special Operations Command, speaking at the Aspen Security Forum in July 2017 about ISIL fighters. Robin Wright, "ISIS Jihadis Have Returned Home by the Thousands", *The New Yorker* (23 October 2017). At https://www.newyorker.com/news/news-desk/isis-jihadis-have-returned-home-by-the-thousands.

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, or indeed may 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. Others may choose to remain in Turkey. More recent reports indicate that fighters who remain loyal to ISIL 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.[56]

For FTFs seeking new battlefields, there are a number of potential destinations. As stated above, the branches of ISIL in Afghanistan, Libya, Sinai and Yemen are all very active, and already include FTFs in their ranks. Movement of escaping fighters to these ISIL provinces has already been reported.[57] Other terrorist groups affiliated with ISIL, 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[58] or to move to new theatres of operation. According to 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.[59] 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.[60] Iraqi and Syrian

[54] "Iraq accused of violating due process for Islamic State suspects", *Reuters*, 5 December 2017. At https://www.reuters.com/article/us-mideast-crisis-iraq-report/iraq-accused-of-violating-due-process-for-islamic-state-suspects-idUSKBN1DZ0AO.

[55] "IS Fighters Fleeing to Assad-controlled Parts of Syria", *Voice of America (Washington, D.C.)*, 27 December 2017. At https://www.voanews.com/a/islamic-state-fighters-fleeing-to-assad-controlled-parts-ofsyria/4181821.html.

[56] Robin Wright, "ISIS Jihadis Have Returned Home by the Thousands", *The New Yorker* (23 October 2017). At https://www.newyorker.com/news/news-desk/isis-jihadis-have-returned-home-by-the-thousands.

[57] Evan W. Burt, "The Sinai: Jihadism's Latest Frontline", Wilson Center (13 September 2017). At https://www.wilsoncenter.org/article/the-sinai-jihadisms-latest-frontline. "Afghan Officials: Islamic State Fighters Finding Sanctuary in Afghanistan", *Voice of America (Washington, D.C.)*, 18 November 2017. At https://www.voanews.com/a/afghan-officials-islamic-state-finds-sanctuary-in-afghanistan/4122270.html.

[58] United Nations Security Council Counter-terrorism Committee, "Foreign terrorist fighters" (accessed 28 March 2018). At https://www.un.org/sc/ctc/focus-areas/foreign-terrorist-fighters/.

[59] "Islamic State and the crisis in Iraq and Syria in maps", *BBC News*, 21 December 2017. At http://www.bbc.co.uk/news/world-middle-east-27838034.

[60] "Paris attacks: Who were the attackers?", *BBC*, 27 April 2016. At http://www.bbc.co.uk/news/world-europe-34832512. "Paris attacks: IS claims two attackers were Iraqi nationals", *BBC News*, 20 January 2016. At http://www.bbc.co.uk/news/world-europe-35360354.

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.[61]

Al-Qaida

While fear of an attack by ISIL is the highest ranked concern of the public and of governments globally,[62] the threat of other terrorist organizations should not be forgotten. Al-Qaida in particular seeks to make a comeback. Al-Qaida has pursued planning for 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.[63]

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 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.[64] 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 United States airstrikes against suspected bomb factories in the Syrian Arab Republic.[65]

Al-Qaida continues to be a significant worldwide threat, with its regional offshoots conducting mass-casualty attacks.[66] 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.[67] In an attempt to expand its sphere of influence, in 2017 Al-Qaida announced a new affiliate in Jammu and Kashmir.[68] 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, narrating 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, states that followers who live in the West do not need to migrate, instructing them on how to conduct martyrdom attacks in their home lands. Outside of western countries, he urges Muslims to rise up against "tyranny".[69]

[61] 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.

[62] "Globally, People Point to ISIS and Climate Change as Leading Security Threats", Pew Research Center (1 August 2017). At http://www.pewglobal.org/2017/08/01/globally-people-point-to-isis-and-climate-change-as-leading-security-threats/.

[63] Katherine Zimmerman, "Testimony: 'Al Qaeda's strengthening in the shadows", statement before the House Homeland Security Committee Subcommittee on Counterterrorism and Intelligence (13 July 2017). At http://www.aei.org/publication/testimony-al-qaedas-strengthening-in-the-shadows/.

[64] "What is the Khorasan Group?", *BBC News*, 24 September 2014. At http://www.bbc.co.uk/news/world-middle-east-29350271. 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). At https://ctc.usma.edu/posts/a-view-from-the-ct-foxhole-lisa-monaco-former-assistant-to-president-barack-obama-for-homeland-security-and-counter-terrorism.

[65] "What is the Khorasan Group?", *BBC News*, 24 September 2014. At http://www.bbc.co.uk/news/world-middle-east-29350271.

[66] "Country Reports on Terrorism 2016", United States Department of State. At https://www.state.gov/j/ct/rls/crt/2016/272228.htm.

[67] Katherine Zimmerman, "Testimony: 'Al Qaeda's strengthening in the shadows", statement before the House Homeland Security Committee Subcommittee on Counterterrorism and Intelligence (13 July 2017). At http://www.aei.org/publication/testimony-al-qaedas-strengthening-in-the-shadows/.

[68] "How Al-Qaida Came to Kashmir", *The Diplomat* (20 December 2017). At https://thediplomat.com/2017/12/how-Al-Qaida-came-to-kashmir/.

[69] "Hamza Bin Laden Calls on Muslims to Avenge the Death of His Father, Osama", *Newsweek* (7 November 2017). At http://www.newsweek.com/hamza-bin-laden-calls-muslims-avenge-death-his-father-osama-704276. "Al-Qaida Makes its Move with a Video Primer by Hamza bin Laden", The International Center for the Study of Violent Extremism (20 June 2017). At http://www.icsve.org/brief-reports/Al-Qaida-makes-its-move-hamza-bin-laden/?utm_content=buffere78e8&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

In the Syrian Arab Republic, 20 per cent of FTFs are estimated to have gone to militant groups other than ISIL,[70] chiefly, the Al-Qaida-affiliated Al-Nusrah Front. In July 2016, the Al-Nusrah Front publicly disaligned 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",[71] its stated objective is to dominate "the armed opposition within Syria's civil war, with the ultimate goal of toppling Bashar al-Assad and establishing a jihadist emirate in Syria."[72] In 2017, it announced an alliance with four smaller factions to form Hayat Tahrir Al-Sham (HTS), or Liberation of the Levant Organization.[73]

Many analysts view the Jabhat Fateh Al-Sham element of the alliance "as a covert Al-Qaida affiliate",[74] simply rebranded to appear less extreme and win the support of other militant factions and the civilian population, while also trying 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"[75] in Idlib province in the north of the Syrian Arab Republic. Standing to profit both politically and militarily from any decline of ISIL, the numbers of fighters are likely to grow as it integrates units from other defeated rebel groups. To date, the group remains relatively unscathed by any foreign military action[76]. The number of FTFs that remain with HTS is unknown. If HTS starts to suffer losses, these FTFs may also seek to return home.

1.4 Regional situation

The threat level in South and South-East Asia continues to rise, with both ISIL and Al-Qaida wanting to establish a stronger operational presence in the region.[77] The attempted takeover of the city of Marawi in the Philippines in 2017 has emphasized the seriousness of ISIL's attempt to establish a province, and has demonstrated the potential for attracting FTFs from both within the region and outside.

FTFs are also likely to return to South and South-East Asia if they are defeated in foreign conflicts, bringing enhanced military capability and the motivation to conduct attacks. Their skills are likely to bolster local terrorist groups. The region may become "a preferred relocation destination" for displaced FTFs from other countries, "thereby resulting in the conflict being exported to the region".[78]

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

[71] "Independent Assessment of U.S. Government Efforts against Al-Qaida", CAN Center for Strategic Studies (October 2017). At https://www.academia.edu/35170628/Independent_Assessment_of_U.S._Government_Efforts_against_Al-_Qaeda.

[72] Ibid.

[73] "Tahrir al-Sham: Al-Qaida's latest incarnation in Syria", *BBC News*, 28 February 2017. At http://www.bbc.co.uk/news/world-middle-east-38934206.

[74] Zack Gold, "Al-Qaida-Syria (AQS): An Al-Qaida Affiliate Case Study", Center for Naval Analyses (October 2017). At http://www.dtic.mil/dtic/tr/fulltext/u2/1041744.pdf.

[75] Brett McGurk, statement of the United States Special Presidential Envoy for the Global Coalition to Counter ISIS, to Middle East Institute session on United States Counterterrorism Policy (July 2017). At https://www.youtube.com/watch?v=UgzqabDYK7I#t=59m03s.

[76] "Al-Qaida Affiliate and Ahrar al-Sham Compete for Control in Idlib", Omran Center for Strategic Studies (3 July 2017). At http://en.omrandirasat.org/publications/reports/Al-Qaida-affiliate-and-ahrar-al-sham-compete-for-control-in-idlib.html.

[77] United Nations Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015), "Twentieth report of the Analytical Support and Sanctions Monitoring Team" (7 August 2017). At http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2017/573.

[78] United Nations Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015), "Nineteenth report of the Analytical Support and Sanctions Monitoring Team" (11 January 2017). At https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/000/13/PDF/N1700013.pdf?OpenElement.

Table 1. Estimated figures of foreign terrorist fighter travel or interception since 2012 (figures from Member States, as of October 2017)

	Travelled to and arrived in the Syrian Arab Republic/Iraq	*Percentage women and children*	*Returned from the Syrian Arab Republic/Iraq*	*Prevented from leaving home country*	*Prevented from continuing travel by Turkey*
Bangladesh	40[a]	[b]	[b]	[b]	[b]
Indonesia	671	31% (208)	84	66	639[c]
Malaysia	95	30% (29)	8	[b]	265
Maldives	49[d]	[b]	0	47	5
Philippines	4[e]	[b]	[b]	[b]	[b]

[a] Includes small number of women.

[b] No official record available.

[c] About 40 per cent women and children.

[d] Fighters only.

[e] Other sources have reported between 12 and 100 FTFs departing from the Philippines.

About 1,000 South-East Asians are estimated to have travelled to ISIL-controlled territory in the Syrian Arab Republic and Iraq, with at least the same number going from South Asia, but not all to fight.[79] Data supplied by Member States (see table above) shows that women and children form a high percentage of those that have successfully reached the Syrian Arab Republic from South-East Asia (about 30 per cent of the total). On a per capita basis, Maldives is one of the largest contributors of FTFs to the Syrian Arab Republic and Iraq,[80] reinforcing concerns expressed about the radicalization of young Maldivians and their support for transnational terrorist groups.[81]

Terrorist attacks

Bangladesh, Indonesia, Malaysia and the Philippines all suffered terrorist attacks in 2016 resulting in the loss of more than 70 lives (including perpetrators). The majority of the attacks were either inspired by, or to different degrees directed by, ISIL. For instance:

- *Bangladesh:* Al-Qaida in Iraq and the Syrian Arab Republic claimed responsibility for two machete attacks.[82]
- *Indonesia:* Five attacks in the period, with one claimed by ISIL (a multiple bombing and firearms attack in central Jakarta).[83]

[79] Richard Barrett, "Beyond the Caliphate", The Soufan Center (October 2017). At http://thesoufancenter.org/research/beyond-caliphate/.

[80] Sudha Ramachandran, "The Maldives: Losing a Tourist Paradise to Terrorism", The Jamestown Foundation (22 January 2016). At https://jamestown.org/program/the-maldives-losing-a-tourist-paradise-to-terrorism/. The United Nations, Soufan Group and others estimate the number of Maldivian FTFs even higher at 200.

[81] "Country Reports on Terrorism 2016: Maldives", United States Department of State. At https://www.state.gov/j/ct/rls/crt/2016/272233.htm#MALDIVES.

[82] "Country Reports on Terrorism 2016: Bangladesh", United States Department of State. At https://www.state.gov/j/ct/rls/crt/2016/272233.htm#BANGLADESH.

[83] "Country Reports on Terrorism 2016: Indonesia", United States Department of State. At https://www.state.gov/j/ct/rls/crt/2016/272230.htm#Indonesia.

- *Malaysia:* one attack, claimed by ISIL (the Movida bar bombing).[84]
- *Philippines:* the ISIL-affiliated Maute Group carried out about 22 attacks (including a bomb attack on a public market in Davao City).[85] Abu Sayyaf Group, also affiliated with ISIL, conducted attacks against the Philippines army together with about 19 kidnappings for ransom.[86]

In 2017, the number of deaths from terrorism increased as a result of the siege of Marawi, leading to the Philippines being called, at one point, "the deadliest ISIL franchise outside Iraq and Syria".[87] Other notable attacks in 2017 included the suicide bombings in Jakarta in May that killed three policemen, with responsibility claimed by ISIL.[88]

In the face of these attacks, security services and law enforcement agencies throughout the region have combined efforts to successfully prevent other terrorist plots from coming to fruition, with significant numbers of arrests and successful prosecutions.[89] At the same time authorities are still required to deal with the separate threat posed by domestic terrorism. For instance, in Bangladesh in 2017, some 905 terrorist suspects were reported to have been arrested and a further 52 killed in fighting with security forces (predominantly from the groups Jamaat-e-Islami and Neo Jamaat-ul-Mujahideen), with several large seizures of explosives and firearms.[90]

Pro-ISIL groups and individuals will undoubtedly plot to conduct further mass casualty attacks, focusing on soft targets, law enforcement, and Western and national government interests.[91]

[84] "Country Reports on Terrorism 2016: Malaysia", United States Department of State. At https://www.state.gov/j/ct/rls/crt/2016/272230.htm#Malaysia.

[85] "Overview: Terrorism in 2016", University of Maryland Study of Terrorism and Responses to Terrorism. At https://www.start.umd.edu/pubs/START_GTD_OverviewTerrorism2016_August2017.pdf. "Marawi, the 'East Asia Wilayah' and Indonesia", Institute for Policy Analysis of Conflict Report No. 38 (21 July 2017). At http://file.understandingconflict.org/file/2017/07/IPAC_Report_38.pdf.

[86] "Terrorist Activities of the Abu Sayyaf", The Mackenzie Institute, (14 March 2017). At http://mackenzieinstitute.com/terrorist-activities-abu-sayyaf/. "Report: ISIS franchise in the Philippines carries out its first attack", *Jerusalem Post* (10 May 2016). At http://www.jpost.com/Middle-East/ISIS-Threat/Report-ISIS-franchise-in-the-Philippines-carries-out-its-first-attack-453604.

[87] "Considering Claimed Attacks: Islamic State's Hidden Narrative", Terrorism Research & Analysis Consortium (Internet Archive Wayback Machine preservation of page on 28 October 2017). At https://web.archive.org/web/20171028025146/; https://www.trackingterrorism.org/article/considering-claimed-attacks-islamic-states-hidden-narrative/introduction-summer-2017-executi.

[88] "Islamic State claims responsibility for Jakarta bus station attacks", *Channel News Asia* (26 May 2017). At https://www.channelnewsasia.com/news/asiapacific/islamic-state-claims-responsibility-for-jakarta-bus-station-8884438.

[89] For example, "Special Branch drop IS bombshell, reveal 14 attack attempts in M'sia foiled", *New Straits Times* (6 December 2016). At https://www.nst.com.my/news/2016/12/194965/special-branch-drop-bombshell-reveal-14-attack-attempts-msia-foiled?m=1. "Indonesia and the Islamic State Threat", *The Diplomat*, (15 March 2017). At https://thediplomat.com/2017/03/indonesia-and-the-islamic-state-threat/.

[90] "Relentless Response", *South Asia Intelligence Review* (1 January 2018). At http://www.satp.org/satporgtp/sair/Archives/sair16/16_27.htm#assessment1.

[91] United Nations Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015), "Twentieth report of the Analytical Support and Sanctions Monitoring Team" (7 August 2017). At http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2017/573.

Case study: Malaysia—Movida bar bombing 2016

On 28 June 2016 at 2:30 a.m., a bar in Puchong, Malaysia was attacked by two men, who threw a grenade into the premises while 20 customers were watching a football match. The explosion injured eight people, some seriously. The attackers, Imam Wahyudin Karjono, 21, and Jonius Indie, 24, left the scene on a motorcycle, but were both arrested within three days of the attack. The police investigation revealed that the two had received instructions from a Malaysian in the Syrian Arab Republic, Muhamad Wanndy Mohamad Jedi, a commander of Khatibah Nusantara, the joint Indonesian-Malaysian wing of ISIL.

This was the first attack by ISIL in Malaysia. The men were charged with eight counts of attempted murder under Section 307 of the Penal Code, one count of using a hand grenade to commit a crime under the Firearms (Heavy Penalties) Act 1971, and under Section 130(c)(1)*(b)* of the Penal Code for committing terrorist acts. In March 2017, they pleaded guilty at Kuala Lumpur High Court and were each sentenced to 25 years imprisonment. In May 2017, Jedi was reported to have been killed in Raqqa.[a]

[a] "Nightclub blast in Puchong linked to IS: Malaysian police chief", *Channel News Asia* (4 July 2016). At http://www.channelnewsasia.com/news/asiapacific/nightclub-blast-in-puchong-linked-to-is-malaysian-police-chief-7946138. "Movida bombers sentenced to 25 years' jail", *New Straits Times* (29 March 2017). At https://www.nst.com.my/news/2017/03/225333/movida-bombers-sentenced-25-years-jail. "Top Malaysian ISIS terrorist Muhammad Wanndy Mohamed Jedi is dead: Police chief", *The Straits Times* (8 May 2017). At http://www.straitstimes.com/asia/se-asia/top-malaysian-isis-terrorist-muhammad-wanndy-mohamed-jedi-is-dead-police-chief.

Regional influence of ISIL and Al-Qaida

Although terrorist groups in the region are believed to be ideologically divided on ISIL, its propaganda messaging has resonated with extremists in the region, especially with the younger generation.[92] Groups in Indonesia and the Philippines have pledged allegiance to the leader of ISIL, Abu Bakr al-Baghdadi, the most prominent group to do so, being the Abu Sayyaf Group.[93]

As ISIL fought to retain territory, an audio message from al-Baghdadi was released in November 2016, appealing to the "caliphate's soldiers" outside of Iraq and the Syrian Arab Republic to take their own action and launch attacks. Included in the countries in which he urged action were Bangladesh, Indonesia and the Philippines.[94] The group's online magazine *Rumiyah* has been issued in 11 languages, including English and Bahasa Indonesia, with editions praising terrorist action in the Philippines, Bangladesh and elsewhere in Asia.[95]

Al-Qaida in the Indian subcontinent has pledged to turn India, Pakistan and Bangladesh "into an Islamic subcontinent".[96] Jemaah Islamiyah is reported to have sent fighters to the Syrian Arab Republic

[92] Ibid.

[93] "Islamic State's 43 Global Affiliates", IntelCenter (15 December) 2015. At https://intelcenter.com/maps/is-affiliates-map.html#gs.7BiwAow.

[94] "The Jihadi Threat: ISIS, Al Qaeda, and Beyond", United States Institute of Peace (December 2016/January 2017). At https://www.usip.org/sites/default/files/The-Jihadi-Threat-ISIS-Al-Qaeda-and-Beyond.pdf.

[95] "Islamic State's (ISIS, ISIL) Horrific Magazine", Clarion Project (10 September 2014). At https://clarionproject.org/islamic-state-isis-isil-propaganda-magazine-dabiq-50/. "'Isis' new magazine Rumiyah shows the terror group is 'struggling to adjust to losses'", *The Independent* (6 September 2016). At https://www.independent.co.uk/news/world/middle-east/isis-propaganda-terror-group-losses-syria-iraq-a7228286.html.

[96] "Al-Qaeda's 'Indian subcontinent' branch re-focuses on India, Bangladesh", *BBC News* (27 November 2017). At https://monitoring.bbc.co.uk/product/c1dnqkka.

for training by the Al-Qaida linked Al-Nusrah Front, to gain combat experience and military training in order to serve the group's long-term goal of amalgamating Indonesia, Malaysia and the southern Philippines into a regional Islamic State.[97] Although not responsible for any recent attacks, Jemaah Islamiyah continues to represent a major regional threat.[98]

The region's foreign terrorist fighters in the Syrian Arab Republic

A special unit named Katibah Nusantara (the Malay Archipelago Unit for ISIL) was established by ISIL in September 2014 for Malaysian and Indonesian FTFs. The unit initially demonstrated its military capability by capturing several Kurdish-held areas in Iraq.[99] Indonesian and Malaysian recruits have engaged in all aspects of the conflict, including use of heavy weapons, bomb making and carrying out suicide attacks; they also have appeared as executioners in beheading videos.[100] While fighting in the Syrian Arab Republic and Iraq, Katibah Nusantara also assists ISIL's ambition to make South-East Asia part of its worldwide caliphate[101] through encouraging attacks in the region.

One of the group's leaders, the Indonesian Bahrun Naim, has called in his blog for "lone wolves" to "rise up against the Indonesian archipelago". Naim is suspected of organizing the attack in Jakarta in January 2016, which resulted in the deaths of four civilians and the four perpetrators.[102]

In June 2016, the Malaysian FTF Mohd Rafi Udin appeared in a video produced by Katibah Nusantara, alongside a Filipino[103] and an Indonesian fighter, in which they beheaded three purported spies. Urging war against "Taghut governments",[104] they called upon supporters in their home countries to stage attacks to kill "disbelievers". Udin also issued a threat against the Royal Malaysia Police.[105]

Bangladeshi and Maldivian FTFs have similarly been heavily engaged in fighting in the Syrian Arab Republic and have used it as a base to issue propaganda.[106] Bilad Al Sham, the media section of Maldivians fighting in the Syrian Arab Republic, in 2016 released a YouTube video in which Maldivian FTFs are seen shooting at pictures of previous presidents of the country and denouncing their national leaders as "taghut".[107]

The situation in the Philippines is complex, with numerous militant groups engaged in terrorist activity and various factions within them pursuing different objectives. Prominent among these has

[97] Sidney Jones, "National Security & Cross Border Security Threat in Asean", presentation at Civil Society Conference on National Security in Kula Lumpur (18 August 2016). At https://www.youtube.com/watch?v=AR0Rfaoxt4k. "Indonesian and Malaysian Support for The Islamic State", USAID, (6 January 2016). At https://www.globalsecurity.org/military/library/report/2016/PBAAD863.pdf.

[98] "The Re-emergence of Jemaah Islamiyah", Institute for Policy Analysis of Conflict (27 April 2017). At http://www.understandingconflict.org/en/conflict/read/59/The-Re-emergence-of-Jemaah-Islamiyah.

[99] Jasminder Singh, "Katibah Nusantara: Islamic State's Malay Archipelago Combat Unit", RSIS Commentary No. 126 (26 May 2015). At https://www.rsis.edu.sg/rsis-publication/icpvtr/co15126-katibah-nusantara-islamic-states-malay-archipelago-combat-unit/#.WjZbPjfLj-s.

[100] "Indonesian and Malaysian Support for The Islamic State", USAID, (6 January 2016). At https://www.globalsecurity.org/military/library/report/2016/PBAAD863.pdf. "Young Malaysian ISIS suicide bomber 'killed 14 in Syria'", *The Straits Times* (18 December 2016). At http://www.straitstimes.com/asia/se-asia/young-malaysian-isis-suicide-bomber-killed-14-in-syria.

[101] United Nations Security Council Counter-Terrorism Committee Executive Directorate, "Global survey of the implementation of Security Council resolution 1373 (2001) by Member States" (20 January 2016). At https://www.un.org/sc/ctc/wp-content/uploads/2016/10/Global-Implementation-Survey-1373_EN.pdf.

[102] "Jakarta attacks: Profile of suspect Bahrun Naim", *BBC News* (14 January 2016). At http://www.bbc.co.uk/news/world-asia-35316915. "Jakarta Terror Attack 14/1/2016 - What do we know?", IDC Herzliya International Institute for Counter-Terrorism (24 January 2016). At https://www.ict.org.il/Article/1591/Jakarta-Terror-Attack#gsc.tab=0.

[103] "Filipino millennial joins ISIS in Syria", Rappler (27 January 2017). At https://www.rappler.com/newsbreak/in-depth/159609-millennial-terrorism-isis-philippines.

[104] In this context the phrase is used to mean "false gods" or "tyrants", leaders who are considered not to be following the teachings of Allah by not applying sharia law.

[105] "Police brace for attacks as IS gains strength", *New Straits Times* (23 June 2016). At https://www.nst.com.my/news/2016/06/153883/police-brace-attacks-gains-strength.

[106] "How many Bangladeshis have joined IS?", *Dhaka Tribune* (28 June 2017). At http://www.dhakatribune.com/bangladesh/crime/2017/06/28/many-bangladeshis-joined/.

[107] "Maldives fighters in Syria warn government and leaders", *Maldives Independent* (3 June 2016). At http://maldivesindependent.com/feature-comment/maldives-fighters-in-syria-warn-government-and-leaders-124623.

been the Abu Sayyaf Group and the Maute Group, which have been responsible for bombings, attacks against government forces, piracy, kidnapping and the beheading of hostages including foreign nationals.

In July 2014, Isnilon Hapilon, the leader of the Abu Sayyaf Group, pledged allegiance in a YouTube video to Abu Bakr al-Baghdadi and ISIL. This was followed by other groups, including in 2015 by the leaders of the Maute Group, the brothers Abdullah and Omar Maute, thereafter referring to themselves as Islamic State-Ranao. In April 2016, ISIL's weekly newsletter Al Naba announced that Hapilon had been appointed as emir of all ISIL forces in the Philippines.[108]

In May 2017, fighters of the Abu Sayyaf Group and the Maute Group joined forces with other local factions in an attempt to seize control of the city of Marawi. At that time, the Solicitor General of the Philippines stated that there were about 23 "terrorist organizations with ISIL links" operating on the island of Mindanao, all with the objective of removing the island's allegiance to the Philippines government.[109] Five months later, the Philippines military regained control of Marawi.

Despite the deaths of its leaders during the battle, the Maute Group is reported to have continued recruiting since the end of the siege, utilizing social media and offering "financial remuneration" to new fighters.[110]

Case study: The Philippines—Marawi siege 2017

The siege of Marawi was triggered when on 23 May 2017, the Philippines military moved into the city in an attempt to arrest Isnilon Hapilon, and clashed with armed fighters from the Abu Sayyaf Group and the Maute Group. Hapilon had moved to central Mindanao to find a suitable area to establish a province of ISIL's caliphate.[a] The scale of the response that followed showed those plans were already at an advanced stage.

The fighting quickly spread throughout the city, with other insurgent groups joining forces and large areas including government buildings being taken over. A Catholic church, the city prison and schools were set on fire, with churchgoers and residents taken hostage, prison inmates freed and a police officer beheaded. President Duterte placed the island of Mindanao under martial law.[b]

The Philippines Army, Air Force and Navy became involved in the ensuing battle, carrying out artillery shelling and air strikes on a near-daily basis in an attempt to retake the city. ISIL was quick to publicize the successes in its name, publishing videos showing masked fighters placing black ISIL flags across the city.[c] Evidence showed the use of child soldiers recruited locally by the Maute Group, some "as young as 12 years

[108] "Islamic State details activity in the Philippines", *Long War Journal* (12 June 2016). https://www.longwarjournal.org/archives/2016/06/islamic-state-details-activity-in-the-philippines.php. "Maute rebel group: A rising threat to Philippines", BBC (31 May 2017). At http://www.bbc.co.uk/news/world-asia-40103602. "Philippines unrest: Who are the Abu Sayyaf group?", *BBC News* (14 June 2016). At http://www.bbc.co.uk/news/world-asia-36138554.

[109] "20 IS-linked terrorist groups operating in Mindanao – Calida", *The Inquirer* (19 June 2017). At http://newsinfo.inquirer.net/906858/20-is-linked-terrorist-groups-operating-in-mindanao-calida.

[110] "ISIS Is Gearing Up For A Comeback In The Philippines", Task & Purpose (18 December 2017). At http://taskandpurpose.com/isis-gearing-comeback-philippines/.

old".[d] From the Syrian Arab Republic, ISIL reportedly sent funds via Indonesia,[e] and in official media releases urged fighters to travel to the Philippines.

Current estimates indicate that up to 30 Indonesians (some having travelled from the Syrian Arab Republic) and 16 Malaysians were among the FTFs fighting in Marawi.[a] The Malaysian contingent included Amin Baco, who since then may have become the new ISIL leader in the region, and Dr. Mahmud bin Ahmad, a senior member of Aby Sayyaf involved in recruitment and funding.[e]

On 23 October 2017, five months after the start of the siege, Philippine Defence Secretary Delfin Lorenzana declared an end to combat operations, stating that "There are no more militants in Marawi City".[f] Hapilon and the two Maute brothers were killed. The conflict has been described as "the longest and bloodiest Philippine military operation since World War II".[g] According to official government statistics, at least 920 militants, 165 soldiers and 47 civilians were killed during the battle. 1,780 hostages were eventually rescued. Around 360,000 people were displaced by the fighting, and the government estimated it would cost $1 billion to rebuild the city over several years.[h]

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

[b] "What happened in Marawi?", *Al Jazeera* (29 October 2017). At http://www.aljazeera.com/indepth/features/2017/10/happened-marawi-171029085314348.html.

[c] "'The Battle of Marawi.' Death and Destruction in The Philippines", Amnesty International (2017). At http://www.refworld.org/pdfid/5a0e99724.pdf.

[d] "Nearly half of remaining Maute fighters in Marawi are children", *CNN Philippines* (27 August 2017). At http://cnnphilippines.com/news/2017/08/27/maute-fighters-marawi-children.html.

[e] "Marawi, The 'East Asia Wilayah' and Indonesia", Institute for Policy Analysis of Conflict, Report No. 38 (21 July 2017). At https://www.academia.edu/33978316/MARAWI_THE_EAST_ASIA_WILAYAH_AND_INDONESIA.

[f] "Lorenzana: No more militants in Marawi City", *The Philippine Star* (23 October 2017). At http://www.philstar.com/headlines/2017/10/23/1751650/lorenzana-no-more-militants-marawi-city.

[g] "Marawi: 153 Days and More", *Rappler* (23 October 2017). At https://www.rappler.com/newsbreak/in-depth/186075-marawi-series-rappler-timeline.

[h] "Pictures reveal devastation to Philippine city of Marawi after Isis siege", *The Independent* (25 October 2017). At http://www.independent.co.uk/news/world/asia/marawi-city-photos-philippines-isis-siege-islamic-state-muslim-army-a8019266.html.

Foreign terrorist fighters from outside the region

Fighters of the Chinese Uighur minority, linked to the Eastern Turkistan Islamic Movement, have been arrested or killed by Indonesian security forces in Poso, Indonesia. Those fighters were embedded with the local ISIL-aligned terrorist group Mujahidin Indonesia Timur.[111] Two Chinese Uighurs have been charged in relation to the bombing in 2015 at the Erawan Shrine in Bangkok, which killed 20 people.[112]

FTFs have used ASEAN Member States to transit as part of broken travel patterns disguising their true destination, either en route to the Syrian Arab Republic or returning. Due to generous visa-free policies, many FTFs are reportedly requesting deportation from Turkey to South-East Asia rather than to their home countries.[113] In August 2017, Malaysian authorities were searching for 16 suspected FTFs who had arrived from Turkey after being caught trying to enter the Syrian Arab Republic to join

[111] "The Uighurs and China's Regional Counter-Terrorism Efforts", *Terrorism Monitor* (15 August 2017). At https://jamestown.org/program/the-uighurs-and-chinas-regional-counter-terrorism-efforts/. "Facing down terror", *Sunday Star* (23 April 2017). At https://www.thestar.com.my/news/nation/2017/04/23/facing-down-terror-the-man-who-leads-a-bukit-aman-division-in-fighting-terrorism-has-many-tales-to-s/.

[112] "No justice in sight two years after Erawan shrine bombing in Bangkok", *Asia News Network* (18 August 2017). At http://www.straitstimes.com/asia/se-asia/no-justice-in-sight-two-years-after-erawan-shrine-bombing-in-bangkok.

[113] "Beyond the Caliphate", The Soufan Center (October 2017). At http://thesoufancenter.org/research/beyond-caliphate/.

ISIL. The men, all non-Malaysian citizens, had requested to be sent there because of visa-free arrangements with their home countries.

FTFs are attempting to exploit this situation, seeing South-East Asia not only as a transit zone but also a potential safe haven and theatre of operations. The United Nations Security Council has noted, "Once fighters arrive in one of the countries of South-East Asia, the porous nature of the maritime borders in the region allows movement between the Philippines, Indonesia and Malaysia without detection".[114] In 2017, more than 45 suspected FTFs were arrested in Malaysia, believed to be "seeking shelter, collecting funds, planning to either launch attacks here [Malaysia] or using Malaysia as their operation base to launch attacks at other countries".[115] Police alleged they were members of the Abu Sayyaf Group, ISIL (including "three southern Iraq commanders"),[116] an Albanian group linked to ISIL, the Bangladeshi group Jamaat-ul-Mujahideen, and Fetullah Turki.[117] They originated from Albania, Bangladesh, China, Indonesia, Iraq, Maldives, Morocco, Palestine, the Philippines and Yemen .[118]

Case study: region as a transit point

The French citizen charged with the attack at the Jewish Museum in Brussels in May 2014, in which four people were shot dead, travelled from the Syrian Arab Republic via Istanbul, Malaysia, Singapore and Hong Kong before entering Belgium via Frankfurt.

Source: "French militant in Brussels terror attack transited in Malaysia", *Channel News Asia* (29 Mar 2017). At http://www.channelnewsasia.com/news/asiapacific/french-militant-in-brussels-terror-attack-transited-in-malaysia-8594492.

FTFs returning to the region may also look for new conflicts. In the first months of 2017, human rights violations and widespread and systematic violence against the Rohingya in Myanmar led to about 655,000 displaced Rohingya arriving in Bangladesh.[119] While the militant group Arakan Rohingya Salvation Army is conducting its own campaign of attacks against military targets in Myanmar,[120] migrants may be susceptible to radicalization from either ISIL or Al-Qaida and seek the outside support of FTFs.

In a video message released in September 2017 by Al-Qaida in the Arabian Peninsula, a senior leader called upon Muslims in Bangladesh, India, Indonesia and Malaysia to support their Rohingya

[114] United Nations Security Council, 8116th meeting (28 November 2017). At http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_pv_8116.pdf.

[115] "Malaysian police arrest 45 foreign terrorist fighters", *The Straits Times* (14 October 2017). At http://www.straitstimes.com/asia/se-asia/malaysian-police-arrest-45-foreign-terrorist-fighters.

[116] Ibid.

[117] "OIC lists Gülen network as 'terror group'", *Hurriyet Daily News* (19 October 2016). At http://www.hurriyetdailynews.com/oic-lists-gulen-network-as-terror-group--105128.

[118] "Islamic State remains the top terror threat for Malaysia in 2018: Police", *The Malaysian Times* (31 December 2017). At https://www.themalaysiantimes.com.my/islamic-state-remains-top-terror-threat-malaysia-2018-police/.

[119] "IOM Bangladesh: Rohingya Refugee Crisis Response", IOM External Update (14 December 2017). At https://reliefweb.int/sites/reliefweb.int/files/resources/2017-12-14%20-%20IOM%20Rohingya%20Crisis%20Response%20-%20External%20Sitrep.pdf.

[120] "Myanmar Rohingya militants Arsa vow to fight on after attack", *BBC News* (7 January 2018). At http://www.bbc.co.uk/news/world-asia-42595275.

Muslim brethren against the "enemies of Allah".[121] A week later, Al-Shabaab, the Somali Al-Qaida affiliate, issued a similar message urging attacks in support of "persecuted" Rohingya Muslims.[122]

1.5 Typology and motivation

Who are foreign terrorist fighters?

A number of studies have been conducted into the backgrounds of the current wave of foreign terrorist fighters. The one common conclusion to emerge is that there is no single profile for those who become FTFs, with recruits being drawn from a diverse range of age, educational, vocational and socio-economic backgrounds. While the majority of male recruits are in the age range 20-30, young teenagers and people up to 60 years old have joined ISIL.[123] Although a large proportion are young, economically disadvantaged males from socially or politically marginalized backgrounds,[124] others are affluent and well-educated. "Some are school dropouts, others have graduate qualifications. Some are itinerant workers, but others have successful professional careers as doctors, teachers, engineers and public servants".[125] Many have troubled pasts, but others would have had great prospects had they remained at home. Some are pious, but others are not. Some have criminal records (often for petty crime), but a large percentage are previously unknown to law enforcement.

How are they recruited?

Community-based networks have 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.[126] Religious leaders have been responsible for radicalization and guiding individuals on a path to violent extremism. Membership in non-violent radical groups and association with activists has also played a part in influencing prospective fighters. The average recruitment age has dropped, and FTFs are being recruited while still at school or college. Da'wah (religious outreach) groups on university campuses have also been cited as places of recruitment.

Some recruits are already members of terrorist groups or previous FTFs, but many have travelled without any prior contact with the terrorist organizations with whom they seek to fight. Others have been groomed and facilitated in their travel by recruiters working online, including by fighters who have already gone to the Syrian Arab Republic and are reaching out to their friends and acquaintances, encouraging them to do the same.

In June 2017, a report from the European Union Radicalisation Awareness Network stated: "… [ISIL's] recruitment focuses on grooming techniques that exploit identity confusion and focus on persuasion,

[121] "Yemeni al Qaeda leader calls for attacks in support of Myanmar's Rohingya", *Reuters* (2 September 2017). At https://www.reuters.com/article/us-myanmar-rohingya-alqaeda/yemeni-Al-Qaida-leader-calls-for-attacks-in-support-of-myanmars-rohingya-idUSKCN1BD0U8.

[122] "Gulf of Aden Security Review", *Critical Threats* (8 September 2017). At https://www.criticalthreats.org/briefs/gulf-of-aden-security-review/gulf-of-aden-security-review-september-8-2017#_ftn6.

[123] "A New Age of Terror? Older Fighters in the Caliphate", Combating Terrorism Center (4 May 2017). At https://ctc.usma.edu/posts/a-new-age-of-terror-older-fighters-in-the-caliphate.

[124] 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). At http://www.un.org/en/counterterrorism/assets/img/Report_Final_20170727.pdf.

[125] "Indonesian and Malaysian Support for The Islamic State", USAID, (6 January 2016). At https://www.globalsecurity.org/military/library/report/2016/PBAAD863.pdf.

[126] 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). At http://www.un.org/en/counterterrorism/assets/img/Report_Final_20170727.pdf.

emotional manipulation and total obedience … recruiters identify individual psychological weaknesses and skilfully exploit these through online and offline techniques".[127]

Advances in means and ease of communication over the Internet, through social networking sites and chat applications, have played a major role in assisting recruiting. Even when there is no online contact, the Internet enables potential recruits to view terrorist propaganda and discover more information about the conflict, thus playing a key role in reinforcing decisions.[128] In a recent report from the United Nations Counter-Terrorism Executive Directorate on the implementation of Security Council resolution 2178 in States affected by FTFs, it was 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.[129]

Why do individuals become foreign terrorist fighters?

The motivation for wanting to join terrorist organizations also varies significantly. There is no single psychological profile.

Studies into those who have travelled to the Syrian Arab Republic have found a number of factors that account for the movement of recruits towards ISIL, including political, religious and personal reasons:

- *Living in a caliphate:* a desire, coupled with a sense of duty, to live within a caliphate under the governance of sharia law in a manner that they believe was ordained by the Prophet himself. The narrative of ISIL involves labelling governments in Muslim countries as un-Islamic, 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 was perceived as a utopian destination for the pious Muslim.
- *A just war:* especially in the early stages of the conflict in the Syrian Arab Republic, many FTFs saw themselves in the role of defending Islam and protecting followers of their own religion, 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.[130]

[127] "Responses to returnees: Foreign terrorist fighters and their families", Radicalisation Awareness Network (July 2017). At https://ec.europa.eu/home-affairs/sites/homeaffairs/files/ran_br_a4_m10_en.pdf.

[128] 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). At http://www.un.org/en/counterterrorism/assets/img/Report_Final_20170727.pdf.

[129] United Nations Security Council Counter-Terrorism Committee Executive Directorate, "Implementation of Security Council resolution 2178 (2014) by States affected by foreign terrorist fighters: A compilation of three reports (S/2015/338; S/2015/683; S/2015/975)". At https://www.un.org/sc/ctc/wp-content/uploads/2016/09/FTF-Report-1-3_English.pdf.

[130] 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). At http://www.un.org/en/counterterrorism/assets/img/Report_Final_20170727.pdf.

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

[a] "The Islamic State's Perversion of Hijra", Project Syndicate (11 August 2015). At https://www.project-syndicate.org/commentary/meaning-of-hijra-jihad-islamic-state-by-rebecca-gould-2015-08.

[b] "Dabiq", Issue 3. At http://www.ieproject.org/projects/dabiq3.pdf.

- *ISIL success and legitimacy:* the victories initially accomplished by ISIL gave it an aura of power and invincibility. In defeating Syrian and Western-backed Iraqi forces and occupying large swathes of territory, ISIL achieved more than any movement had succeeded in doing since the mujahidin war in Afghanistan. Control of territory enabled it to create the appearance of a credible functioning State, 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 showing that ISIL was on the path to creating a new world order.[131]
- *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) led by the Mahdi (Muhammad's successor).[132] These prophesies became a fundamental part of the ideology of ISIL, and according to its propaganda, the captured town of Dabiq was to be the scene of this final apocalyptic battle between Muslims and Christians. Many FTFs have viewed this as their chance to take part in the "battle to end all battles",[133] 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:* the attraction can include material benefits. Some defectors from ISIL have mentioned promises of food, luxury goods and cars, and having their debts paid.[134] ISIL offered to pay higher salaries to recruits from Asia than they could earn at home, together with providing low-cost accommodation and generous health and education packages for their families.[135]

While religion and ideology are stated as the *de facto* reason for enlisting, many of those recruited in both Europe and Asia have also become involved due to the "thrill factor" and excitement provided by fighting in a foreign conflict.[136]

[131] "Indonesian and Malaysian Support for The Islamic State", USAID, (6 January 2016). At https://www.globalsecurity.org/military/library/report/2016/PBAAD863.pdf.

[132] Ibid.

[133] 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). At https://www.unodc.org/documents/southeastasiaandpacific/Publications/2016/Radicalisation_SEA_2016.pdf.

[134] "Victims, Perpetrators, Assets: The Narratives of Islamic State Defectors", International Centre for the Study of Radicalisation (2015). At http://icsr.info/2015/09/icsr-report-narratives-islamic-state-defectors/.

[135] "Indonesian and Malaysian Support for The Islamic State", USAID, (6 January 2016). At https://www.globalsecurity.org/military/library/report/2016/PBAAD863.pdf.

[136] 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). At https://www.unodc.org/documents/southeastasiaandpacific/Publications/2016/Radicalisation_SEA_2016.pdf.

A common motivation cited in interviews of FTFs from Europe is one of feelings of exclusion and lack of belonging to their local communities or society at large, engendering "a feeling that by joining the fight in Syria they have nothing to lose and everything to gain".[137] ISIL propaganda has offered an attractive message of belonging, purpose, brotherhood, adventure and respect.[138]

Stated another way, one source categorizes FTFs into four primary types:

- The Revenge Seeker (frustrated and angry and seeking an outlet to discharge that frustration and anger toward some person, group or entity whom he may see as being at fault)
- The Status Seeker (seeking recognition and esteem from others)
- The Identity Seeker (primarily driven by a need to belong and to be a part of something meaningful, seeking to define their identities or sense of self through their group affiliations)
- The Thrill Seeker (attracted to the group because of the prospects for excitement, adventure, and glory).[139]

The lack of any form of common profile poses a significant challenge for States when attempting to identify potential FTFs. Increasing numbers of women have also travelled, mainly accompanying their husbands or seeking to marry FTFs and live under the caliphate.

Case study: The recruiter—United Kingdom

Anjem Choudary, 49, was convicted in 2016 of inviting support for ISIL. 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 became radicalized and then travelled abroad as FTFs or went on to commit terrorist acts in the United Kingdom. Choudary, a former solicitor, was always careful to stay on the boundaries of the law without crossing the criminal threshold in what he said. However, he was judged to have crossed that line after posting speeches on YouTube legitimizing the caliphate established by ISIL, and stating that for true Muslims "obedience to the caliph [al-Baghdadi] is an obligation". Choudary was jailed for five years and six months.

Source: "Anjem Choudary jailed for five-and-a-half years for urging support of Isis", *The Guardian* (6 September 2016). https://www.theguardian.com/uk-news/2016/sep/06/anjem-choudary-jailed-for-five-years-and-six-months-for-urging-support-of-ISIS.

[137] 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). At http://www.rikcoolsaet.be/files/art_ip_wz/Egmont%20paper%2081.pdf.

[138] "Foreign Fighters: An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq", The Soufan Group (December 2015). At http://soufangroup.com/wp-content/uploads/2015/12/TSG_ForeignFightersUpdate3.pdf.

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

Case study: the Netherlands— the recruiters

In 2015, six men were convicted in the Netherlands for their roles in a "recruitment organization" which incited, recruited, facilitated and financed youngsters who wanted to travel to the Syrian Arab Republic to fight. They had sought to recruit young people to fight with ISIL and other terrorist groups. 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.

Source: "Dutch court convicts nine for terror offences", *BBC News* (10 December 2015). At http://www.bbc.co.uk/news/world-europe-35064597.

1.6 Women and children

Around one in five of those who have travelled to the Syrian Arab Republic from Europe are females, with even greater numbers of women making the journey from Asia, the Gulf States and North Africa.[140] 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 fighters idolized as heroes. Entire families have migrated in search of a better life in ISIL-held territory, including children and grandparents. For instance, in 2015, 12 members of a British Bangladeshi family ranging in age from 1 to 75 travelled from the United Kingdom to the Syrian Arab Republic via Bangladesh and Turkey.[141] There are many similar examples.

Al-Qaida in Iraq and other such groups have historically used females as combatants and in some cases, such as the ISIL affiliate in Nigeria, Boko Haram, as suicide bombers. However, ISIL does not consider the function of women 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 magazine Dabiq: "the wife of a mujahid and the mother of lion cubs".[142] The role of a good mother is seen as being to indoctrinate her children into the core values of ISIL, raising sons as fighters and potential martyrs, and raising daughters to follow their mother's example as the future wives of fighters.[143]

Women may however still receive firearms training and are permitted to carry arms in public. Similarly, women have been issued with suicide bomb vests, but only for the purpose of defending themselves if attacked by enemy forces.[144] As an alternative to fighting, 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 claimed to be responsible for torturing prisoners and meting out punishment, such as floggings, to those found guilty of breaching the strict code of conduct of ISIL.

[140] "The Foreign Fighters Phenomenon in the European Union", International Centre for Counter-Terrorism (April 2016). At https://www.icct.nl/wp-content/uploads/2016/03/ICCT-Report_Foreign-Fighters-Phenomenon-in-the-EU_1-April-2016_including-AnnexesLinks.pdf.

[141] "All 12 of us are here: Luton family announce arrival in Isis held Syria", *The Times* (4 July 2015). At https://www.thetimes.co.uk/article/all-12-of-us-are-here-luton-family-announce-arrival-in-isis-held-syria-f0hpx20gwrp.

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

[143] "Responses to returnees: Foreign terrorist fighters and their families", Radicalisation Awareness Network (July 2017). At https://ec.europa.eu/home-affairs/sites/homeaffairs/files/ran_br_a4_m10_en.pdf.

[144] "Life with ISIS: the Myth Unravelled", Netherlands General Intelligence and Security Service (January 2016). At https://english.nctv.nl/binaries/Life%20with%20ISIS%20-%20the%20Myth%20Unravelled_tcm32-90366.pdf.

Other functions that women undertake include teaching or nursing, but one of the most important roles is that of radicalizers and propagandists, utilizing their understanding of social media and their online contacts to successfully act as recruiters. Engaging in online conversations with family, friends, other females and potential fighters, they encourage them to migrate and facilitate their travel.[145] Whichever of these roles they partake in, women are making an active contribution to keeping the terrorist organization running.

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.[a] In 2015, Jones issued a series of threatening messages on Twitter, including calling on Muslim women to launch terrorist attacks in the United Kingdom during Ramadan.[b] In June 2016, Jones was killed in a United States drone strike. Her son JoJo, who had appeared in an ISIL video executing a prisoner by shooting him in the head, is believed to have died in the same strike.[c]

[a] "Designations of Foreign Terrorist Fighters", United States Department of State Bureau of Counterterrorism and Countering Violent Extremism (29 September 2015). At https://www.state.gov/j/ct/rls/other/des/266516.htm.

[b] "Sally Jones: Isis recruiter 'issues series of terror threats against UK cities' over Twitter", *The Independent* (25 May 2016). At http://www.independent.co.uk/news/world/middle-east/sally-jones-isis-recruiter-issues-series-of-terror-threats-to-uk-cities-over-twitter-a7049066.html.

[c] "Sally Jones' son collateral damage", *The Times* (13 October 2017). At https://www.thetimes.co.uk/article/sally-jones-son-jojo-collateral-damage-cia-drone-strike-white-widow-z2zt72l79.

For those female returnees considered a risk or who have committed terrorist offences, the criminal and administrative options remain largely the same as for their male counterparts. The approach to female returnees, however, varies between different jurisdictions. Some States have prosecuted the wives of FTFs for terrorism on the basis of their day-to-day support for their husbands. However, in the absence of additional evidence of terrorist conduct, other States do not consider such everyday actions to constitute an offence.

Case study: Indonesia

Ummi Kalsom Bahak, 26 years old, was apprehended in October 2014 at the immigration counter of Kuala Lumpur International Airport. She was on route via Brunei and Turkey to the Syrian Arab Republic, to become the bride of an ISIL fighter. Charged with the offence of attempting to give support to the militant group by marrying one of its members, she pleaded guilty and was sentenced to two years imprisonment.

Source: "Woman who intended to marry IS jihadist sees jail term upheld", *Malay Mail* (20 January 2016). At http://www.themalaymailonline.com/malaysia/article/woman-who-intended-to-marry-is-jihadist-sees-jail-term-upheld#KW51L4ZApb9BEqPA.99.

[145] "Foreign Terrorist Fighters: Trends, Dynamics and Policy", International Centre for Counter-Terrorism (December 2016). At https://icct.nl/wp-content/uploads/2016/12/ICCT-Mehra-FTF-Dec2016-1.pdf.

Case study: the Netherlands

Laura Hansen, 22 years old, left the Netherlands in September 2015 together with her husband and two young children to live under ISIL in the Syrian Arab Republic, where her husband joined the group as a fighter. They went via Turkey where they had booked a family holiday to disguise their travel.

Ten months later Hansen crossed the border into Iraq with her children, claiming that she had escaped after becoming disillusioned with life under ISIL. Helped by her father, she returned to the Netherlands, where she was arrested and charged with terrorism offences. At 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. In November 2017, she was convicted of "preparation or facilitation of a terrorist offence" and sentenced to a term of 24 months imprisonment, with 13 months of the sentence suspended for a period of 3 years.

Sources: Judgement of the Rotterdam District Court, Case No. 10 / 960288-16 (13 November 2017). At https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBROT:2017:8858. "Mother who took her children to Syria found guilty of aiding terrorism", *DutchNews.NL* (13 November 2017). At http://www.dutchnews.nl/news/archives/2017/11/mother-who-took-her-children-to-syria-found-guilty-of-aiding-terrorism/.

While the conventional view is that women are less likely than men to engage in terrorism, returning females still constitute a considerable risk. Researchers have found that women who join terrorist groups tend to be motivated by ideology, seeing themselves as "part of a social movement" and dedicated to a cause that they believe in.[146] Transnational marriages bring the potential for future international collaboration among extremists.

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

Case study: Indonesia

In August 2017, Dian Novi, a 27-year-old Indonesian, was sentenced at court in Jakarta to seven and a half years imprisonment, after pleading guilty to planning to carry out a suicide bomb attack during the changing of the guard ceremony at the Presidential Palace. By her own account, she had become radicalized through viewing social media posts on her smartphone, while employed as a domestic worker in Taiwan. Making contact online with a woman in the Syrian Arab Republic, she was then put in touch with Indonesian ISIL sympathizers. These included Nur Solihin, who had been instructed to find a "bride" for a suicide bombing. After agreeing to become a suicide bomber,

[146] "Intrepid Sisters Reveal How ISIS Depends on Role of Women", *Syria Deeply* (26 May 2017). At https://www.newsdeeply.com/syria/articles/2017/05/26/intrepid-sisters-reveal-how-isis-depends-on-role-of-women.

Case study: Indonesia *(cont'd)*

Novi and Solihin "married" online using the Telegram messaging app (they had not met in person at that time). Novi was arrested when Indonesia's anti-terrorism unit, Detachment 88, raided the room she had rented at a boarding house. There they found a pressure cooker type IED containing triacetine triperoxide explosive and nails.[a]

According to prosecutors, the instructions had been issued by Bahrun Naim, a prominent Indonesian fighting with ISIL in the Syrian Arab Republic.[b]

[a] "ISIS Unveiled: The Story Behind Indonesia's First Female Suicide Bomber", *Time* (3 March 2017). At http://time.com/4689714/indonesia-isis-terrorism-jihad-extremism-dian-yulia-novi-fpi/. "Indonesian woman jailed for suicide bomb plot at Jakarta palace", *CNBC* (28 August 2017). At https://www.cnbc.com/2017/08/28/indonesia-first-female-suicide-bomber-sentenced-to-jail.html.

[b] "IS-aligned militant jailed over plot to bomb Indonesian presidential palace", *The Star* (21 September 2017). At https://www.thestar.com.my/news/regional/2017/09/21/is-aligned-militant-jailed-over-plot-to-bomb-indonesian-presidential-palace/#3Vh86vD6014UPJRw.99.

While large numbers of male FTFs were killed in fighting in the Syrian Arab Republic and Iraq during 2017, many of their wives and children survived. In just one battle, the offensive to liberate Mosul from ISIL, more than 1,300 women and children surrendered and were detained by Iraqi forces. These women, and others from across the region, will seek to be repatriated with their children. Some, such as a 16-year-old German girl captured in Mosul, instead face trial for membership of ISIL.[147]

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 has reportedly been illegal under the rule of ISIL, while women were encouraged to bear multiple children.[148] Those born in conflict zones risk statelessness should both parents be killed or imprisoned, while mothers may try to claim the nationality of the father for their children.[149]

The recruitment and use of children has been a core part of ISIL plans for future survival. In ISIL-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 ideology with gender-specific roles instilled from an early age.

Boys as young as the age of nine have been trained to use weapons and taught to kill, dubbed "cubs of the caliphate".[150] Between 2014 and 2016, ISIL is believed to have recruited and trained more than 2,000 boys between the ages of 9 and 15.[151] Classes include both militarization and indoctrination, with weapons and explosives training coupled with religious instruction.[152] Once trained, children can

[147] "German teenage 'Isis bride' could face death penalty in Iraq", *The Independent* (18 September 2017). At http://www.independent.co.uk/news/world/german-isis-bride-teenage-iraq-death-penalty-hanging-linda-wenzel-a7952876.html.

[148] "Responses to returnees: Foreign terrorist fighters and their families", Radicalisation Awareness Network (July 2017). At https://ec.europa.eu/home-affairs/sites/homeaffairs/files/ran_br_a4_m10_en.pdf.

[149] For example, "Islam Mitat: We escaped Raqqa, but I'm still haunted — and hunted — by Isis", *The Sunday Times* (22 October 2017). At https://www.thetimes.co.uk/article/islam-mitat-we-escaped-raqqa-but-im-still-haunted-and-hunted-by-isis-bdr3ptr5n. "What should happen to the foreign women and children who joined Isis?", *New Statesman* (28 August 2017). At https://www.newstatesman.com/world/middle-east/2017/08/what-should-happen-foreign-women-and-children-who-joined-isis.

[150] Richard Barrett, "Beyond the Caliphate", The Soufan Center (October 2017). At http://thesoufancenter.org/research/beyond-caliphate/.

[151] Ibid.

[152] "ISIS Trains Child Soldiers at Camps for 'Cubs of the Islamic State'", *NBC News* (7 November 2014). At https://www.nbcnews.com/storyline/isis-uncovered/isis-trains-child-soldiers-camps-cubs-islamic-state-n241821.

perform support roles such as treating the wounded, or act as spies, snipers and frontline fighters.[153] A study of children and youths eulogized in ISIL propaganda for dying as martyrs found that a third of those killed while conducting attacks in 2015 came from countries outside of the Syrian Arab Republic and Iraq.[154] In 2016, a 12-year-old Indonesian boy who travelled to the Syrian Arab Republic to fight with ISIL was reported as killed in an airstrike.[155]

ISIL is unique among terrorist groups in its brazen use of child soldiers, who have increasingly been given a star role in propaganda videos. Young boys, including the sons of FTFs, have been filmed executing prisoners by detonating explosives, shooting or beheading them. The youngest 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 the explosives in a car killing three prisoners.[156]

Case study: Indonesia

The ISIL video "The Generation of Epic Battles", released in May 2016, shows young children purportedly from Indonesia and Malaysia undergoing firearms training in the Syrian Arab Republic. The commentary in Arabic, with subtitles in Bahasa Indonesia, is addressed as a threat to the governments of Indonesia and Malaysia. The Malaysian Zainuri Kamaruddin, leader of the Malay Archipelago Unit of ISIL, Katibah Nusantara, is featured in the video. Individual children are shown pledging to wage jihad against those who have "changed the laws of God", with Kamaruddin saying that the "cubs of the caliphate" are preparing to "become the fighters of tomorrow". Further stating that they renounce their citizenship, he then leads the child fighters in throwing their passports into a bonfire.[a]

Kamaruddin is reported to have been killed in January 2017 in a Syrian government airstrike.[b]

[a] "Islamic States child fighters video is worrying, say experts", *Free Malaysia Today* (24 May 2016). At http://www.freemalaysiatoday.com/category/nation/2016/05/24/islamic-statess-child-fighters-video-is-worrying-say-experts/.

[b] "Malaysian IS leader killed in Syria recruited members through Facebook: Police", *Channel News Asia* (15 January 2017). At https://www.channelnewsasia.com/news/asiapacific/malaysian-is-leader-killed-in-syria-recruited-members-through-fa-7559516.

Video at:http://jihadology.net/2016/05/15/new-video-message-from-the-islamic-state-the-generation-of-epic-battles-wilayat-al-barakah/.

When young children return to the countries of their birth, or for those born abroad, the countries of their parents, the welfare of the child and their psychological health must be the first priority of a multi-agency response. They are likely to be severely traumatized, deeply impressionable, and

[153] Ibid.

[154] 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 12 (February 2016). At https://ctc.usma.edu/posts/depictions-of-children-and-youth-in-the-islamic-states-martyrdom-propaganda-2015-2016.

[155] "Indonesian school a launchpad for child fighters in Syria's Islamic State", *Reuters* (7 September 2017). At https://www.reuters.com/article/us-indonesia-militants-school-insight/indonesian-school-a-launchpad-for-child-fighters-in-syrias-islamic-state-idUSKCN1BI0A7.

[156] "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). At http://www.dailymail.co.uk/news/article-3441125/Shocking-new-ISIS-video-shows-four-year-old-British-boy-dubbed-Jihadi-Junior-blowing-four-alleged-spies.html.

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

Indoctrinated by ISIL teachers, the older children are likely to have undergone military instruction and taught to kill as part of their training to become the next generation of terrorists, and therefore any remnants of radicalization need to be countered to prevent problems in years to come.[157] Where they are above the age of criminal responsibility they may be subject to prosecution, but any charging decisions should balance the young person's level of involvement against the coercion they might have experienced.

In the first three batches of deportees from Turkey to Indonesia in 2017, from a total of 137 individuals, 79 per cent were women or children under the age of 15.[158] Not only have children been taken to the conflict zones, but large numbers have been born there to FTFs. A minority of females will undoubtedly have been coerced or tricked into travelling to ISIL. Others, very naïve and expecting an exciting romantic adventure, will instead have experienced enforced domestication and possibly been the victims of 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, taking 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".

Source: United Nations Security Council Counter-Terrorism Committee, "Madrid Guiding Principles" (23 December 2015). At https://www.un.org/sc/ctc/wp-content/uploads/2016/10/Madrid-Guiding-Principles_EN.pdf.

1.7 Criminal justice and administrative options

Pre-travel

When information concerning a person's intention to travel as an FTF reaches law enforcement, any action taken will depend on the urgency of the situation. If travel is imminent, arrest or other forms of intervention will need to be considered. Where a situation is not time imperative, intervention can be delayed and further evidence covertly gathered, possibly including details of associates and facilitators.

A search of the suspect's home address, together with forensic examination of his or her computer and mobile phones, could provide sufficient evidence to prosecute for preparatory terrorism offences. The same evidence could be uncovered through online investigation of social media pages, or enquiries

[157] "German Intelligence Warns from New Generation of ISIS Recruits", *Asharq Al-Awsat Newspaper* (21 October 2017). At https://aawsat.com/english/home/article/1059306/german-intelligence-warns-new-generation-isis-recruits.

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

on financial transactions. Evidence of involvement in unrelated criminal activity might also provide a means of preventing a suspect's travel (see below, "Prosecution of FTFs").

Frontline officers tasked with controlling the movement of persons across borders need to be supplied with updated information, allowing them to conduct effective evidence-based screenings of travellers in order to identify potential FTFs.[159] Targeted questioning of suspects and searches of baggage, may additionally reveal immigration offences or the possession of prohibited articles (such as large amounts of cash), thereby preventing suspects from leaving the country or at the very least delaying travel while other action is considered.

Many States have legislated to introduce administrative measures in order to restrict the movements of suspected FTFs and prevent their travel abroad. These measures include:

- Preventive detention
- Control/restriction orders–restricting the movement of the suspect (discussed in greater detail below)
- Travel bans
- Denying the issue of, or revoking, passports and other travel documents—including powers to prevent travel by seizing passports at the border

For example, In the United Kingdom, a police officer at the border can seize the passport of someone he suspects is travelling for the purposes of terrorism. With court authority, this can then be retained for up to 30 days, while the Home Secretary decides whether there is sufficient information to justify revoking the passport.

Source: United Kingdom Counter-Terrorism and Security Act 2015. At http://www.legislation.gov.uk/ukpga/2015/6/notes/division/5.

Administrative measures are often designed to be invoked on the authorization of government officials, usually at the ministerial level (the executive), and can be applied on the basis of secret intelligence which is not disclosable to the suspect. Judicial or other effective oversight mechanisms are therefore required, to both ensure human rights are adequately protected, and to ensure that any imposition of such measures is justified by reliable and credible information.[160]

Police, social services agencies or family courts may be able to intervene to safeguard children when an entire family may potentially travel, thus preventing parents from putting their children at risk in conflict zones. Family law tools can include court orders to remove children from their parents, supervision of the child's care, or restrictions on travel and the removal of passports. The breakup of the family unit is a serious course of action, and should generally be considered as a temporary measure while any elements of risk are mitigated.

[159] United Nations Security Council Counter-Terrorism Committee Executive Directorate, "Implementation of Security Council resolution 2178 (2014) by States affected by foreign terrorist fighters: A compilation of three reports (S/2015/338; S/2015/683; S/2015/975)". At https://www.un.org/sc/ctc/wp-content/uploads/2016/09/FTF-Report-1-3_English.pdf.

[160] United Nations Security Council Counter-Terrorism Committee, S/2015/123 (23 February 2015). At https://www.un.org/sc/ctc/wp-content/uploads/2015/09/S_2015_123_EN.pdf.

After travel

If law enforcement agencies only become aware of a suspected FTF's travel after they have left the country, then a search of the suspect's home address and the interviewing of friends and family may assist in confirming his intentions. Evidence can also be obtained to start building a prosecution file for if and when the suspect returns, together with details of social media accounts and telephone numbers that can be monitored. Gaining cooperation from the family can allow an assessment of the risk posed by other family members who may similarly seek to travel or be radicalized.

Once travel is discovered, possible transit countries or countries of destination will need to be urgently alerted, through INTERPOL or other established liaison mechanisms. More than 60 countries, and the United Nations, now contribute profiles of FTFs to INTERPOL.[161] Checks of passenger manifests, CCTV at ports and airports, financial transactions and cell phone tracking, and public appeals can all assist in intercepting travellers.

United Nations resolution 2178 calls upon Member States to "prevent the entry into or transit through their territories" of suspected FTFs.[162] International cooperation is a key requirement in monitoring and detecting FTFs, especially liaison with transit countries. Once alerted, foreign law enforcement agencies may be able to either arrest suspects for terrorism offences in their own jurisdiction, or take action for immigration offences in order to prevent onward travel.

Since the start of the Syrian civil war in 2011, 4,957 individuals from 99 countries seeking to cross to the conflict zones in the Syrian Arab Republic/Iraq have been detained and deported by the Turkish authorities. Following the adoption of United Nations Security Council resolution 2178 (2014), the Turkish National Police established 66 Risk Analysis Units at airports and border crossings in an effort to prevent the movement of FTFs.

As a result of intelligence from foreign partners, the names of 53,781 individuals from 146 countries suspected of involvement in terrorism have been included in the Turkish "no entry" list. Since 2014, 4,550 of those on the list have been refused entry and repatriated.

Since 2011, a total of 9,350 suspected FTFs have been taken into custody in Turkey, including 3,840 foreign nationals.

Source: "Turkey's Fight Against DEASH", Ministry of the Interior (July 2017). At http://www.mia.gov.tr/kurumlar/mia.gov.r/Genel/deas%CC%A7%207%20temmuz.pdf.

Should it be determined that the suspect has reached his or her destination and is already involved in terrorist activity, then in addition to starting a criminal investigation, action can be considered to prevent or control their return home. Some States are armed with administrative measures empowering them to strip an individual of citizenship. International conventions, however, stipulate that a person should not be made stateless, and this power can therefore only be used against those who are legally

[161] Official INTERPOL figures as at 30 January 2018.

[162] United Nations Security Council resolution 2178 (2014).

nationals of more than one country. Applied against FTFs who are abroad, the stripping of citizenship removes the right to return to their country of nationality.

Other States have legislated to be able to prohibit their citizens, who are abroad and suspected of terrorist activity, from re-entering the country for a set number of years. These temporary exclusion orders can allow conditions to be imposed to control an individual's eventual return home.[163] Measures such as these help protect the home State, but may prove problematic for countries where FTFs remain after their ability to travel is curtailed.

Returning foreign terrorist fighters

Unsurprisingly, FTFs are perceived to be a major threat to their home countries. As discussed above, the fear is that once they return they will utilize their terrorist training in order to plan and carry out attacks, set up new terrorist cells, or otherwise facilitate future terrorist acts. Large numbers of FTFs have already returned to some countries. Many have been arrested, and others will have returned without triggering alerts within law enforcement authorities, who thus may be unaware of their identities.

United Nations resolution 2178 calls upon Member States to bring to justice their nationals who travel (or attempt to travel) to other States for the purpose of engaging in the planning or perpetration of terrorist acts. Therefore, immediate coordinated action is required upon the return of an FTF, to secure any retrievable evidence, and if possible, file charges for prosecution.

Where prosecution and custody of the individual are not possible or not considered an appropriate strategy for other reasons, a full risk assessment needs to be undertaken on a case-by-case approach as to the level of threat posed by the returning FTF. All available options need to be explored in an attempt to ensure returning FTFs do not cause a danger to the community.

Alternatives to prosecution of returning FTFs include:

- *Monitoring—surveillance:* employing conventional and technical covert surveillance of the suspect, both to prevent any risk to the public and to gather evidence to prosecute.
- *Monitoring—control/restriction orders:* a temporary administrative measure limiting the freedom of movement of individuals in an attempt to prevent their involvement in terrorism, normally only applied in the most serious cases due to restrictions on human rights. Possible conditions may include a curfew and electronic monitoring, together with restrictions on where a suspect may live or work, who they may associate with, their access to the Internet or phones, financial transactions and travel.[164]
- *De-brief:* in addition to interviews to determine an individual's criminal involvement, attempts should be made to debrief all of those returning from conflict zones, irrespective of their level of participation. Valuable intelligence can be obtained to give a picture of the situation on the ground, together with more specific intelligence on individuals and planning. Those who have played a minor role may be willing to act as witnesses in court against former associates, or be capable of recruitment as informants to go out into the community and obtain intelligence.
- *Rehabilitation:* disengagement and reintegration programmes can be used where prosecution is neither possible nor appropriate. Also, they can be employed in addition to criminal

[163] For example, the United Kingdom where a Temporary Exclusion Order can be imposed on a person for a period of up to two years. Permits to return are issued when authority to return to the United Kingdom is granted, which can be subject to a number of conditions. Counter-Terrorism and Security Act 2014.

[164] Control orders are available in countries such as Australia and the United Kingdom (where now referred to as TPIMS), and Malaysia (Restriction Orders).

proceedings, or in tandem with the imposition of administrative measures. For instance, travel bans can allow for the concurrent application of deradicalization strategies.[165]

By way of example, Malaysia and Singapore have developed ongoing government programmes to rehabilitate and reintegrate terrorist inmates into society through preventive/administrative detention, working in cooperation with various civil society organizations.[166] Indonesia has begun a programme whereby all those returning from the Syrian Arab Republic are required to undergo a one-month deradicalization programme run by the Social Affairs Ministry.[167]

In certain circumstances the prosecution of returning fighters may not be considered appropriate, for example because of their age or participation in a group which ultimately did not engage in terrorist acts. In the early stages of the Syrian conflict, there were an estimated 1,000 armed opposition groups with a variety of political and ideological aims.[168] Since then there have been alliances and counter-alliances among the various groups, many fighting each other in a complicated political landscape. Those returning may have fought with the Syrian Democratic Forces or Free Syrian Army. More than 400 FTFs from Europe, America and Australia, both male and female, have joined the Kurdish People's Protection Units, with the stated intention of helping to defeat ISIL. [169] These units are, however, affiliated with the Kurdistan Workers Party (PKK), which some other countries list as a terrorist organization. Whatever their original intentions, their actions may amount to criminal offences.

1.8 Prosecution of foreign terrorist fighters

Possible offences

Certain States have made it a crime for their citizens to fight in an overseas conflict.[170] Some have come up with other innovative solutions in attempting to combat the problem of FTFs. Australia, for example, can prosecute persons returning from conflict zones for having entered a "declared area", which the government has deemed off-limits due to terrorist activity.[171]

The specific circumstances of each case need to be considered against available laws and legislative tools, together with a careful assessment of the impact of prosecution decisions, weighing factors such as sufficiency of evidence and public interest. Unique and complex scenarios require an informed understanding of the situation, with both investigators and prosecutors required to consider all the options at their disposal.

[165] "Administrative Measures against Foreign Fighters: In Search of Limits and Safeguards", International Centre for Counter-Terrorism (December 2016). At https://icct.nl/wp-content/uploads/2016/12/ICCT-Boutin-Administrative-Measures-December2016-1.pdf.

[166] United Nations Security Council Counter-Terrorism Committee Executive Directorate, "Implementation of Security Council resolution 2178 (2014) by States affected by foreign terrorist fighters: A compilation of three reports (S/2015/338; S/2015/683; S/2015/975)". At https://www.un.org/sc/ctc/wp-content/uploads/2016/09/FTF-Report-1-3_English.pdf.

[167] "National Counterterrorism Agency (BNPT) is requiring all Indonesia people returning from Syria to join a deradicalization program", *The Jakarta Post* (4 July 2017). At http://www.thejakartapost.com/news/2017/07/04/all-returnees-from-syria-required-to-join-deradicalization-program.html. See also "152 sent home after undergoing deradicalization program", *The Jakarta Post* (28 June 2017). At http://www.thejakartapost.com/news/2017/06/28/152-sent-home-after-undergoing-deradicalization-program.html.

[168] "Guide to the Syrian rebels", *BBC News* (13 December 2013). At http://www.bbc.co.uk/news/world-middle-east-24403003.

[169] "More than 400 fighters from Australia, America and Europe join YPG", Syrian Observatory for Human Rights (11 June 2015). At http://www.syriahr.com/en/?p=19983.

[170] It is a crime for "Maldivians to join or attempt to join or fight in any overseas conflict". Prevention of Terrorism Act, No:32/2015. At http://www.presidencymaldives.gov.mv/Documents/4560_ee6e0576-8_.pdf.

[171] Criminal Code Act 1995, Section 119.2. See https://www.nationalsecurity.gov.au/whataustraliaisdoing/pages/declareda reaoffence.aspx; https://www.legislation.gov.au/Details/F2015L00245/Explanatory%20Statement/Text.

One of the most useful offences to come out of the previously discussed United Nations resolutions is that of the preparation of terrorist acts, which removes the need to prove either a conspiracy or an attempt to commit a substantive offence. A series of acts, such as an FTF making travel arrangements, buying equipment or undertaking physical training, can be used to prove the offence when the intent to engage in terrorism can also be shown. In the United Kingdom, for instance, since 11 September, this offence has been the most frequently charged piece of terrorism legislation.[172] Preparatory offences are similarly useful when extra-jurisdictional powers do not exist to prosecute substantive offences committed abroad.

Where there is insufficient evidence of terrorist intent, there may be other offences within domestic criminal law that can be considered against returning or aspiring FTFs. For example, there may be evidence of immigration offences or fraud in relation to travel documents. Where evidence of crimes such as murder or conspiracy to murder exist, then terrorism legislation may provide additional powers of investigation or enhanced sentencing provisions. Where terrorism legislation has not been updated, the creative application of ordinary criminal legislation may be the only alternative. Prosecuting for such offences can serve to place FTFs in custody or disrupt their networks of associates. However, relying on ordinary offences runs the risk that the courts will be unable to address the full severity of the case; punishments may be light.

When framing charges, the whole range of available legislation needs to be considered. For example, FTFs who upload material or appear in videos in support of terrorist groups (disseminated either at home or when they are abroad), might not simply be guilty of glorifying terrorism but also of more serious offences including incitement to murder. The proven swearing of an oath of allegiance and other declarations of assistance to a terrorist group, can lead to charges of membership or support of a proscribed organization. At the same time, returning FTFs who have been involved in fighting or executions can additionally be considered for war crimes, such as the killing of civilians.

In deciding upon possible charges against a suspect, a balance needs to be struck between prosecution and prevention, as one cannot ultimately be successful without the other. Tackling the phenomenon of FTFs requires prosecutors to adopt a strategic approach that ensures respect for human rights and the rule of law. Prosecutions, and how they are conducted, should never play into the propaganda of terrorists.[173]

Converting intelligence into admissible evidence

Cases involving FTFs pose unique challenges to prosecutors and investigators, particularly in respect to the collection of admissible evidence. Material that can often be gathered to prove domestic terrorism offences such as eye witness testimony and recovered weapons, may be unavailable in cases involving foreign conflict zones. In particular, a major hurdle is proving intent to travel.

Early liaison and a constructive working relationship between investigators and prosecutors can help to resolve some of these issues, determining the evidence that will be required to support a prosecution, as well as indicating any potential problems regarding the admissibility of evidence. This is particularly so in jurisdictions applying the Common Law legal system, with investigations led by the police and where prosecutors might not ordinarily be involved until charges are laid or a case proceeds to court.

[172] "The Terrorism Acts in 2015: Report of The Independent Reviewer on the Operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006", Terrorism Legislation Reviewer (December 2016). At https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/12/TERRORISM-ACTS-REPORT-1-Dec-2016-1.pdf.

[173] United Nations Security Council Counter-Terrorism Committee, S/2015/123 (23 February 2015). At https://www.un.org/sc/ctc/wp-content/uploads/2015/09/S_2015_123_EN.pdf.

As with terrorism investigations in general, collection of evidence can be resource-intensive and very time consuming. In attempting to protect public safety, enquiries are often time imperative and urgency can be required to preserve available evidence. Coordinated investigations by dedicated teams of investigators can help to meet these challenges. As the nature of the threat constantly evolves, so does the need to adapt to meet it. This section now briefly looks at some of the main evidential challenges faced in FTF investigations.[174]

Case study: Maldives

In February 2016, intelligence was received that five males were leaving Maldives with the intention of travelling to fight in the Syrian Arab Republic and partaking in "jihad". An investigation began into the activities of those involved, who by that time had already left the country telling their families that they were going on holiday to Sri Lanka. International partner agencies were contacted, leading to the suspects being intercepted and detained in Turkey and three being deported back to Maldives.

However, upon return they had no physical evidence of their planned activities. Also, no statements or other official documentation was received concerning events in Turkey; none had been received even at the time the matter went to court. In the absence of this material, the trial judge noted that the officer responsible for the intelligence report could prove neither the route taken by the suspects to Turkey, nor their detention there. The trial ended with the court stating that there was insufficient evidence to support the charges of travelling abroad with the intent of joining a terrorist group.

Source: "Alleged Maldivian jihadis cleared of intent to join terror group", *Maldives Independent* (23 October 2017). At http://maldivesindependent.com/crime-2/alleged-maldivian-jihadis-cleared-of-intent-to-join-terror-group-133542.

In FTF cases, much of the information about persons fighting overseas comes from the work of domestic or foreign intelligence services. Generally classified as "secret", conditions imposed on the sharing of material normally mean that it cannot be adduced as evidence in open court. This is often due to genuine fears of exposing methodology or the sources of information, exposure of which could be counterproductive to future intelligence gathering and even endanger lives. The protection of national security and other public interests can conflict with the administration of justice in a specific prosecution.

That is not to say that investigators cannot show the same facts in other ways. With the consent of the respective intelligence service, the information could be used in a redacted form in applications for the use of special investigative techniques, such as interception of communications, covert searches of the subject's premises, or surveillance that could all generate admissible evidence. Intelligence reports, though often correct, must in any case be treated with caution. Conclusions can be founded on assumptions; the content may be uncorroborated and imprecise, based on hearsay, or gathered in a way that would not permit its use as evidence.

[174] Based on those challenges highlighted by participating states in South and South-East Asia, both at workshops and in response to post-workshp questionnaires.

Historically, intelligence services have focused their efforts on identifying and combating threats to national security, briefing their own governments and the military, with intelligence purely used to inform decision-making. The lack of a good working relationship with police in some States has in the past led to missed opportunities on both sides and serious security failings. Although competing aims need to be recognized and accommodated, law enforcement and intelligence services can provide mutual assistance and support in terrorism cases, complementing one another in their separate operational objectives.[175]

Ideally, police and intelligence services will regularly meet together to discuss and decide on the direction of investigations that might lead to a prosecution. Early police involvement can ensure that evidential openings are not missed. In many instances, material gathered by means of special investigative techniques does not need to be treated as secret and can be used as evidence in court. For example, the management of a covert listening device could be undertaken by police, ensuring that the product is gathered to an evidential standard and put before the court by police witnesses. Or, an undercover police officer could be introduced into a covert operation, gathering evidence and protecting the involvement of the intelligence services. Inter-agency cooperation should therefore begin before the point when executive action (arrest or other intervention) is needed. Furthermore, there may not be a barrier to agents of intelligence services actually becoming part of the evidence chain themselves, and with suitable protection, providing witness testimony in court.

In the United Kingdom, judges have allowed MI5 (Security Service) staff to give evidence in criminal trials anonymously, including appearing behind screens. These arrangements are similar to those that are made for undercover and specialist police officers and members of the Special Forces when giving evidence. The evidence given by MI5 witnesses remains subject to cross-examination by the defence in the normal way.

Source: "Evidence and Disclosure" Security Service MI5. At https://www.mi5.gov.uk/evidence-and-disclosure.

International cooperation

Easier world travel and advances in methods of communication have facilitated the growth of the phenomenon of FTFs. Terrorist groups have become increasingly international both in terms of recruitment and objectives, meaning cooperation between countries is essential to prevent and prosecute terrorist activity. The prosecution of FTFs relies not only on evidence collected in countries of origin, but also from countries of transit and countries of destination, as well as from other jurisdictions such as those holding data in relation to Internet usage.

Mutual legal assistance requests are the recognized way of obtaining evidence from other jurisdictions, but this can be a slow and cumbersome process. Another difficulty can be the dual criminality requirement, preventing requests being granted when the conduct alleged does not constitute an offence in the other jurisdiction (or was not an offence at the time in question).

Many States face significant backlogs of requests for mutual legal assistance, making some form of direct contact between investigators or prosecutors advisable if evidence in serious cases is to be

[175] "Evidence and Disclosure" Security Service MI5. At https://www.mi5.gov.uk/evidence-and-disclosure.

obtained within time limits. Liaison can often take place in advance of an official letter of request, assisting in the preservation of evidence. Where criminal contacts are discovered in the other jurisdiction, a parallel terrorism investigation could be opened.

Liaison can further assist in enabling prosecutors to determine what material might be available and how the request should be worded. In urgent cases where searches of premises or other executive action is required, a faxed copy of the letter of request can serve to start action. Many larger States now have law enforcement officers stationed abroad at their embassies, part of their role being to assist their home agencies in obtaining evidence, conversely, they can be approached for advice on gaining assistance from their own countries.

It is important for States to coordinate their efforts on FTFs. Some have already developed mechanisms for integrated international investigations that can be used in such cases. For example, where one of the countries involved is a European Union member, the European Union body Eurojust can facilitate the formation of what are termed Joint Investigation Teams. These enable the direct exchange of information and evidence, without the need to use traditional channels of mutual legal assistance.[176]

Case study: joint operation Bangladesh—Spain

A joint operation between Bangladeshi and Spanish police anti-terrorism investigators led to successful arrests in both countries. The investigation focused on a Bangladeshi male living in Spain, the owner of a telecommunications software company originally set up by his brother, who had been killed in an airstrike in 2015 while providing technical assistance to ISIL in the Syrian Arab Republic. The company, with branches in nine countries, is alleged to have been a front for terrorist activity, including supplying military-grade equipment to ISIL and sending funds to Bangladesh for the purchase of weapons by terrorist groups.

To progress the enquiry, Spanish investigators were invited to a meeting in Bangladesh, at which intelligence was shared and an official channel established for exchanging information. In September 2017, simultaneous raids were conducted in both countries, resulting in the arrest and charging of the company's CEO in Spain and of 11 employees in Bangladesh.

Sources: "Cardiff man held in Spain over ISIL(Da'esh) link", *The Times* (24 September 2017). At https://www.thetimes.co.uk/article/cardiff-man-held-in-spain-over-isis-link-hchnq7dzt.
"Terror funding thru' IT firm", *The Daily Star* (24 September 2017). At http://www.thedailystar.net/frontpage/terror-funding-thru-it-firm-1466725.

[176] EUROJUST, "Joint Investigation Teams (JITs) – Practitioner's Area". At http://www.eurojust.europa.eu/Practitioners/JITs/Pages/JITs-sitemap.aspx.

Case study: joint operation Bangladesh—Malaysia

In December 2015, Redwanul Azad Rana, an organizer of the Al-Qaida linked Bangladeshi terrorist group Ansarullah Bangla Team (ABT), was convicted in absentia and sentenced to death for his role in the 2013 murder of secular blogger Ahmed Raijeb Haider. Rana had fled Bangladesh in 2014 while the murder investigation was under way, entering Malaysia on a forged passport. There he made contact with other extremists and reportedly swore an oath of allegiance to ISIL before trying to travel to the Syrian Arab Republic. He was unsuccessful in entering the Syrian Arab Republic, and then attempted to get to the Philippines to undertake training with the Abu Sayyaf Group. Before he could leave, in February 2017, Rana was detained by Malaysian police who had been working in liaison with their counterparts in Bangladesh. Three days later he was deported back to Bangladesh, where he was put under surveillance by the Counter Terrorism Unit and subsequently arrested.

Sources: "Blogger Rajib Murder: Convicted planner, deported from Malaysia, arrested", *The Daily Star* (21 February 2017). At http://www.thedailystar.net/frontpage/blogger-rajib-murder-convicted-planner-deported-malaysia-arrested-1364539.

"How Southeast Asian and Bangladeshi Extremism Intersect", IPAC Report No. 37 (8 May 2017). At http://file.understandingconflict.org/file/2017/05/IPAC_Report_37.pdf.

Evidence from conflict zones

Collecting evidence in a foreign war zone is virtually impossible. Countries such as the Syrian Arab Republic and Iraq remain in a state of armed conflict, making travel by foreign investigators extremely hazardous. Even where evidence is obtained on the ground by armed forces or local police, there will be challenges to producing witnesses in court and ensuring the reliability of testimonies. Furthermore, if suspicion exists that evidence was obtained through torture or duress, it may be ruled inadmissible by a judge.

Evidence, however, may exist closer to home. Investigators can talk to witnesses in their own country, such as family and friends of suspected FTFs. Experience has shown that many FTFs keep in touch with their friends and relatives after travel. Building an early working relationship with families, who are invariably anxious for information and advice, often enables additional evidence to be obtained. They may provide witness statements, identify communications from an FTF on their mobile phones and computers, or reveal social media identifiers and telephone numbers that can subsequently be researched and monitored.

Contact officers

After terrorism arrests in the United Kingdom, contact officers are appointed to liaise with the families of suspects. In FTF cases this contact can start once police are notified that someone has travelled to a conflict zone. Contact is maintained until the conclusion of the investigation. The role of these specially trained police officers includes:

Contact officers *(cont'd)*

- Gathering evidence and information in a sensitive manner, to assist with the investigation
- Providing a communication channel to the officer-in-charge and the investigation team
- Advising family members on the criminal justice system, and where possible providing information and practical support about the investigation and associated procedures

Where it is not possible to obtain evidence from transit countries or end destinations, other means of proving travel can be considered. This can include: evidence from airlines, immigration records, CCTV from airports, financial transactions, telephone cell siting, Internet IP addresses, location data in photographic images and social media posts. Other evidence such as traces of explosives on clothing or evidence of recent wounds may also assist to prove the presence of a returning FTF.

Collection of evidence from social media and electronic devices

Evidence collected from social media pages can provide very powerful evidence, in some instances effectively tracking the activity of individuals in conflict zones. Many fighters actively engage online in recruitment and the glorification of terrorist acts, posting videos and messages encouraging others to follow them and engage in violence. Not initially intending to return, they may be quite open in communications regarding their role. Whenever possible, efforts should be made to evidentially download online content in real time before it is potentially erased, thereby collecting evidence for use in a prosecution should the suspect return home.

When this is not possible, applications need to be submitted to preserve content in advance of either a court order, or letter of request to the relevant overseas jurisdiction. In considering such action, the requirement for evidence will sometimes need to be balanced against any intelligence dividend that might be compromised by a social media or web hosting company taking an account down once alerted to its terrorist use. Requests may also be fruitless with some providers holding little or no data that will assist an enquiry. For instance, the only message content recoverable from WhatsApp are the undelivered messages (retained for 30 days).[177] Others may retain potentially useful evidence. For example, Facebook not only holds postings and pictures, but also private messages that, unless preserved on behalf of law enforcement, are only held for a maximum of 90 days once deleted by the account holder.

Retrieving and analysing evidence from recovered electronic communication devices is a highly skilled task. The vast number of different apps, ever increasing size of hard drives, encryption and other difficulties, also mean that once retrieved, analysis and assessment of the data can be extremely time consuming. Efforts need to be triaged, initially (at least) focused on available operational information. Ideally a more in-depth examination will then follow, as data can easily be hidden. Time can be saved, however, by building a library of propaganda and instructional media files found during the course of investigations. These can be indexed and their hash values then checked against future seizures, removing the need to repeatedly view and assess the same files.

[177] WhatsApp, "Information for Law Enforcement Authorities". At https://faq.whatsapp.com/en/general/26000050.

Al-Qaida operative Dhiren Barot, convicted of conspiracy to cause explosions, carried out hostile reconnaissance of buildings in the financial district of New York. The film footage that he shot was then hidden by being spliced into an outwardly innocent video of the movie Die Hard with a Vengeance. This footage was only discovered as a result of the content of every recovered video being checked.

Source: "Prosecution case against Al-Qaida Briton", *BBC News* (6 November 2006). At http://news.bbc.co.uk/1/hi/uk/6122270.stm.

Bangladeshi national Rajib Karim conspired online (from the United Kingdom) with members of both Jamaat-ul-Mujahdeen in Bangladesh and of Al-Qaida in the Arabian Peninsula in Yemen. Convicted of planning to put a bomb on a transatlantic passenger flight, he communicated by means of heavily encoded word documents that were uploaded to file sharing websites and deleted after being read. Karim, however, kept encrypted copies in a hidden partition on a portable hard drive. These were only discovered because of the examiner's suspicions about the lack of free space shown on the drive.

Source: "Terror plot BA man Rajib Karim gets 30 years" *BBC News* (18 March 2011). At http://www.bbc.co.uk/news/uk-12788224.

Although some suspects will be very careful in hiding their online and computer history, others will be less technically aware or more brazen. Recovered phones and computers can be an evidential goldmine, revealing evidence of chat and other communications, financial activity, photographs and videos and locations visited, together with browsing activity, showing operational planning or the viewing of propaganda.

In preparing a case for court, analytical charts can illustrate the links between the accused and their actions online or elsewhere. Expert testimony can be presented to the court to explain the technical elements underlying the recovery of data, while other subject matter experts can provide context on terrorist groups and the role played by social media in the recruitment of FTFs. The topic of digital data recovery is covered in greater depth in chapter 4.

Proving intent prior to travel

One of the hardest challenges is in trying to prove the purpose of a person's intended travel, before they actually join the terrorist organization in the conflict zone. Nowadays FTFs will often break their journeys, routing through different countries in order to disguise their final destination and will create elaborate cover stories in an attempt to show that their actions are innocent. Another complicating factor is the diffuse structure of terrorist networks, often making the link between the individual planning to travel and the terrorist organization very tenuous. Individuals have even travelled to conflict zones without being a part of any terrorist network before leaving. In many cases it may not be possible to sufficiently prove the individual's intent, and where available, administrative measures might need to be used as an alternative means of preventing travel. Unless carefully managed however, they may only serve to postpone or divert the problem.

Corroborating evidence can be gained, for example, from Internet activity, including posts on social media and communications with friends regarding their intentions; voicing support for ISIL and other groups; research online about destinations, terrorist groups and ways of crossing borders; downloading of weapons training manuals and other instructional material; or the viewing of propaganda illustrating the terrorist mindset of the individual. Financial transaction information can also assist. For instance, facts relevant to intent include receiving loans to cover the cost of travel, unexplained receipt of cash transfers from abroad, the termination of the rental on a home, and disposal of personal possessions. New "clean" mobile phones will often be purchased prior to travel, as well as boots, rucksacks and specialized outdoor clothing for the conflict zone. With these elements added together, a prosecution case can start to build.

Most of the methods referred to in this chapter are reactive investigation techniques. Pro-active criminal investigations can additionally be carried out into FTFs and their networks, using techniques developed for collecting intelligence but employing them for the purpose of gathering sufficient evidence to prosecute. Techniques may include:

- Directed surveillance, such as following and observing suspects
- Interception of communications, such as monitoring emails or phone calls
- Monitoring of other forms of Internet activity
- Analysis of communications data obtained from communications service providers
- Intrusive surveillance, such as putting eavesdropping devices in someone's home or car
- Equipment interference, such as covertly accessing computers or other electronic devices
- Deployment of undercover operatives, either in person or online (members of a law enforcement agency trained to gather intelligence and evidence)

Case study: Imran Khawaja

In January 2014, British national Imran Khawaja left the United Kingdom for the Syrian Arab Republic, to join a group of ex-criminal gang members from London who had travelled to fight alongside ISIL. There Khawaja undertook weapons training, and under the nomme-de-guerre of Abu Daigham al-Britani, he appeared in videos and social media posts encouraging other United Kingdom nationals to join the conflict. The online postings were monitored and captured evidentially by counter-terrorism investigators. Then, in May 2014, it was announced on Instagram that Abu Daigham had been killed in battle. This was false. Khawaja was still alive and had travelled out of the Syrian Arab Republic to Sofia, Bulgaria. There he met his cousin Tahir Bhatti, who had driven across Europe in a hired car to drive back to London together, where it was believed Khawaja intended to engage in further terrorist activity.

A week later both men were stopped entering the United Kingdom and arrested on suspicion of involvement in terrorism. The evidence against Khawaja was initially extremely thin; in the videos he had been fully masked, and he claimed to have been on holiday touring Europe. He was wearing new clothes purchased in France, and stated his mobile phone had been stolen. Searches were conducted at the homes of family members and associates, and their smartphones and computers were seized and examined. Discovered on these devices were photographs sent by Khawaja with chat messages, showing him unmasked and handling firearms.

These images were forensically examined against those downloaded from social media. Experts in facial mapping compared facial features, body features and identifying characteristics of clothing. Military experts identified the weapons shown in photographs, while others using satellite imagery were able to show that the locations depicted were in areas of combat in the Syrian Arab Republic. Encrypted chat with family members was also recovered from phones and decrypted. In messages Khawaja spoke of training with ISIL, stating that he intended to die a martyr.

Due to the weight of the evidence against him Khawaja pleaded guilty at court. Admitting the offences of preparation of terrorist acts, attending a terrorist training camp and receiving weapons training, he was sentenced to 12 years' imprisonment. His cousin Bhatti received 21 months' imprisonment for the offence of assisting an offender.

Source: The Crown Prosecution Service of England and Wales, R v Imran Mohammed Khawaja, Tahir Farooq Bhatti and Asim Ali. At https://www.cps.gov.uk/counter-terrorism-division-crown-prosecution-service-cps-successful-prosecutions-end-2006.

Chapter 2

Global framework

2.1 Introduction

The global framework on preventing and countering violent extremism and terrorism is principally set through the United Nations Global Counter-Terrorism Strategy, composed of four pillars:

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

The global strategy relies on both criminal justice measures as well as through governance measures with both approaches mutually reinforcing the other.

The criminal justice approach to preventing violent extremism and terrorism derives its foundation principally from the application of criminal laws of the Member States that establish 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 (discussed below), Member States are required to implement obligations arising under Security Council resolutions and other binding international conventions and protocols into their national laws.

The governance approach is principally used to prevent violent extremism through minimizing or eliminating the conditions conducive to violent extremism leading to terrorism. Deeply entrenched and inconspicuous sociocultural issues that are considered to be root causes of violent extremism may not always be solved through a criminal justice approach. The causes of such problems are typically systemic rather than attributable to a particular individual or even groups of individuals. These "non-criminal" aspects, which include for instance, inequality, perceptions of dissatisfaction and social disenfranchisement, may all factor into the causes that ultimately motivate 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 to 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 of these aspects is reliant upon the other elements for their effective functioning, and collectively espouses a holistic whole-of-government and whole-of-society approach to preventing and countering violent extremism and terrorism.

2.2 International legal framework on terrorism

Overview

Terrorism has been on the agenda of the international community since the 1930s. During the past 40 years, a total of 19 international conventions and protocols have been adopted for the purpose of addressing terrorism and terrorists.

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
- Taking of hostages, and protection of international staff

These instruments are complemented by the United Nations Security Council resolutions to prevent and counter terrorism. Collectively, these instruments create obligations for Member States under international law, whereby Member States must implement these obligations under its national laws.[178]

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

A long list of Security Council resolutions has been adopted in order to meet the challenges of terrorism and violent extremism, and the changing nature of the threat. Among these, resolution 1373 (2001) represents one of the most far-reaching Security Council resolutions adopted for the purposes of countering terrorism.

Agreed and adopted in the wake of the 11 September terrorist attacks in the United States, resolution 1373 provided the impetus and foundation for a series of international instruments targeting terrorism and violent extremism conducive to terrorism. Reaffirming its earlier unequivocal condemnation of these attacks,[179] 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 most revolutionary aspects of resolution 1373 was the introduction of the obligation to criminalize not only terrorist acts themselves, but also preparatory acts such as the financing, planning, facilitating or supporting terrorist acts.

By September 2014, however, a pattern of individuals travelling abroad to join terrorist entities including ISIL, Al-Nusrah Front and other related entities of Al-Qaida, had grown into such a concern that the Security Council adopted resolution 2178 (2014). The resolution specifically addressed such individuals, termed "foreign terrorist fighters" (FTFs). The scope of resolution 2178 (2014) is explored in depth below.

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

[179] Security Council resolution 1368 (2001).

In December 2017, the Security Council adopted resolution 2396. While the subject focus of that resolution is on FTFs, it is principally concerned with returning FTFs, marking a contrast to resolution 2178 that focused on individuals headed outbound to become FTFs. Resolution 2396 also emphasizes the need for Member States to be equipped and ready to deal with not only returning FTFs, but also their families, including children born in conflict zones. Issues are wide ranging, from making assessments of the degree and extent of involvement of the returning FTFs and family members in the conflict, to making determinations on the legal status of their children, including citizenship rights.

Security Council resolutions dealing with FTFs, and terrorism more generally, should be interpreted and understood in light of resolutions adopted earlier. For instance, resolution 2178 builds upon the framework established by resolution 1373 and similarly, resolution 2396 on the resolution 2178 framework. In addition to the three resolutions discussed, a number of other Security Council resolutions exist within the counter-terrorism and counter-FTF framework.

2.3 Criminal justice response to foreign terrorist fighters

Overview

The most relevant United Nations Security Council resolution concerning FTFs is resolution 2178 (2014). This resolution calls upon Member States to enhance their criminal justice response to FTFs by introducing several 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 on 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 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 objective of criminal laws dealing with FTFs. Sanctions regimes suppress and debilitate the capacity of individual FTFs and terrorist organizations that are listed under the sanctions list. 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 list. Preventative measures are self-explanatory in that their primary function is to prevent the would-be FTFs or terrorists from travelling or otherwise engaging in FTF or terrorism-related activities.

These measures may in some instances appear to be the same or similar, but are actually 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. All three measures are contained in the resolution 2178 framework, as summarized in the table below:

Table 2. Security Council resolution 2178 (2014)—Overview of criminal justice measures

<table>
<tr><th colspan="2">Criminal offences</th></tr>
<tr><td>Resolution para.</td><td>Text</td></tr>
<tr><td>6<i>(a)</i></td><td>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.</td></tr>
<tr><td>6<i>(b)</i></td><td>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.</td></tr>
<tr><td>6<i>(c)</i></td><td>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.</td></tr>
<tr><th colspan="2">Sanctions</th></tr>
<tr><td>Resolution para.</td><td>Text</td></tr>
<tr><td>20</td><td>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 <i>calls upon</i> States to propose such foreign terrorist fighters and those who facilitate or finance their travel and subsequent activities for possible designation.</td></tr>
<tr><th colspan="2">Preventative measures</th></tr>
<tr><td>Resolution para.</td><td>Text</td></tr>
<tr><td>8</td><td>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.</td></tr>
</table>

Criminal offences

Resolution 2178 requires Member States to establish serious criminal 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.

The tables below show a breakdown of the elements of the offences of these aspects relating to FTF-related offences.

Table 3. Breakdown of the elements of the offence—Travel or attempted travel of foreign terrorist fighters

Particulars	Element (act)	Element (intent)
A national, or	travels to a State other than his/her State of residence or nationality	to perpetrate, plan, prepare, or participate in terrorist act, or
an individual in the territory of the Member State		to provide or receive terrorist training

Member States are required to criminalize the travel of nationals to a State other than his or her State of residence or nationality for one of the listed prohibited purposes. This article applies to all Member State nationals travelling to a State other than his or her State of residence or nationality, irrespective of their starting point of travel. The actual act of perpetration, planning, preparation or participation in a terrorist act, or the providing or receiving of terrorist training, is not required for the completion of the offence. What is required, is the act of travelling to a State other his or her State of residence or nationality with the intention to perpetrate, plan, prepare or participate in a terrorist act, or to provide or receive terrorist training. In addition to this, Member States are also called upon to criminalize the *attempt* of the above offences. Thus, having basis in evidence to prosecute, Member States should ideally be able to prevent the travel of individuals travelling abroad as FTFs, by charging the individual(s) concerned with attempting to commit one of the offences.

Example 1:
Individual K, who is a national of and resident in Member State K may travel from Member State A to Member State B to provide terrorist training, without passing through Member State K. This article requires Member State K to establish criminal offences sufficient to prosecute individual K under these circumstances. As individual K is outside the territory of Member State K, he or she can only be prosecuted if the Member State K's national laws criminalize acts committed abroad, outside of its territorial boundaries (i.e. extraterritorial jurisdiction).

Example 2:
Individual K, who is a national of and resident in Member State K, may travel from Member State K, transit through Member State A, to reach final destination in Member State B to participate in a terrorist act. This article requires Member States A and B to establish criminal offences sufficient to prosecute individual K, who has been in their territories and has travelled to a State other than the State of his or her residence or nationality for the purposes of participating in a terrorist act. Thus, authorities of Member States A and B should have the legal authority to arrest and prosecute individual K, based on evidence and in accordance with due process and respect for his or her fundamental rights.

Table 4. Breakdown of the elements of the offence—Financing the travel of foreign terrorist fighters

Element (intent)	Element (act)	Particulars	Particulars	Element (intent)	Particulars
The wilful	provision, directly or indirectly	of funds	by nationals, or	with the intention that they should be used to finance the travel of individuals, or	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
	collection, directly or indirectly		in their territories	in the knowledge that they are to be used to finance the travel of individuals	

Whereas resolution 1373 requires Member States to criminalize the financing of terrorist acts, resolution 2178 builds on the 1373 framework by requiring that such financing activities should be criminalized not only when used to carry out terrorist acts, but also when used to finance the travel of foreign terrorist fighters.

Member States that have already established criminal offences in their national laws to implement requirements under resolution 1373 paragraph 1*(b)* may be able to implement requirements under resolution 2178 paragraph 6*(b)* by making amendments to existing national laws dealing with countering and suppression of terrorism financing. Member States are required to criminalize such acts perpetrated by their nationals, wherever they are situated in the world, as well as acts carried out by non-nationals being carried out in the territory of the Member State. Domestic laws of Member States must give due consideration as to when an act of collecting or providing funds can be construed as being carried out “in their territories”, particularly when such acts are undertaken digitally.

An offence under resolution 2178 does not require that an individual for whom funds are being provided or collected to has actually engaged in travel abroad, in order for the offence to have been committed. What is required is that such funds are provided or collected “with the intention” or “in the knowledge” that they be used to finance the travel of potential FTFs. Funding may come from a single or from multiple sources.

Member States will need to interpret “provision” and “collection” in accordance with the definition and meaning established under its own laws. Similarly, “funds” will also need to be interpreted under national laws. Given the increasingly sophisticated methods of financing for illicit purposes, Member States may wish to ensure that other exchangeable items such as virtual currencies are also covered within their definition of “funds”. Member States may consider the definition of article 1(1) of the International Convention for the Suppression of the Financing of Terrorism, which defines “funds” as: “assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, traveller’s cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit.”

Example 3:

A citizen of Member State Q may be recruiting people in that country to join a terrorist group based in Member State S, as a result of which a number of citizens of Member State Q decide to travel to Member State S. At the same time, another person may provide funds for airfare tickets from State Q to State R, and additional funds for travelling from State R to State S.

Although this article does not require Member State to criminalize the attempt of the provision or collection of funds for one of the listed prohibited purposes, Member States are free to do so and may wish to consider this aspect in their national laws.

Table 5. Breakdown of the elements of the offence—Organizing or facilitating (including recruitment) the travel of foreign terrorist fighters

Element (intent)	Element (act)	Particulars	Particulars	Element (act)	Element (intent)
The wilful	organization of travel, or	by a national, or	of the travel of individuals who	travel to a State other than their States of residence or nationality	to perpetrate, plan, prepare, or participate in terrorist act, or
	facilitation of the travel	in the territory of the Member State			to provide or receive terrorist training

Security Council resolution 1373 requires Member States to ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice and ensure that, in addition to any other measures against them, such terrorist acts are established as serious criminal offences in domestic laws. Resolution 2178 expands on this by requiring Member States to criminalize any act of "organization or facilitation, including acts of recruitment" that assists a person who is committing the crime of travelling abroad for the purpose of terrorism.

While terms such as "organization" and "facilitation" will be interpreted in accordance with the definitions and meanings given under such domestic legislation, broadly, "organization" may cover conduct related to practical arrangements connected with travelling, such as planning the travel routes, while "facilitation" may refer to a more direct form support, such as assisting in unlawful border crossing. The perpetrator must act intentionally, unlawfully and with the knowledge that the organization or facilitation is provided for terrorism purposes. Of particular interest and concern for many Member States will be the recruitment of its nationals, minors and youth in particular, through the Internet and other digital platforms such as encrypted messaging services.

As with other criminalization requirements under resolution 2178, Member States are required to criminalize such acts perpetrated by their nationals, wherever they are situated in the world, as well as acts carried out by non-nationals being carried out in the territory of the Member State.

Table 5. (cont'd)

Member States are required to criminalize any act of "organization or facilitation, including acts of recruitment" that assist a person who is committing the crime of travelling abroad for the purpose of terrorism. While terms such as "organization" and "facilitation" will be interpreted in accordance with the definitions and meaning given under such domestic legislation, broadly:

- "Organization" may cover conduct related to practical arrangements connected with travelling, such as planning the travel routes, while
- "Facilitation" may refer to a more direct form of support, such as assisting in unlawful border crossing.

Example 4:

A group from State M may have close links with other nationals of State M who left for State X and have joined a terrorist organization in State X. Their mutual understanding is that those living in State M will organize the travelling of a number of persons from State M to State X by making plans and providing funds for their route through the State G. The locals in State G assist the recruits to enter the borders of their respective countries illegally and transport them to the next border or the airport. In such case, the group in State M involved in the logistical/practical arrangements have "organized" travelling abroad for the purpose of terrorism, whereas the locals in the State G have "otherwise facilitated" the travelling abroad for the purpose of terrorism.

Sanctions: Security Council resolutions 1267/1989/2253 and 1373

Resolution 2178 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 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 regimes, resolution 1373 requires Member States to establish national sanctions regimes. Individuals subject to national sanctions regimes are designated by governments on their own initiative or following review of a request made by the government of another Member State.

Sanctions typically employ one or more of three measures: travel bans, asset freezing and arms embargos. For FTFs, travel bans are of particular importance to disrupt the travel of FTFs into conflict zones.

In order for sanctions to be effective, 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, in order to implement sanctions effectively and in a timely manner. Law enforcement officials should be familiar with the listing and de-listing procedures applicable under the United Nations sanctions regimes as well as the national terrorist sanctions regime within their respective jurisdictions.

Preventative measures

Security Council resolution 1373 (2001) requires Member States to prevent the movement of terrorists or terrorist groups by effective border controls and controls on the issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents.[180]

[180] Security Council resolution 1373 (2001), paragraph 2(*g*).

Resolution 2178 (2014), among other things, requires Member States to prevent the entry into or transit through their territories of any individual about whom the 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 one of the criminal offences established under the resolution.[181]

As per the text of the resolution, such preventative measures in the nature of travel restrictions are triggered when the legal threshold of having "reasonable grounds to believe …" is met, based on "credible information". 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 that 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, but with insufficient evidence to successfully prosecute and secure a conviction.

2.4 Regional cooperation frameworks

Introduction

As the movements of FTFs are transnational by definition, regional and cross-regional cooperation becomes a vital part of implementing the global counter-terrorism framework.

Both in South Asia and South-East Asia, regional bodies such as the South Asian Association for Regional Cooperation (SAARC) and the Association of Southeast Asian Nations (ASEAN) have provided a platform for regional cooperation on preventing and countering violent extremism and terrorism.

In ASEAN, the issue of terrorism was largely treated as one part of the wider transnational crime agenda up until the terrorist attacks on 11 September 2001, which marked a turning point from this approach. As early as October 2001, ASEAN ministers agreed that the work programme to implement the ASEAN Plan of Action to Combat Transnational Crime should have a particular focus on terrorism.[182] The framework dealing specifically with terrorism prevention was set out by the ASEAN Heads of Governments, through the adoption of the ASEAN Declaration on Joint Action to Counter Terrorism.[183]

Similarly, in February 2009, the SAARC Council of Ministers adopted the Declaration on Cooperation in Combating Terrorism. The meeting also served as a platform for the Ministers to review existing cooperative terrorism prevention mechanisms including the SAARC Terrorism Offences Monitoring Desk, intelligence sharing and police cooperation. A summary of the broadly drafted key measures endorsed in ASEAN and SAARC are summarized below:

[181] Security Council resolution 2178 (2014), paragraph 8.

[182] ASEAN, Joint Communique of the Third ASEAN Ministerial Meeting on Transnational Crime Singapore, paragraph 18 (11 October 2001). At http://asean.org/?static_post=joint-communique-of-the-third-asean-ministerial-meeting-on-transnational-crime-ammtc-singapore-11-october-2001.

[183] ASEAN, Joint Declaration on Joint Action to Counter Terrorism (2001). At http://asean.org/?static_post=2001-asean-declaration-on-joint-action-to-counter-terrorism.

Table 6. Key provisions in regional declarations in South Asia and South-East Asia

ASEAN Declaration on Joint Action to Counter Terrorism	SAARC Declaration on Cooperation in Combating Terrorism
• Review and strengthen national mechanisms to combat terrorism. • Call for the early signing/ratification of or accession to all relevant anti-terrorist conventions including the International Convention for the Suppression of the Financing of Terrorism. • Deepen cooperation among front-line law enforcement agencies in combating terrorism and sharing “best practices”. • Study relevant international conventions on terrorism with the view to integrating them with ASEAN mechanisms on combating international terrorism. • Enhance information/intelligence exchange to facilitate the flow of information, in particular, on terrorists and terrorist organizations, their movement and funding, and any other information needed to protect lives, property and the security of all modes of travel. • Strengthen existing cooperation and coordination between the AMMTC and other relevant ASEAN bodies in countering, preventing and suppressing all forms of terrorist acts. Particular attention would be paid to finding ways to combat terrorist organizations, support infrastructure and funding and bringing the perpetrators to justice. • Develop regional capacity building programmes to enhance existing capabilities of ASEAN member countries to investigate, detect, monitor and report on terrorist acts. • Discuss and explore practical ideas and initiatives to increase ASEAN’s role in and involvement with the international community including extra-regional partners within existing frameworks such as the ASEAN + 3, the ASEAN Dialogue Partners and the ASEAN Regional Forum (ARF), to make the fight against terrorism a truly regional and global endeavour. • Strengthen cooperation at bilateral, regional and international levels in combating terrorism in a comprehensive manner and affirm that at the international level the United Nations should play a major role in this regard.	• Implement measures against organizing, instigating, facilitating, financing, fund raising, encouraging, tolerating and providing training for or otherwise supporting terrorist activities. Take appropriate practical measures, administrative and legal, to ensure that Member States’ territories are not used for terrorist installations or training camps, or for the preparation or organization of terrorist acts intended to be committed against other States or their citizens. • Ensure the apprehension and prosecution or extradition of persons connected, directly or indirectly, with the commission of terrorist acts, subject to the provisions of our national laws and our international commitments towards this end, to extend cooperation, inter alia, through rendering mutual legal assistance. • Ensure that nationals of Member States or other persons and entities within Member States’ territories that commit or attempt to commit, facilitate or participate in the commission of terrorist acts are appropriately punished. • Support the promotion of cooperation and exchange of information, consistent with the Member States’ respective domestic legal and administrative regimes, improve immigration and customs control measures to detect and prevent the international movement of terrorists and their accomplices, and trafficking in arms, narcotics and psychotropic substances or other materials, intended to support terrorism, and in this context, to consider the development of an integrated border management mechanism. • Take steps to share expertise and information about terrorists, their movements, their support facilities and their weapons, bearing in mind in particular, the threats posed to maritime and coastal security and to share information regarding the investigation and prosecution of terrorist acts. • Contribute to the efforts in the United Nations General Assembly for the early adoption of the United Nations draft Comprehensive Convention on International Terrorism. • Urgently ratify and effectively implement the SAARC Convention on Mutual Legal Assistance in Criminal Matters. • Strengthen the SAARC and the global regime against terrorism and to establish a High-Level Group of Eminent Experts to review and make proposals to further strengthen SAARC anti-terrorism mechanisms, including for pragmatic cooperation.

Regional counter-terrorism conventions

By its very nature, investigating and prosecuting FTFs requires effective and fluid international cooperation and information exchange practices among Member States. The effectiveness of national criminal justice frameworks on investigating and prosecuting FTFs is inextricably linked to the effectiveness of international cooperation measures. Depending on the locality of the evidence, access may be granted through international, regional or bilateral, or informal cooperation.

The ASEAN Convention on Counter-Terrorism,[184] creates rules on jurisdiction and mutual legal assistance, and lists extensive areas of cooperation among ASEAN Member States. The architecture of the ASEAN Convention is intrinsically tied to 14 of the 19 international conventions and protocols on terrorism, as it defines criminal acts of terrorism as terrorism offences within the scope of those 14 instruments. In this regard, the convention does not create any new offences relating to terrorism. Rather, it serves as a framework for regional cooperation to counter, prevent and suppress terrorism among ASEAN Member States. The convention creates a minimum requirement for that cooperation, but encourages Member States to go beyond the minimum requirements and forge closer relationships for greater cooperation.

A related instrument in the context of investigating and prosecuting FTFs is the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters. While the focus of the ASEAN Convention is primarily on establishing criminal jurisdiction over terrorist offences and implementing the principle of "prosecute or extradite", the ASEAN Treaty on Mutual Legal Assistance deals with cooperation to support investigation and prosecution, such as the taking of evidence or execution of search and seizures. It does not apply to the arrest or detention of an individual with a view to the extradition of that individual, which is covered by the ASEAN Convention.

SAARC Member States adopted the Regional Convention on Suppression of Terrorism[185] as early as 1987 as a regional agreement to counter, prevent and suppress terrorism. The SAARC Additional Protocol to the Convention[186] was adopted in 2004, incorporating requirements of resolution 1373 into the 1987 Convention. Practitioners are encouraged to familiarize themselves with the Convention and the Additional Protocol.

Regional mutual legal assistance treaties

FTF movements are transnational by nature. Regional and cross-regional cooperation therefore becomes a vital part of implementing the global counter-terrorism framework. In South Asia and South-East Asia, regional bodies such as SAARC and ASEAN have provided a platform for regional cooperation on preventing and countering violent extremism and terrorism.

In ASEAN, the issue of terrorism was largely treated as one part of the wider transnational crime agenda up until the terrorist attacks on 11 September 2001, which marked a turning point from this approach. As early as in October 2001, ASEAN Ministers agreed that the work programme to implement the ASEAN Plan of Action to Combat Transnational Crime should have a particular focus on terrorism. The framework dealing specifically with terrorism prevention was set out by the ASEAN Heads of Governments, through the adoption of the ASEAN Declaration on Joint Action to Counter

[184] The ACCT was adopted in 2007 and entered into force in May 2011. By January 2013, all ten ASEAN Member States were State Parties to the Convention. The full text of the convention is accessible at http://asean.org/?static_post=asean-convention-on-counter-terrorism.

[185] Signed 4 November 1987 and entered into force on 22 August 1988 following its ratification by all Member States. The full text of the Convention is accessible at https://treaties.un.org/doc/db/Terrorism/Conv18-english.pdf.

[186] Signed 6 January 2004 and entered into force on 12 January 2006 following its ratification by all Member States. The full text of the Additional Protocol is accessible at http://www.refworld.org/pdfid/49f6b7ad2.pdf.

Terrorism.[187] Similarly, in February 2009, the SAARC Council of Ministers adopted the "Declaration on Cooperation in Combating Terrorism". The meeting also served as a platform for the Ministers to review existing cooperative terrorism prevention mechanisms including the STOMD (SAARC Terrorism Offences Monitoring Desk), intelligence sharing and police cooperation as well as discussion of issues surrounding terrorist financing and other related topics.

The ASEAN Convention on Counter-Terrorism,[188] among other things, creates rules on jurisdiction and mutual legal assistance, in addition to listing extensive areas of cooperation among ASEAN Member States when dealing with individuals suspected of terrorism offences. The architecture of this Convention is intrinsically tied to 14 of the 19 international conventions and protocols, as it defines criminal acts of terrorism by reference to criminal offences established under these 14 instruments. In this regard, it should be noted that unlike international instruments, including Security Council resolutions, the ASEAN Convention does not create any new terrorism offences. Rather, it serves as a framework for regional cooperation to counter, prevent and suppress terrorism among ASEAN Member States. The Convention establishes minimum requirements for cooperation but encourages Member States to go further and forge closer collaborative relationships.

A related instrument in the context of investigating and prosecuting FTFs is the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters.[189] While the focus of the ASEAN Counter-Terrorism Convention is primarily on establishing criminal jurisdiction over terrorist offences, the Mutual Legal Assistance Treaty deals with cooperation to support investigation and prosecution, such as the taking of evidence or execution of search and seizures. It does not apply to the arrest or detention of an individual with a view to the extradition of that individual, which fall in the ambit of the Counter-Terrorism Convention. The ASEAN Mutual Legal Assistance Treaty applies in relation to investigation and prosecution of all criminal matters, including terrorism and FTF offences.

While these instruments serve as a basis for international cooperation on various terrorism-related matters, they may not cover the entire spectrum of international cooperation and information exchange needs and requirements arising in the course of the investigation, prosecution and adjudication of FTF cases. Even where assistance requests may fall within the coverage of these instruments, it may not necessarily be the most appropriate or effective means of requesting and obtaining such assistance. Law enforcement personnel should consider the full range of options available at their disposal, including informal cooperation, bilateral agreements and other multilateral agreements.

In South Asia, SAARC Member States adopted the Regional Convention on Suppression of Terrorism[190] as early as 1987, as a regional agreement to counter, prevent and suppress terrorism. Following the attacks of 11 September 2001, which provided the impetus for the adoption of Security Council resolution 1373, the SAARC Additional Protocol to the Convention[191] was adopted in 2004, incorporating requirements of Security Council resolution 1373 into the 1987 Convention. The two documents—the Convention (1987) and the Additional Protocol (2004)—should be read together as one document.[192]

[187] ASEAN, Joint Declaration on Joint Action to Counter Terrorism (2001). At http://asean.org/?static_post=2001-asean-declaration-on-joint-action-to-counter-terrorism.

[188] The ACCT was adopted in 2007 and entered into force in May 2011. By January 2013, all ten ASEAN Member States were State Parties to the Convention. The full text of the convention is accessible at http://asean.org/?static_post=asean-convention-on-counter-terrorism.

[189] The ASEAN MLAT was adopted in November 2004 and enters into force for each Member State upon ratification. All 10 ASEAN Member States have ratified the treaty, with the final instrument of ratification having been deposited by Thailand in January 2013. The full text is accessible at http://agreement.asean.org/media/download/20160901074559.pdf.

[190] Signed 4 November 1987 and entered into force on 22 August 1988 following its ratification by all Member States. The full text of the Convention is accessible at https://treaties.un.org/doc/db/Terrorism/Conv18-english.pdf.

[191] Signed 6 January 2004 and entered into force on 12 January 2006 following its ratification by all Member States. The full text of the Additional Protocol is accessible at http://www.refworld.org/pdfid/49f6b7ad2.pdf.

[192] See Article 2 of the Additional Protocol: Relationship to the SAARC Convention.

In 2008, SAARC's Convention on Mutual Assistance in Criminal Matters was adopted to enable Member States to request, receive and provide each other with the widest possible measures of mutual legal assistance in criminal matters. The Mutual Assistance Convention is not yet in force, as it requires formal ratification by all Member States.[193] Entry into force of the SAARC MLAT will provide Member States with a regional MLA framework allowing Member States to make requests to one another, including for locating and identifying persons, obtaining information, evidence, search and seizure, and measures to locate, freeze and confiscate funds, among other forms of rendering mutual assistance. The scope of such assistance would not however extend to the arrest or detention of any person with a view to the extradition of such persons, although a State Party may temporarily transfer a detained individual to a requesting State to assist in investigations or to testify, if the individual consents to such an arrangement.

While the SAARC Mutual Assistance framework may, upon entering into force, be important for the purpose of investigating cases involving FTFs, the framework governing the extradition of individuals suspected of FTF offences will continue to be found outside this document, including the 1987 Convention, the 2004 Additional Protocol, bilateral agreements and extradition requests granted on the basis of reciprocity or otherwise.

For more information on mutual legal assistance, see also:

- The website of the Official Portal of Secretariat for the Treaty on Mutual Legal Assistance in Criminal Matters among Like-Minded ASEAN Member Countries[194]
- UNODC Guide to Mutual Legal Assistance from East Asia and the Pacific Region, 2013 [195]
- Compendium of Bilateral and Regional Instruments for South Asia (International Cooperation in Criminal Matters), 2015 (Volumes 1and 2)[196,197]
- Counter Terrorism Legal Training Manual Module 3: International cooperation in criminal matters: counter-terrorism [198]
- The Mutual Legal Assistance Writer Tool. The Tool is made available by UNODC for criminal justice practitioners [199]

2.5 International legal framework and civil society

The United Nations Secretary-General's Plan of Action on Preventing Violent Extremism 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 in terms of preventing and countering violent extremism in order to deliver a rounded and effective approach has been addressed on a number of occasions by the international community:

[193] As of December 2017, 5 of 8 SAARC Member States are parties to the Convention.

[194] Accessible at http://aseanmlatsec.agc.gov.my/index.php?r=portal/index&id=UWxJVHc4NWpiNENxRG9FclZBVGxlUT09.

[195] Accessible at https://www.unodc.org/documents/southeastasiaandpacific//2013/07/mla/Guide_To_Mutual_Legal_Assistance.pdf.

[196] Accessible at https://www.unodc.org/documents/terrorism/Publications/SAARC%20compendium/SA_Compendium_Volume-1.pdf.

[197] Accessible at https://www.unodc.org/documents/terrorism/Publications/SAARC%20compendium/SA_Compendium_Volume-2.pdf.

[198] Accessible at https://www.unodc.org/documents/terrorism/Publications/Training_Curriculum_Module3/Module3_EN.pdf.

[199] Accessible at https://www.unodc.org/mla/.

- The United Nations Security Council, through the resolution 1624 highlights "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 addresses 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".
- Resolution 2178 encourages Member States to "engage relevant local communities and non-governmental actors in developing strategies" to counter violent extremism; this is the first time that countering violent extremism is mentioned in a resolution adopted under chapter VII of the United Nations Charter.

Therefore, it is crucial that South and South-East Asian States consider this cooperation and collaboration with civil society organizations when drafting their own national plans to prevent and counter violent extremism. States should allocate appropriate resources for these efforts.

Chapter 3

Investigations and foreign terrorist fighters

3.1 Introduction

The increased dependency on communication and data networks presents new challenges to law enforcement and prosecutorial authorities in combating the threat posed by terrorism, and FTF in particular. Terrorists have been among the first groups to exploit these new technologies for criminal purposes.

Computers and the Internet are rapidly becoming one of the key features of modern terrorism investigations, and both can be used in the commission of crime. They can also contain evidence of crime and can even be targets of crime.

The spread of radicalization on social media is causing increasing concern, with a reported 90,000 Twitter accounts having been controlled by ISIL at its peak, to target and recruit young people into a war—a war where hashtags have become a new weapon.[200]

This chapter will discuss the challenges faced and review current good practices in securing digital evidence (also known as e-evidence) as well as looking into online investigations, and will cover areas including:

- Technical terminology
- Storage media typologies
- New technologies in the fields of encryption
- Hidden data programs
- Techniques in developing online investigations
- The impact of social media on FTF investigations
- Stages by which social media intelligence (SOCMINT) can be exploited for evidential gain
- Methods and techniques for exploiting SOCMINT

3.2 Securing digital evidence

For the purposes of this manual, unless referring to a direct quote, the term “digital evidence” means information and data of value to an investigation that is stored on, received or transmitted by an electronic device. Other terms, roughly equivalent, are:

[200] “How Terrorists Communicate - Dark Web”. At https://www.retire.ly/how-terrorists-communicate-dark-web/.

ESI (Electronically stored information)

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 cell phones
- Information stored on computers, computer systems, thumb drives, flash drives, CDs, tapes and other digital media

Computer-based electronic evidence

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 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.

Much of this evidence is acquired when data or electronic devices are seized during investigations and secured for examination. Digital evidence can rapidly transit jurisdictional borders with ease, can easily be altered, damaged or destroyed, and can be time sensitive. 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 with legal and procedural requirements relating to admissibility and rules of evidence (domestic and international) is also required. When deciding on what digital evidence to collect, consideration should be given to the environment in which such information and evidence will be gathered, for example, through an online investigation, or at a crime scene (for instance, on a device at the premises of a suspect).

Terminology: the worldwide web, websites and web pages

The worldwide web (www) is only one part of the Internet. Fundamentally, it is an information space where documents and other resources can be accessed (music files, videos or images, for example).

At the time that the “web” was developed, three specifications for web technologies were defined. These are:

- Hyper Text Markup Language (HTML)
- Hyper Text Transfer Protocol (HTTP)
- Uniform Resource Locators (URL)

A web page is a document that is suitable for the worldwide web and can be viewed using a web browser, which is a piece of software that displays the web page on a computer monitor or mobile device. Examples of web browsers include: Internet Explorer, Safari, Firefox and Google Chrome. In order for a computer monitor to correctly display a web page, the page is written in a programming language called Hyper Text Markup Language (HTML). HTML contains formatting instructions for the web browser to coordinate the various elements required to present the web page, such as style, scripts, images and links.

Web pages are accessed and transported (i.e. made accessible) with the Hypertext Transfer Protocol (HTTP), which may optionally employ encryption (HTTP Secure or HTTPS) to provide security and privacy for the user.

To display the contents of a web page on a computer, the computer's browser must know where on the worldwide web the web page is housed. The address of the web page is known as a Uniform Resource Locator (URL).

A typical address looks like this: http://www.something.com/filename, where "filename" is the file being viewed (if the web page being viewed is from a secure server used, the address would instead begin with https://...)

A website is a collection of related web pages, including multimedia content, typically identified with a common domain name (e.g. www.something.com) and published on at least one web server (computer servers where websites are housed).

The Internet

The Internet is a huge system of interconnected computer networks (a network of networks), and consists of millions of private, public, academic, business and government networks, linked by a broad array of electronic, wireless and optical networking technologies. These links are possible due to a number of global protocols (or rules), the most important of which for an investigator is the Transmission Control Protocol and Internet Protocol (or TCP/IP).

Internet Protocol (IP) is a scheme of assigning an address to each device attached to the Internet. This address allows a device to connect and communicate with any other device that is also connected to the Internet using this scheme.

Transmission Control Protocol (TCP), on the other hand, enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

There are two versions of IP: IPv4 and IPv6. IPv4 allows for the possibility of over 4 billion unique addresses. With the massive growth of the Internet, it is expected that the number of unused IPv4 addresses will eventually run out. Thus, Internet Protocol version 6 (IPv6) is being deployed to create more Internet addresses. The two IP versions will be running in tandem for some time in the future, so investigators can expect to see both versions during their research.

What do version 4 and version 6 IP addresses look like?

IP version 4	IP version 6
A 32-bit numeric address is written in decimal as four numbers separated by full stops. Each number can be zero to 255. For example, 1.160.10.240 would represent an IPv4 address.	IPv6 addresses are 128-bit IP addresses written in hexadecimal[a] and separated by colons. An example IPv6 address could be: 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

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

There are two ways in which a device can be allocated an IP address when it connects to the Internet: either with a dynamic or static allocation:

- A static IP address is normally allocated to a server providing a service, such as a web page. Assigning a static (or permanent) address helps devices return to that same location on the Internet.
- Dynamically assigned addresses are created through a process called Dynamic Host Configuration Protocol (DHCP). This protocol is a piece of software running, for example, on a server or router 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 that are available. Discovering the IP address of a suspect's device forms part of the investigation trail that needs to be followed.

Once an IP address has been identified, an Internet search can reveal the Internet Service Provider (ISP), the company that connected the device to the Internet. Gaining access to the Internet via an ISP requires a subscription to that particular company. These companies have records of the details of their subscribers as well as those subscribers' activities on the Internet.

The timeframe that ISPs retain data relating to subscribers' activities online varies, therefore an investigation must attempt to make progress as quickly as possible. Investigators can make a formal request to the ISP requesting that they preserve the data in question while a subpoena, warrant or court order is made requiring production of the records. As there is no common data retention policy in place, ISPs have the discretion to decide on data retention time frames: some retain data for six months or more; some for two months; and some for as little as 14 days.

There are two kinds of IP addresses:

- *Local IP*: Local IP addresses are used to identify a computer within a single network (e.g. an office network). Because they are network-specific, these are often re-occurring. They can also change whenever you (re)connect to a network.
- *Global IP:* A global IP address (also called a public, or external IP address) is used to identify a device across the Internet: it is network specific. This means that every computer using the same network to access the Internet (e.g. at your home) will have the same global IP address.

Websites and cookies

Ultimately, any information on the Internet physically resides on one or more computer systems and, therefore, it could be retrieved through a forensic examination of those physical devices. However, some of this information may be volatile (e.g. instant messaging content), or it could be altered or deleted prior to locating and examining 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.[201]

[201] "Association of Chief Police Officers Good Practice Guide for Digital Evidence" (March 2012). At http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf.

There are many tools freely available to assist including:

- HT Tracks[a]
  - This is a website copier that allows the complete download of a website from the Internet to a computer in a local directory. The software downloads all website content, including links and allows the site to be viewed (completely) offline as a "mirrored" site.
- Wget[b]
  - A program that retrieves content from web servers.
- Wayback machine
  - Wayback machine is a website archive site. The site contains a large collection of sites saved from the past. As such you are able to view a website as it would have looked in the past.
- Scrapbook[c]
  - An easy to use "plug in" for the Firefox browser that helps to save websites, web pages or snippets of web pages.

[a] Accessible at www.httrack.com/.

[b] Accessible at https://archive.org/web/.

[c] Accessible at http://www.whatarecookies.com/.

Once a website has been captured or collected, an investigator will have access to potentially useful investigative information. The pages themselves can be reviewed, as can the way in which the browser produces the page. An investigator can look for who wrote the web page and also check on names of people, organizations or groups that claim responsibility for a website. For instance, there may be an email address for a person or group, and an investigator can utilize Internet research tools to establish if that email has been used elsewhere on the Internet.

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 and website and can be accessed either by the web server or the client computer. This allows the server to deliver a page tailored to a particular user (for instance, remembering use of a password), or to learn information about the user's visits to web pages prior to the current page.[202]

Imagine, for example, 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 his or her Facebook account while in the Syrian Arab Republic. The Facebook website would have "left" a cookie on the suspect's mobile phone (unless of course cookies were denied or deleted by the user). Upon investigation, it is discovered that the same Facebook cookie is associated with a number of other Facebook users. This could possibly indicate that the suspect's phone was used by other foreign fighters while in the Syrian Arab Republic, which provides intelligence leads for further development.

[202] Accessible at www.whatarecookies.com/.

Deep web and dark web

The Internet as a whole may be divided into three sections:

- *Surface Web*: also called the Visible Web—that part of the worldwide web that can be searched with standard web search engines.
- *Deep Web*: content of the Deep Web that is not indexed by search engines, but can be reached through clicking links, filling forms or entering personal login credentials. For example, after a search engine provides links to hotel booking websites, the user must visit a website and specify hotel criteria to view a list of available offers—an interaction with Deep Web content.[203] This content includes email messages, chat messages, electronic bank statements and private content on social media sites.
- *Dark Web*: part of the Internet that is not indexed by search engines, such as Google or Bing, and where connections are intentionally encrypted to disrupt the possibilities of tracking web activity.[204] This is the area where much of the criminal activity on the Internet takes place.

Log files

Web servers maintain log files listing every request made to the server. With log file analysis tools, it is possible to get a good idea of the Internet activity of visitors prior to visiting the site under investigation, how often they return, and how they navigate through a site. Using cookies enables the person or organization responsible for administering a website (known as the "Webmaster") to log even more detailed information about how individual users are accessing and interacting with a site.

Each computer stores a number of log files that can provide evidence of a user's activity. Through these log files, it can be determined what websites have been accessed, to and from whom emails are sent and received and also, the kinds of applications being used. In many cases, this information can be located even after a user has deleted what is thought to have been all the evidence—deleting an email, or a file, doesn't completely erase the trail.

Here are a few places where log files can be found:

- Operating systems
- Web browsers (in the form of a cache)
- Applications (in the form of backups)
- Email
- Temporary Internet Files

Other examples of information that can be gathered from devices, and used very effectively as evidence, include computer documents, emails, SMS and instant messages, transactions, images and Internet histories.

Websites themselves maintain IP logs, which are automatically created and record the traffic accessing a site. For instance, the Google email site Gmail would maintain IP logs for email account holders and for the original IP from where the account was first registered. Subsequent enquiries with Internet Service Providers (ISP) would reveal the person or organization associated with those IP addresses.

Encryption and anonymizing techniques employed in connection with other forms of Internet communication are similarly applicable to files shared via, inter alia, peer-to-peer (P2P) and File

[203] "Clearing Up Confusion - Deep Web vs. Dark Web", *BrightPlanet* (27 March 2014). At https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/.

[204] "How Terrorists Communicate - Dark Web". At https://www.retire.ly/how-terrorists-communicate-dark-web/.

Transfer Protocol (FTP) technology. Multiple file-sharing websites exist, offering varying degrees of anonymity, file size limits and file expiration times; these provide parties with the ability to easily upload, share, locate and access multimedia via the Internet. Some file-sharing websites may maintain transfer logs or payment information, which may be relevant to an investigation. Because these sites attract scrutiny for intellectual property violations, they permanently shut down without notice, or resurface under different branding in different jurisdictions.

It is more than likely that the data servers used to provide these services will 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 authorities in those jurisdictions may therefore be required to obtain key evidence for legal proceedings.[205] In such cases, competent national authorities should make use of the available tools for international cooperation, i.e. requesting mutual legal assistance (MLA).[206]

Investigators should also consider referring to the UNODC document "Basic tips for investigators and prosecutors for requesting electronic/digital data/evidence from foreign jurisdictions",[a] which outlines a number of good practices including, for instance, the need to have exhausted internal/national sources for obtaining electronic data/evidence prior to sending requests to a foreign country and, in consideration of an investigative strategy, to verify with the requested authority whether an account holder may learn of any preservation request (for instance if it is the policy of an ISP to notify their clients). Also, see the UNODC website for assistance in preparing an MLA request with the Mutual Legal Assistance Request Writer Tool:
http://www.unodc.org/mla/en/index.html

[a] UNODC, "Basic tips for investigators and prosecutors for requesting electronic/digital data/evidence from foreign jurisdictions". At https://www.unodc.org/documents/legal-tools/Tip_electronic_evidence_final_Eng_logo.pdf.

Consideration should also be given as to whether the formal requirements in the MLA procedures may be different depending what data is requested—for example, whether it is subscriber, traffic or content data). Subscriber data relates to information about the user of a service; traffic data relates to information about the connections made between telephones or computers; content data relates the actual content of a message or conversation.

In some cases, there are specific procedures that law enforcement agencies must follow in order to begin the process of obtaining records from, for example, social media companies and email service providers. The respective websites' terms of service and privacy policies provide details of the standards and requirements for obtaining user information. Some web services have a specific portal through which law enforcement authorities, as a starting point, can make official requests (for instance, Facebook Law Enforcement Online Requests). Web services may also have a law enforcement liaison office to advise and facilitate requests.

[205] UNODC, "Use of the Internet for Terrorist Purposes" (2012). At www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

[206] UNODC, *Manual on Mutual Legal Assistance and Extradition* (2012). At http://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf.

It is good practice, when making data requests, to narrow down the request as much as possible. A request to obtain a year's worth of email data is likely to fail, whereas a targeted request for email data between two suspects may have a greater chance of success. Even if a request for actual email content fails, it may be possible to obtain email headers or other metadata.

Email headers

An email header includes vital information, such as the sender, receiver, return path, email subject, who is in CC and date, etc.

Metadata

Data that describes or summarizes other data.
This kind of data is not normally displayed when viewing the content to which it refers and would include information on, for example, author, date created, date modified and file size.

In many jurisdictions, requirements for access to subscriber data tend to be lower than for traffic data, while a more stringent regime applies to content data.[207]

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 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, Twitter* and *Google* can be found on the website of the International Association of Chiefs of Police (IACP).[208] However, any evidence obtained in this manner may not be admissible in court unless it is "officialized" through the MLA framework.

3.3 Digital evidence at a crime scene

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 crime scene, where physical evidence can be recovered and forensically examined. A physical crime scene in the sense of a digital investigation could also include an element of non-physical evidence, such as information accessed in the "cloud" from a suspect's device. The difficulties 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:

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

[208] Accessible at http://www.theiacp.org.

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

Handling digital evidence

Precautions should always be taken in the collection, preservation and transportation of digital evidence in order to maintain its integrity. The United Kingdom Association of Chiefs of Police guidelines for computer evidence discuss good practice principles in capturing electronically stored information or digital evidence. Devices, peripherals and other materials may be collected once a crime scene has been secured and a legal authority is in place to seize evidence.

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.

- 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 PINs and passwords.
- Recover associated chargers, cables, peripherals and manuals, along with thumb drives, cell phones, external hard drives and electronic photo frames, etc.
- Many of these devices are examined using different tools and techniques, and 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.

Source: "Association of Chief Police Officers Good Practice Guide for Digital Evidence" (March 2012). At http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf.

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 that may subsequently be relied upon in court.
2. In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Source: "Association of Chief Police Officers Good Practice Guide for Digital Evidence" (March 2012). At http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf.

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

As well as a main computer, investigators should also consider computer peripherals that could potentially be of an evidential or intelligence value, along with other potentially valuable digital sources, not immediately obvious in terms of a digital crime scene, including (but not limited to):

- Printers have built-in solid-state memory chips and may contain residual data on previously printed documents that may be recovered using forensic software. Removable storage media may also be present (e.g. SD flash memory cards).
- As well as storing images, digital camera memory (in most cases a removable SD flash memory card) may also be used for storing other files. Even though the memory may have been erased, there will be residual data that can be recovered using forensic software.
- Routers are the bridge between computers and the Internet. They can work in Broadcast (wireless) or Ethernet (hard-wired) modes, and are usually provided by the Internet Service Provider (ISP). Routers contain information on connected devices, IP addresses and network passwords.
- Modern external hard drives can store huge amounts of data. Some may be connected to networks, allowing remote access to data (such as a personal "cloud" service).
- Multimedia storage devices, such as music players, may contain data other than music or video files, for instance web pages or documents.
- USB sticks or flash drives come in various guises and can often look like common household objects, such as a credit card or a cork from a wine bottle.

- The removable memory card from a phone or digital camera is known as SD or flash memory, and comes in various capacities. As with all memory, these cards can store any type of digital data. For instance, 1GB of memory may contain, on average, around 7,000 text documents or around 6,000 messages.
- Previous journeys of a suspect's vehicle may be stored in the satellite navigation system memory. Bear in mind that some satellite navigation systems may also have removable SD/flash memory storage (see above).
- As well as images that may be useful in an investigation, digital photo frames may also store other data, either on the device itself or on removable media such as a USB drive or SD/flash memory cards.

Live forensics

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

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 exists only in the form of the temporary data contained within the computers Random Access Memory or RAM, which is typically lost once the device is powered off.[208] 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 RAM data that could be lost. If a computer is on, using a computer forensic expert is highly recommended, as turning off the computer may result in loss of evidence. Note, however, that turning the power off may be necessary if investigators determine that a data destruction program is active.

A suspect's computer may be running software configured to carry out certain tasks where certain conditions are met. For instance, if there are two unsuccessful attempts to enter a user name and/or password the software will activate. This type of destructive software can format a hard drive or delete/remove/wipe certain information.

If the suspect's computer is on but is running destructive software, power to the computer should be disconnected immediately to preserve whatever is left on the machine.

[209] "Incident Response: Live Forensics and Investigations", p. 103. At http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Incident-Response-Live-Forensics-and-Investigations.pdf.

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

- In 2007, a man was convicted in the United Kingdom for charges under the Terrorism Act, which included developing an encrypted version of an extremist website and posting videos online explaining how to use encryption software to remain anonymous and avoid authorities over the Internet. Some of the software explained included:
  - *ZeroNet*: A program that allows for a version of a website to be created that is virtually impossible for law enforcement to “take-down”. The service uses open source peer-to-peer technology to create multiple copies of Internet files, spread across multiple computers.
  - *Tails*: An operating system that allows users to operate anonymously on the Internet without leaving data behind on their computers.
  - *Veracrypt*: A program that creates a virtual encrypted disk within a file or which encrypts a partition of a drive.
  - *PGP*: An encryption program for emails.
  - *Pidgin*: Secure instant messaging software.
- 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, for example, Firefox.

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 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.

Many computer users often are unaware of the existence of services running on a computer, as services run in the background and may not belong to a user. For example, discovering registered drivers may give investigators information about the peripheral devices associated with a suspect’s computer. [210] While at a crime scene conducting live forensic examinations, it may be possible, for instance, to see an installed driver for a digital camera. 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 leaving the scene, thereby securing valuable evidence.

Seizing mobile devices

Mobile devices can provide potentially crucial evidence and intelligence. Data found in phones can place a suspect in the vicinity of a crime, show who their associates are and show how the suspect operates. Where possible, upon seizing a mobile phone, record phone numbers and SIM cards used with the phone as well as the IMEI number.

[210] A driver is a program that controls a device. Every device, whether it be a printer, hard drive or keyboard, must have a driver program. Many drivers, such as the keyboard driver, come with the operating system. For other devices, one must install a new driver upon connecting the device to your computer.

IMEI number (International Mobile Station Equipment Identity)	Unique to each phone and can identify: • If a reported stolen phone is on a network • What SIM cards have been used in the handset The number is normally printed on the inside of the battery compartment or on the case. If you cannot, or decide not to open the phone, the IMEI number will be displayed on the phone screen when *#06# is dialled.
SIM card (Subscriber Identity Module)	Phone numbers are attached to the SIM card and a unique serial number, known as the Integrated Circuit Card Identifier (ICCID). The SIM has two passwords: one for the user and one for the provider (PUK code)

In relation to mobile devices, cloud-based systems can provide forensic investigators with access to text messages and pictures taken from a particular device, retaining an average of 1,000-1,500 (or even more) of the last text messages sent to and received from that phone. Investigators can also determine the past locations of the phone, and when the phone was at those locations.

Smartphones often tag pictures with Global Positioning System (GPS) coordinates (known as a GeoTag), which enables identification of where a picture was taken by looking inside its Exchangeable Image File Format (EXIF) data.[211]

Note: This information is deleted from photographs uploaded to Facebook, but may be preserved on other sites, such as Twitter and Photobucket. 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).[212]

[211] 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 cameras. See https://en.wikipedia.org/wiki/Exchangeable_image_file_format.

[212] Accessible at www.hamstermap.com.

If a mobile device is switched OFF

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

If a mobile device is switched ON

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

The device should be placed in "Airplane" mode in order to disable Wi-Fi, Bluetooth or other communication systems.

If the mobile device is switched ON (BUT LOCKED)

Plugging it into a power source will (in most cases) force the device to synchronize with any "cloud" services running. This should maximize the amount of evidence potentially available in the "cloud". However, capturing this evidence may pose some major challenges, as the target machine(s) may be sited outside of the concerned State's jurisdiction. Or, data could be easily changed or deleted remotely by someone with access to the "cloud" account.

In such cases, retrieval of the available evidence has a time-critical element and investigators may resort to time- and date-stamped screen captures of the relevant material, or to obtaining a digital extraction of the entire contents of the device using forensic tools.

⚠ **Remember**

Opening or using the mobile phone may automatically alter the evidence.

3.4 Online evidence and intelligence

The Internet provides a vast range of information sources and is a vital tool for information collection and intelligence development. Sources can include:

- News websites or blogs
- Official databases with public access (such as company registrations)
- Hotel and guest house websites, including online booking companies
- Commercial databases, airline route guides, telephone directories, etc.

Carrying out investigations online may involve specialist techniques ranging from exploiting information freely available on the Internet (usually referred to as open sources) to fully authorized undercover operations:

- *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.
- *Undercover law enforcement operations*: authorized covert activities by specially trained law enforcement officers. This type of Internet investigation is governed by domestic legislation and therefore differs among jurisdictions.
- *Open source intelligence gathering (OSINT):* this includes general research on the Internet, accessing information that is available to anyone without the need for a surveillance authority, a subpoena or warrant.
- *Social media intelligence gathering (SOCMINT):* research and analysis carried out on information derived from social media platforms where content is available for public access, such as Facebook, Twitter or LinkedIn.

Open source intelligence

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, thus benefitting 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. Effectively this means that the investigator's computer can be made to appear as if it is located somewhere other than its actual location; the IP address will not be associated with an official government server.
- *Pay-as-you-go SIMs:* use of a cell 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 that 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 that 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".[213] 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 and, as such, is commonly used for criminal activity on the Dark Web.

When carrying out open source research, investigators should utilize anonymous systems and 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, each time that a connection is made.

[213] "Privacy for People Who Don't Show Their Navels", *New York Times* (25 January 2008). At www.nytimes.com/2006/01/25/technology/techspecial2/privacy-for-people-who-dont-show-their-navels.html.

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

Throughout this phase, and as an investigation moves to the next stage (by concentrating research towards proving specific criminal acts), records should be kept of the process and progress of the research. These records form the foundation of the online evidence chain.

One of the first phases of an investigation in identifying the person(s) responsible for online criminal activity is to trace and follow Internet Protocol (IP) addresses. As stated previously, IP addresses provide the basis for online communication. Tracing IP addresses and domains is a key part of any Internet investigation; there are many resources available on the Internet to assist with this process. Firstly, there are the entities responsible for the addressing system itself, the Internet Assigned Number Authority, where searches can be carried out by region through the Regional Internet Registries.[214] Each site has a "Who Is" function that allows investigators to identify IP registration information.[215] The registration information refers to the Registrant, the person or entity paying for the service. In order to access for instance, payment information or IP logs, investigators would need to contact the Registrar, again in accordance with their respective domestic guidelines, procedures and legislation. Once an IP address has been traced, the investigator will be able to request data from an ISP in order to determine who is actually behind the device to which with IP address refers. Such requests are usually in the form of a subpoena or warrant to the local judge, depending upon domestic legislation and procedures.

Other online tools for tracing and investigating IP addresses include Network Tools[216] and Robtex.[217]

Encryption

ISIL members and other terrorist groups 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 had released a manual for its fighters, entitled "How to Tweet Safely Without Giving out Your Location to NSA", which purports to explain how to avoid surveillance.[218]

Besides propaganda purposes, these applications mainly serve to facilitate secure communications, making it increasingly difficult for authorities to monitor and disrupt terrorist-related activities. Alongside these bespoke applications, there are also many proprietary software options and online techniques available to terrorists to facilitate the security of their data and activities. Studies have

[214] Available at www.iana.org/.

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

[216] Accessible at http://network-tools.com/.

[217] Accessible at www.robtex.com/.

[218] (12 May 2016). "The ISIS has released a manual for its militants", *Security Affairs Blog* (3 November 2014). At https://securityaffairs.co/wordpress/29801/intelligence/isis-twitter-use-manual.html.

In addition to some of the software listed above, other examples of how technologically competent terrorists have become include a number of applications developed by terrorists themselves, such as:

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

[a] "Terrorist Group Al-Qaeda Uses New Encryption Softwares After NSA Revelations", *The Hacker News* (24 May 2014). At https://thehackernews.com/2014/05/al-qaeda-encryption-tool.html.

[b] "Dark Motives Online: An Analysis of Overlapping Technologies Used by Cybercriminals and Terrorist Organizations", *Trend Micro* (3 May 2016). At http://www.trendmicro.com.hk/vinfo/hk/security/news/cybercrime-and-digital-threats/overlapping-technologies-cybercriminals-and-terrorist-organizations .

indicated communications through "normal" channels using secret encoding techniques such as steganography and hidden watermarking remain an option.[219] These techniques, when employed with encryption, create serious challenges for intelligence, law enforcement and prosecution services.

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

Social media as an intelligence resource

Social media is now ubiquitous. People live their lives online, giving away details of themselves voluntarily. The rise in the use of social media provides opportunities for law enforcement to generate operational intelligence. Although terrorists are known to use encrypted communications, there are many who may be registered on websites such as Facebook, Twitter, WeChat and LinkedIn, while not enabling high privacy settings, meaning that their personal details, posts and photographs may be openly available.

[219] Steganography is the practice of hiding data within data—for instance, hiding a text file within an image. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data. Hidden watermarking is typically used to identify ownership of copyrighted material. Digital watermarks may be used to verify the authenticity or integrity of material, or show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication.

Therefore, online investigation skills are an essential part of the investigator's tool box in developing an intelligence picture that could:

- Assist in identifying criminal activity, for example, through cross referencing of individuals' accounts, the identification of accomplices, uncovering assumed identities, etc.
- Provide intelligence about individuals or groups
- Inform proactive investigations

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 worldwide web (for instance, "closed forums" that are password protected and moderated by nominated users and would, more than likely, require surveillance authorities or warrants prior to an investigation). The veracity of the intelligence should be treated with care and, in practice, corroboration of OSINT is always desirable before executive action is considered.

There are numerous programs available (commercial and freeware) that can assist in analysing mass data. Many of these programs provide a visualization of a network of connections and can assist in identifying key individuals in that network, such as those who 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 called Maltego.[220]

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

- *Intel Techniques:* a commercial OSINT training portal that offers (free of charge) a list of online Internet search tools.[221]
- *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.[222]

Many users of social media, especially FTFs, create an alias to use as their username for social media sites, and often this alias will be the same 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. For example, using the Twitter advance search function to search for a username (or alias) can show a person's real name that is associated with the searched for username. SocialMention[223] and CheckUserNames[224] are also useful tools for finding other sites where usernames appear.

[220] Accessible at www.paterva.com/web7/.
[221] Accessible at https://inteltechniques.com/intel/menu.html.
[222] Accessible at https://netbootcamp.org/.
[223] Accessible at www.socialmention.com/#.
[224] Accessible at http://checkusernames.com/.

Example, CheckUserNames

Designed to check the availability of a username, the site is useful for investigators in discovering where a username is already in use in order to target research for a subject. A search for the username "mickeymouse" will show where that user name has been used on a number of social networking sites.

Google Advanced Search

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

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

Finding people who visit certain websites can be difficult. Many sites (especially blogs) do not have a built-in "user search" function that shows all pages where the subject has left a comment or created a profile for example.

It is, however, possible to perform the following search in Google, which will show all comments made by an individual on whatever website is searched for:

> site: [domain.com] ["John Doe"] says: (replacing the domain.com and John Doe with name of the site and subject's name/nickname).
> : For example, site: twitter.com "[suspect's name, username or alias]" says:

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

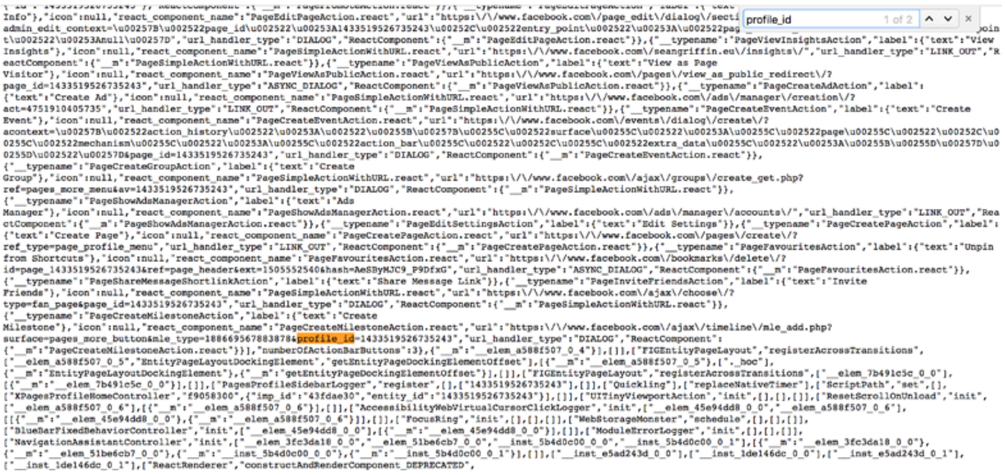
Facebook

After registering to use Facebook, users can create a user profile, add other users as "friends", exchange messages, post status updates and photos, share videos, use various apps and receive notifications when others update their profiles. Additionally, users may join common-interest user groups organized by their workplace, school or other characteristics, and categorize their friends into lists such as "People From Work" or "Close Friends". Facebook is the most popular social networking site in several English-speaking countries, including Canada, the United Kingdom and the United States. In regional Internet markets, Facebook penetration is reported to be highest in North America, followed by the Middle East-Africa, Latin America, Europe and Asia-Pacific.

Facebook can look up telephone numbers. Enter a phone number into Facebook's search box to find the account associated with a phone number. Alternatively, search for a person's profile by entering email addresses into the search box. Other basic searches are also possible in Facebook. While the website previously allowed users to conduct multiple-term searches using the "Graph Search" functionality, this has since been scaled down. Third-party websites such as *searchapp* (www.searchapp.io) can replicate some Graph Search features. For example, the website can conduct a Facebook search for men, named John, living in New York, who have visited London.

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

Figure 1. Searching Facebook source code for unique ID numbers



```
Info"},"icon":null,"react_component_name":"PageEditPageAction.react","url":"https:\/\/www.facebook.com\/page_edit\/dialog\/secti
admin_edit_context=\u00257B\u002522page_id\u002522\u00253A1433519526735243\u00252C\u002522entry_point\u002522\u00253A\u002522pag   poin
t\u002522\u00253Anull\u00257D","url_handler_type":"DIALOG","ReactComponent":{"__m":"PageEditPageAction.react"}},{"__typename":"PageViewInsightsAction","label":{"text":"View
Insights"},"icon":null,"react_component_name":"PageSimpleActionWithURL.react","url":"https:\/\/www.facebook.com\/seangriffin.eu\/insights\/","url_handler_type":"LINK_OUT","R
eactComponent":{"__m":"PageSimpleActionWithURL.react"}},{"__typename":"PageViewAsPublicAction","label":{"text":"View as Page
Visitor"},"icon":null,"react_component_name":"PageViewAsPublicAction.react","url":"https:\/\/www.facebook.com\/pages\/view_as_public_redirect\/?
page_id=1433519526735243","url_handler_type":"ASYNC_DIALOG","ReactComponent":{"__m":"PageViewAsPublicAction.react"}},{"__typename":"PageCreateAdAction","label":
{"text":"Create Ad"},"icon":null,"react_component_name":"PageSimpleActionWithURL.react","url":"https:\/\/www.facebook.com\/ads\/manager\/creation\/?
act=4751910405735","url_handler_type":"LINK_OUT","ReactComponent":{"__m":"PageSimpleActionWithURL.react"}},{"__typename":"PageCreateEventAction","label":{"text":"Create
Event"},"icon":null,"react_component_name":"PageCreateEventAction.react","url":"https:\/\/www.facebook.com\/events\/dialog\/create\/?
acontext=\u00257B\u002522action_history\u002522\u00253A\u002522\u00255B\u00257B\u00255C\u002522surface\u00255C\u002522\u00253A\u00255C\u002522page\u00255C\u002522\u00252C\u0
0255C\u002522mechanism\u00255C\u002522\u00253A\u00255C\u002522action_bar\u00255C\u002522\u00252C\u00255C\u002522extra_data\u00255C\u002522\u00253A\u00255B\u00255D\u00257D\u0
0255D\u002522\u00257D&page_id=1433519526735243","url_handler_type":"DIALOG","ReactComponent":{"__m":"PageCreateEventAction.react"}},
{"__typename":"PageCreateGroupAction","label":{"text":"Create
Group"},"icon":null,"react_component_name":"PageSimpleActionWithURL.react","url":"https:\/\/www.facebook.com\/ajax\/groups\/create_get.php?
ref=pages_more_menu&av=1433519526735243","url_handler_type":"DIALOG","ReactComponent":{"__m":"PageSimpleActionWithURL.react"}},
{"__typename":"PageShowAdsManagerAction","label":{"text":"Ads
Manager"},"icon":null,"react_component_name":"PageShowAdsManagerAction.react","url":"https:\/\/www.facebook.com\/ads\/manager\/accounts\/","url_handler_type":"LINK_OUT","Rea
ctComponent":{"__m":"PageShowAdsManagerAction.react"}},{"__typename":"PageEditSettingsAction","label":{"text":"Edit Settings"}},{"__typename":"PageCreatePageAction","label":
{"text":"Create Page"},"icon":null,"react_component_name":"PageCreatePageAction.react","url":"https:\/\/www.facebook.com\/pages\/create\/?
ref_type=page_profile_menu","url_handler_type":"LINK_OUT","ReactComponent":{"__m":"PageCreatePageAction.react"}},{"__typename":"PageFavouritesAction","label":{"text":"Unpin
from Shortcuts"},"icon":null,"react_component_name":"PageFavouritesAction.react","url":"https:\/\/www.facebook.com\/bookmarks\/delete\/?
id=page_1433519526735243&ref=page_header&ext=1505552540&hash=AeSByMJC9_P9DfxG","url_handler_type":"ASYNC_DIALOG","ReactComponent":{"__m":"PageFavouritesAction.react"}},
{"__typename":"PageShareMessageShortlinkAction","label":{"text":"Share Message Link"}},{"__typename":"PageInviteFriendsAction","label":{"text":"Invite
Friends"},"icon":null,"react_component_name":"PageSimpleActionWithURL.react","url":"https:\/\/www.facebook.com\/ajax\/choose\/?
type=fan_page&page_id=1433519526735243","url_handler_type":"DIALOG","ReactComponent":{"__m":"PageSimpleActionWithURL.react"}},
{"__typename":"PageCreateMilestoneAction","label":{"text":"Create
Milestone"},"icon":null,"react_component_name":"PageCreateMilestoneAction.react","url":"https:\/\/www.facebook.com\/ajax\/timeline\/mle_add.php?
surface=pages_more_button&mle_type=188669567883878&profile_id=1433519526735243","url_handler_type":"DIALOG","ReactComponent":
{"__m":"PageCreateMilestoneAction.react"}}],"numberOfActionBarButtons":3},{"__m":"__elem_a588f507_0_4"}],[]],["FIGEntityPageLayout","registerAcrossTransitions",
["__elem_a588f507_0_5","EntityPageLayoutDockingElement","getEntityPageDockingElementOffset"],[{"__m":"__elem_a588f507_0_5"},["._hoc"],
{"__m":"EntityPageLayoutDockingElement"},{"__m":"getEntityPageDockingElementOffset"}],[]],["FIGEntityPageLayout","registerAcrossTransitions",["__elem_7b491c5c_0_0"],
[{"__m":"__elem_7b491c5c_0_0"}],[]],["PagesProfileSidebarLogger","register",[],["1433519526735243"],[]],["Quickling"],["replaceNativeTimer"],["ScriptPath","set",[],
["XPagesProfileHomeController","f9058300",{"imp_id":"43fdae30","entity_id":"1433519526735243"}],[]],["UITinyViewportAction","init",[],[],[]],["ResetScrollOnUnload","init",
["__elem_a588f507_0_6"],[{"__m":"__elem_a588f507_0_6"}],[]],["AccessibilityWebVirtualCursorClickLogger","init",["__elem_45e94dd8_0_0","__elem_a588f507_0_6"],
[[{"__m":"__elem_45e94dd8_0_0"},{"__m":"__elem_a588f507_0_6"}]],[]],["FocusRing","init",[],[],[]],["WebStorageMonster","schedule",[],[],[]],
["BlueBarFixedBehaviorController","init",["__elem_45e94dd8_0_0"],[{"__m":"__elem_45e94dd8_0_0"}],[]],["ModuleErrorLogger","init",[],[],[]],
["NavigationAssistantController","init",["__elem_3fc3da18_0_0","__elem_51be6cb7_0_0","__inst_5b4d0c00_0_0","__inst_5b4d0c00_0_1"],[{"__m":"__elem_3fc3da18_0_0"},
{"__m":"__elem_51be6cb7_0_0"},{"__m":"__inst_5b4d0c00_0_0"},{"__m":"__inst_5b4d0c00_0_1"}],[]],["__inst_e5ad243d_0_0"],["__inst_1de146dc_0_0"],["__inst_e5ad243d_0_1"],
["__inst_1de146dc_0_1"],["ReactRenderer","constructAndRenderComponent_DEPRECATED",
```

This text can be searched using the function of "Control F" (on the keyboard, hold the "Ctrl" key and press "F" to bring up a search tool). By searching for "profile_id" in the page code, the number shown immediately next to this code is a unique Facebook ID number. The same technique also works for subject pages on Facebook.

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

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

In the above example, the user can be found by entering the web address (in the computer browser window) "http://www.facebook.com/12345678910".

There are a number of Internet tools that establish where the pictures are posted. 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.

Two options appear below:

- *Tineye:* upload a saved image and follow on screen instructions[225]
- *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, for example, Twitter accounts, blogs and personal web sites[226]

Facebook can also be searched via Google, using the syntax “site:facebook.com”. Words that 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 contain INTERPOL in the title, and mention Sweden, the search term would read:

Sweden intitle: INTERPOL site:facebook.com

This technique also works with any other website by substituting the website address after the “site:” syntax.

Twitter

Twitter is an online social networking service that enables users to send and read short 140-character messages called “tweets”. Registered users can read and post tweets, while those who are not registered can only read them. Users access Twitter through the website interface, SMS or mobile device app. As of May 2015, Twitter has more than 500 million users, of whom more than 332 million are active.

Users can group posts together by topic or type by using hashtags—words or phrases prefixed with a # sign. Similarly, the @ sign followed by a username is used for mentioning or replying to other users. To repost a message from another Twitter user and share it with one’s own followers, a user can click the retweet button within the Tweet. 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” mode, which limits this information (and all tweets) to approved followers. Twitter collects personal information about its users and shares it with third parties as specified in its privacy policy.

At its height, it was reported that ISIL was operating approximately 46,000 Twitter accounts, going to show that social media can represent a powerful instrument in terrorist propaganda.[227]

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). Using Twitter’s “Advanced Search” page, one can perform a more detailed search using the operators below.

[225] Accessible at www.tineye.com.

[226] Accessible at https://images.google.com/.

[227] “The Foreign Fighters Phenomenon in the European Union”, International Centre for Counter-Terrorism (April 2016). At https://www.icct.nl/wp-content/uploads/2016/03/ICCT-Report_Foreign-Fighters-Phenomenon-in-the-EU_1-April-2016_including-AnnexesLinks.pdf.

Twitter advanced search operators

- *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 the New York City.
- *Search for tweets with links:* if only tweets that contain links are required, add "filter:links" to your search phrase.
- *Search for tweets from a certain user:* if a keyword search for data from one particular person is required, type "from:[username]" to search within his or her stream.
- *Search up to/from a date:* it is possible to search Twitter for content up to and after certain dates. Typing "since:2012-09-20" will show tweets sent since Sept 20, 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.

Other (free to use) online tools include:

- *Geosocial footprint:* a geosocial footprint is the combined bits of location information that a user divulges through social media, which ultimately forms the user's location or footprint (http://geosocialfootprint.com/).
- *Tweetpaths:* when the name of a user on Twitter is known, searching for that name on tools such as this will display results on a map, showing the location from where that user's tweets were posted (www.tweetpaths.com).
- *Twazzup:* provides real-time monitoring and analytics for Twitter (www.twazzup.com).

Tools for downloading and analysing Twitter data:

- *BirdSong Analytics:* BirdSong Analytics is a useful tool that facilitates the download of all followers of any Twitter account. This is a commercial tool that requires purchasing. The export comes in the form of an Excel spreadsheet, allowing the user to take advantage of Excel's sorting, filtering and searching options: for example, you can download all people who follow your suspect and investigate their habits, or you can download and research all accounts that@[your_suspect] is following.
- *NodeXL:* a simple, but very thorough tool. It is an open source template for Microsoft Excel that works by integrating data pulled from a CSV (Comma Separated Value) file into an informative network graph in order to, for instance, create a visual representation of your tweets from any period you choose.

A recent 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 is reported to have been very active on Twitter, posting about 10,000 tweets and having 3,000 accounts listed as "followers".

Social network analysis

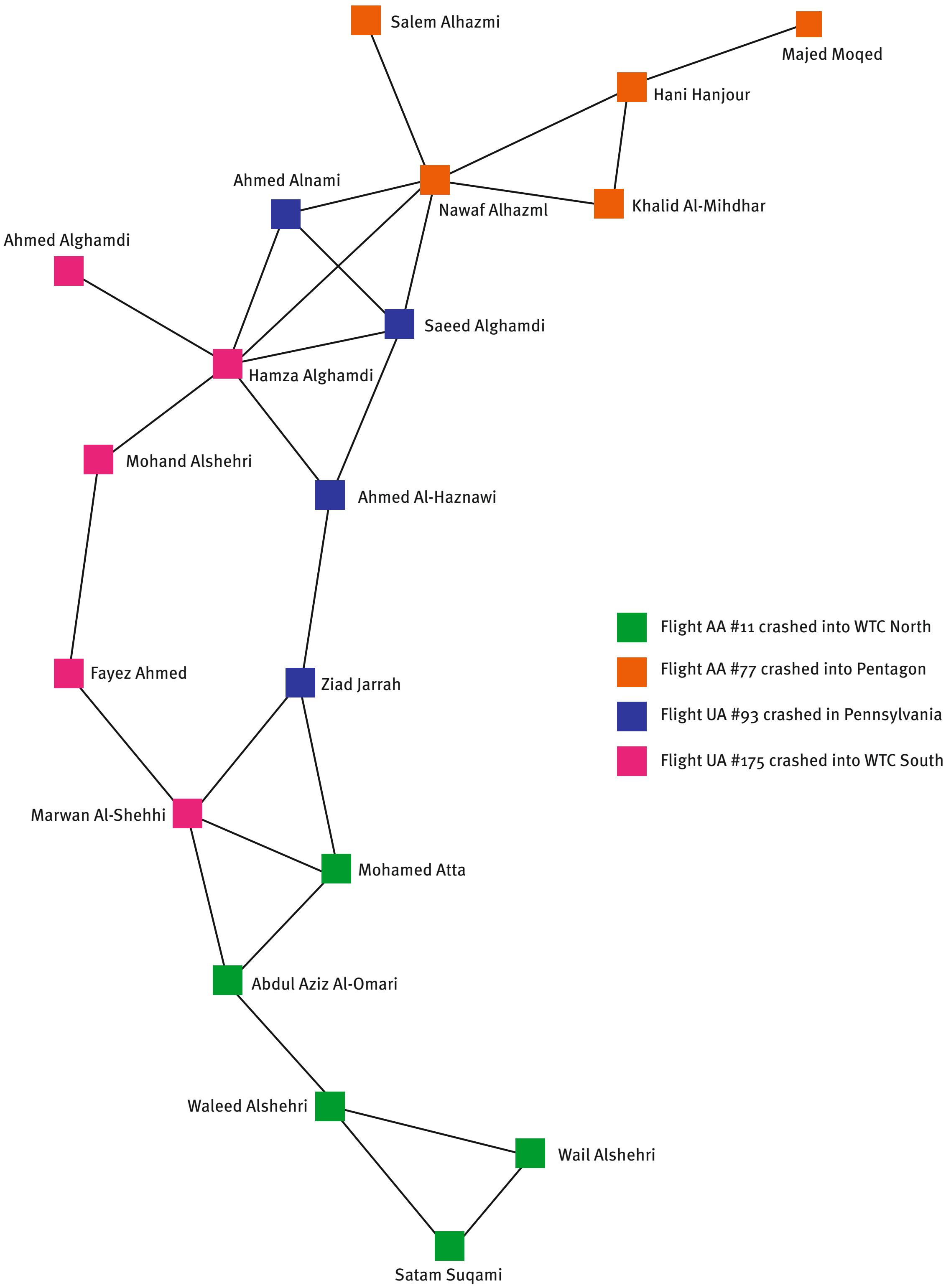
Alongside the analytical tools already discussed, there is also the possibility of using this mass data to map a social network (social network analysis or SNA). SNA provides a visualization of a network and, through a series of algorithms, works out a particular person's place in his or her network. The analysis generates a "Centrality Measure", indicating how "Central" to the group a person is in terms of influence, access, direct contact and as a go-between. An example of a centrality measure is "Betweenness", which measures how likely a person is to be the most direct route between two people in the network. In more concrete terms, "Betweenness" may indicate the person in a network through whom a large amount of information is likely to flow.

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

An excellent example of the power of social network analysis can be found in a paper by Dr Valdis Krebs, who produced an analysis of the 9/11 hijack teams purely from open source information (mainly news articles, as this article was written pre-Twitter and Facebook). Krebs' results come remarkably close to the actual position within the network for each of the hijackers.[228]

[228] Valdis Krebs, "Uncloaking Terrorist Networks", First Monday (April 2002). At http://firstmonday.org/ojs/index.php/fm/article/view/941/863&quot%3B&gt%3BNetwork.

Figure 2. Social network analysis of 9/11 hijack teams



Chapter 4

Preventing and countering violent extremism

4.1 Introduction

This chapter discusses holistic approaches to preventing and countering violent extremism (PVE/CVE), and promoting long-term cooperative participation of the whole of society and the whole of government. The chapter dedicates particular attention to strategies applicable to the phenomenon of FTFs, which can also be generalized to fashion comprehensive national or regional PVE/CVE programmes.

Estimates of the total numbers of individuals that have travelled to the region to fight with ISIL and other groups vary between 27,000 and 40,000. While many have been killed or captured, those that manage to leave the region to return home or travel to countries other than their own pose a unique threat to security. Predicting the scale of such a threat can be extremely challenging, as the motivation of "returnees" is often not known. However, as attacks during 2017 in Western Europe have demonstrated, there are well trained individuals with battle experience who are intent on committing terrorist acts once they leave the conflict zones.

Although research has shown that numbers of travellers to the Syrian Arab Republic and Iraq from South and South-East Asia have been low compared to other regions,[229] the freedom of movement between islands and the appearance of ISIL-linked groups in the region (such as the Philippines) creates a more significant threat. Furthermore, small islands, atolls and archipelagos may have incredibly small communities, and the impact of individuals returning to these communities has the potential to be significantly greater than elsewhere.

National counter-terrorism strategies, with specific emphasis on PVE/CVE, can mitigate this potential threat.

As a preliminary matter, the content of this chapter requires a working definition of violent extremism. Violent extremism is a term often used to describe part of the cycle of behaviour leading to acts of terrorism, but it is important to distinguish violent extremism from terrorism. Otherwise, efforts to counter violent extremism will merely focus on preventing physical acts of terror as opposed to combating the ideologies that drive individuals to commit such acts.[230]

[229] Richard Barrett, "Beyond the Caliphate", The Soufan Center (October 2017). At http://thesoufancenter.org/research/beyond-caliphate/.

[230] See Jason-Leigh Striegher, "Violent-extremism: An examination of a definitional dilemma" (2015). At http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1046&context=asi.

Working definition

Violent extremism is:
"an ideology that accepts the use of violence for the pursuit of goals that are generally social, racial, religious and/or political in nature."

Source: See Jason-Leigh Striegher, "Violent-extremism: An examination of a definitional dilemma" (2015). At http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1046&context=asi.

Member States have the prerogative to define "terrorism" and "violent extremism" within their national legal systems, consistent with their obligations under international law, particularly international human rights law.[231]

4.2 Strategies to counter violent extremism leading to terrorism

Inter-government coordination

A coherent strategy for PVE/CVE should seek to address all forms of violent extremism and terrorism, and recognize that the threat posed will not be solved purely through responsive methods. A "whole-of-society" and "whole-of-government" approach is required to proactively address and negate conditions conducive for violent extremism. As such, a variety of stakeholders (government and non-government) should be involved in working towards reducing this threat. Ministries and departments across government will be involved in delivering the strategy, and it is therefore essential that Member States should consider how to effectively coordinate and deliver that strategy, first and foremost, at the local level.

In March 2010, the United Kingdom House of Commons Communities and Local Governments Committee published a report outlining the vital role that local authorities have in promoting safer, stronger communities and promoting "shared values" at a local level.[232] The report goes on to state that cohesive work that is directly aimed at preventing extremism should encompass all types of extremism, from that inspired by Al-Qaeda, to extremism associated with the far-right.

Creating a localized threat picture

Managing the risks associated with returning FTFs requires developing a comprehensive understanding of the localized threat picture. Also, decisions on managing the conditions in which extremism can develop need to be made at the local level, based upon local risk assessments. In doing this, not only can local areas be assessed to inform national priorities, but also the number of local returnees and the areas to which they are returning can be determined. This, in turn, informs analysis of travel patterns and hotspots and allows effective resource allocation and multi-agency support (and also ensures that returnees are not situated in close proximity).

[231] See United Nations, "Plan of Action to Prevent Violent Extremism" (24 December 1015). At http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/674.

[232] See United Kingdom House of Commons Communities and Local Government Committee, "Preventing Violent Extremism", Sixth Report of Session 2009-10, para. 168 (March 2010). At https://publications.parliament.uk/pa/cm200910/cmselect/cmcomloc/65/65.pdf.

Try it for yourself:

- If there are no localized threat analyses in place, consider creating one.
- If one exists, perhaps look at creating a threat analysis of a particular threat or problem (such as large numbers of fighters returning).

Techniques to consider:

- 5 Ws and H questions: (Who, what, why, where, when and how) for the threat and for the resultant mitigating responses
- Information sources on the threat
- Identify stakeholders
- Horizon scanning techniques—imagine the effect on the following conditions:
  - Political
  - Economic
  - Social
  - Technological
  - Legal
  - Environmental

Further reading: United Kingdom Government, "Futures toolkit for policy-makers and analysts" (8 July 2014). At https://www.gov.uk/government/publications/futures-toolkit-for-policy-makers-and-analysts.

Create a new post or build on an existing role?

In order to coordinate the response to returning FTFs and ensure effective management and direction of a PVE/CVE strategy, a government can either create one or more official posts, or adjust the responsibilities of a pre-existing role. Consideration should be given to the following factors:

- *Resources*: where will the budget for new personnel come from, and likewise, where will these new staff be based?
- *Seniority*: the standing of the new position, for example in grade of post, in order to command respect and ensure cooperation.
- *Autonomy*: it is good practice that the person(s) appointed are able to set strategies and hold their own budget (particularly true at the local level).
- *Regional cooperation*: how will cooperation be implemented at the provincial levels?

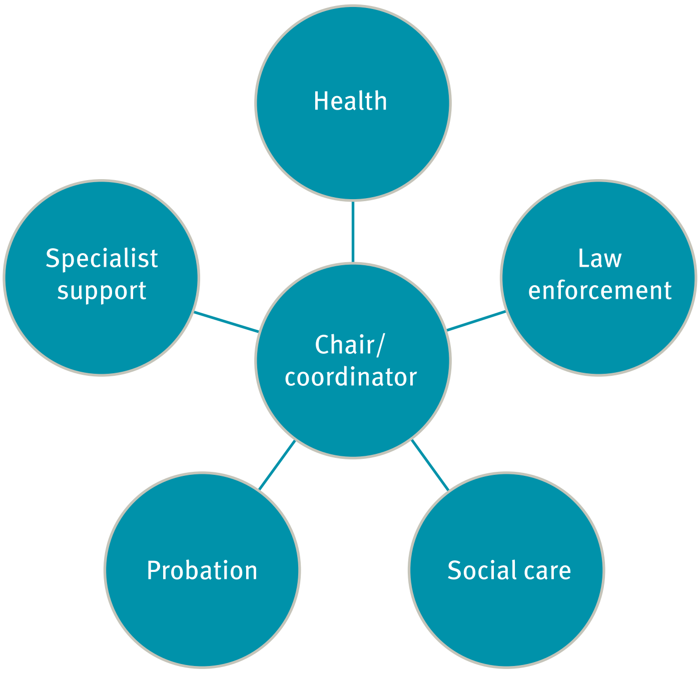
Working groups

It is important to ensure reflective and responsive feedback is gained from all stakeholders, from grassroots (such as community members) to the executive and ministerial level. With that in mind, many States have developed working or steering groups to ensure coordination and feedback from the various stakeholders, such as:

- Executive or decision makers
- Regional working groups

- Specific working groups (for example determining actions for individuals "at risk" such as the United Kingdom Channel panel)
- Ad-hoc or specific problem working groups (for instance returning families from the Syrian Arab Republic and Iraq)

Figure 3. Example of working group roles at the local level



Considerations on forming working groups

- Try to use pre-existing structures if possible (don't create new structures just for the sake of it).
- Consider the amount of time that those involved will need to dedicate to a working group. Are those involved able to give up this time on a regular basis?
- Wherever possible, always meet in person, but also have the ability to update "virtually" if necessary.
- Have clearly defined roles, and ensure those assigned specific roles (such as Chair) are of significant enough standing to be respected and listened to.
- Try to avoid duplication (i.e. local working group, regional working group, police working group, policy owner working group, all doing the same thing).
- Consider the size of the working group. This should be as small as possible, particularly if the group is tasked with discussing actual cases (e.g. how to manage the risk of a returning family to the local community). Ways to manage this can include having a smaller core group that attend every meeting, and then adding specific relevant experts (such as mental health workers, theological mentors) for individual cases.
- Ensure proper information security of all meetings and cases discussed, and have participants sign and adhere to confidentiality agreements.

Rehabilitation, reintegration, deradicalization

Many nations have enacted new legislation in response to resolution 2178 aimed at criminalizing terrorist activities relating to FTF. However, for those individuals who fall outside the legislative framework, programmes need to be in place to deal with issues relating to rehabilitation, reintegration and deradicalization in order to mitigate potential risks associated with their experience.

Elements of such programmes, include (but are not limited to):

- *Psychological support and counselling:* including professional psychological support and counselling services such as regular sessions of cognitive behavioural therapy (or similar).

Practical example

A young boy who is autistic was discovered watching ISIL beheading videos in school. Part of his support package included regular sessions with a mental health professional who helped him understand the context of the videos and the wrongfulness of the portrayed violence.

- *Housing support:* including access to social housing, assistance in relocating or help setting up on one's own.

Practical example

A young girl travelled to the Syrian Arab Republic as part of a larger family. Once there, she reached out to friends saying she wanted to escape but her older brother and cousin (whom she had married in the Syrian Arab Republic) were preventing her. When both brother and husband were killed, she managed to use money to bribe her way across the border and, after being detained by the Turkish authorities, she was deported to her country of origin. Upon her return, she did not wish to live in the same area as before, due to fear of reprisals from family and friends. Therefore, cooperation between housing services from different local authorities allowed her to access social housing in another province.

- *Access to training/vocational courses to enhance job prospects:* this may include providing training courses and paying for vocational qualifications, such as plumbing or electrician qualifications.

Practical example

A community organization's project gave youth from a disadvantaged area the opportunity to undertake a free 12-week course. The course brought together young people who in normal circumstances would never mix and developed soft skills such as communication and anger management. It also gave the young people the opportunity to train and obtain qualifications in IT and cybersecurity, raising their job prospects.

- *Theological support:* religious-based extremism is often exacerbated through obtaining information on religious texts from a single source without access to individuals in a position to challenge incorrect perceptions. People well versed in a particular religion, and in particular those who resonate with the target audience, can provide information and guidance in theological matters.

Practical example:

A young male began embracing a religious interpretation promoted by Internet preachers who were delivering messages similar to those used by extremist groups. A highly-educated and religious scholar was able to convince the young male of less radical interpretations, providing effective counter-arguments to the words of the Internet preachers.

- *Mentoring:* this can include older peers acting as support for young people who may be on the path to becoming radicalized. Mentors can act as friends to young people, give a personal example for them to aspire to, or provide them with a familiar and safe dialogue partner.

Practical example:

A young man joined an extremist group as an 18-year-old. He proselytized on the streets, called for the removal of the democratic government. He and some close friends were later arrested and convicted of terrorism offences.

As one of a number of support measures, he has regular one-to-one meetings with another former extremist who has turned his life around. They have become close friends, and the similarity of their personal backgrounds has shown the young man that there is a pathway away from violence.

- *Family support and access to family members if separated:* families are essential to the process of reintegrating and helping individuals once again feel part of society. This support could include parenting advice and guidance from social care professionals, access to imprisoned individuals or support in reaching distant family members.

Practical example:

A girl who became radicalized via online contact with an ISIL recruiter was stopped at the Turkish border by the authorities and returned to her country of origin. Some of the "push" factors included abusive family members to whom she did not wish to return. She received assistance in finding accommodation elsewhere, with special arrangements enabling communication and in-person meetings with close family and friends; the arrangements were kept secret from the abusive family members.

It is important to recognize that there can be no "one-size-fits-all" approach to rehabilitation or support programmes. Each individual case must be assessed to determine:

- What level of threat do individual returnees pose? Considerations can include criminal histories; offences committed in the conflict zone; motivations for travel; reasons for return; nature and demeanour since entering the programme; psychological trauma; skills (such as prior military experience); and other case-specific facts, such as travelling with friends and family who are now deceased.
- What are their psychological needs? Returnees are likely to have suffered mental trauma that will have had some form of impact on their state of mind.
- What is the status of their social networks? Who are their local contacts who can act as a support network?
- Were they formally employed?
- What is their level of education? (for prospects/training)
- Do they have a home to which they can return?
- What are their general health needs? Do they have drug and alcohol abuse issues?

For further strategies as to the implementation of rehabilitation programmes, see the section 4.5 below.

4.3 Detained and convicted foreign terrorist fighters

Dealing with individuals in prisons can be one of the most challenging aspects of a PVE/CVE strategy. One important aspect is to determine whether to separate violent extremist offenders or mix them into the general population. It is important to appreciate that terrorists may be different from other types of offenders, in that they may actively look to proselytise and recruit while imprisoned. Risk factors of radicalization that exist outside a prison also exist within them, potentially magnified by the mere fact that individuals are incarcerated. For example, grievance narratives are more easily enhanced in prisons, and individuals may turn to violent extremist groups to cope with feelings of increased lack of purpose or sense of demonization. The issues around prisons should be considered in greater depth as a stand-alone issue; the authors direct readers to specialized guidance documents focused on prisons.[233]

As an introduction, there are a number of considerations to bear in mind when dealing with violent extremist offenders, and in particular returning FTFs:

- Theological support, such as through visiting imams or religious leaders. Consider whether the religious leader has experience in dealing with incarcerated populations; often, strong willed violent extremists have usurped religious leaders within prison to radicalize inmates. While imams may provide religious support, they should not be considered as a catch-all solution.
- Provision of vocational education courses.
- Support for transition back into society post-incarceration.
- Family visits, and in particular activities that emphasize the individual's position in the outside community.

[233] See for example, UNODC, *Handbook on the Management of Violent Extremist Prisoners and the Prevention of Radicalization to Violence in Prisons* (2016). At https://www.unodc.org/pdf/criminal_justice/Handbook_on_VEPs.pdf. OSCE, "Countering Violent Extremism and Radicalisation that Lead to Terrorism: Ideas, Recommendations, and Good Practices" (28 September 2017). At https://www.osce.org/chairmanship/346841?download=true.

Case study: family of foreign terrorist fighters scenario

Consider the following scenario:

A female national from your country was known to have travelled to the Syrian Arab Republic in 2014. Intelligence gained from her social media accounts and Internet footprint reveal that she married an ISIL fighter, but there is no evidence suggesting she has been directly involved in terrorist activities or fighting of any kind. Interviews with close family have cleared them of any involvement and the general view from them was of "shock and dismay" that an intelligent, well-intentioned and warm young woman with a bright future could take such a path.

Less than one year ago, the girl gave birth to the couple's first child, and she is currently three months pregnant with the second child. The husband posted pictures on an ISIL social media channel entitled "new cub of the caliphate" with their new born son next to an automatic weapon.

Recently it was confirmed that the woman's husband, and father of the two children had been killed in fighting near Raqqa.

The woman has since re-established contact with her family and has said that she wants to "come home" and that she was "trapped before" and that she "couldn't escape, was so scared but there was no way out". She stated that she saw women who had tried to escape being killed. She expressed that she is willing to talk to the authorities.

The questions below are provided as a guide to assist in designing and/or implementing PVE/CVE strategies and plans when considering the appropriate response to the above scenario:

- What is the status of the two children in terms of their nationality?
- What options are there for their return?
- If she returns, how will you know?
- Will this differ depending on her mode of transport?
- What will happen immediately when she arrives?
- Will the young children be taken into protective custody?
- What offences might the woman have committed?
- What resourcing or support will need to be put in place?
- Who needs to know immediately of her return? Who else must eventually know?

4.4 Civil society

Introduction

The increasing risks of radicalization and terrorist attacks in the regions of South Asia and South-East Asia, coupled with the issue of returnees from conflict zones in the Syrian Arab Republic and Iraq, underlines the need for States within these regions to adopt holistic local, regional and national strategies to effectively address the issues surrounding those risks and threats. In particular, civil society engagement is necessary to solve problems where criminal justice methods, alone, may be ineffective.

Once Member States have developed PVE/CVE strategies, they must be implemented. The implementation should be coordinated by an agency or department that has assumed leadership in the PVE/CVE domain. Implementation partners can include various government and non-government bodies. Key partners should include actors from civil society organizations (CSOs), capable of addressing the different needs of FTFs and their families, and bringing expertise to different PVE/CVE subjects. CSO participation may be essential in fields including health care, education, family assistance and community engagement.

Counter-narratives

A crucial element of any PVE/CVE strategy is the development an alternative to the narratives of extremist groups or organizations. The alternative narrative should seek to discredit and highlight weaknesses and inconsistencies in extremist propaganda and messaging, while keeping sight of the main target audience of such messaging: the youth of South and South-East Asia.

Current good practices in developing alternate narratives include:

- *Actively engaging with the private sector, civil society and local communities.* This exemplifies an open society in which the government interacts with its population and welcomes its participation in the design and implementation of social policies. The counter-narrative should be disseminated on a local level, through the use of networks of participating CSOs. This approach legitimizes the message; facilitates its spread throughout the population; demonstrates inclusive policymaking; supports the principles of freedom of expression and assembly; and creates a sense of belonging and loyalty within the community.
- *Strengthening the sense of national identity and of belonging to the community.* Counter-narratives can emphasize the importance of national or community identity, in contrast to religious identity, thereby increasing resilience against groups who use religion to promote violent extremism. One author has explained, for example, that the term "Indonesian Muslim" can heighten national cohesion more effectively than "Muslims in Indonesia".[234] The former term highlights national identity, while the latter term implies that the nation is merely a place where one is physically located.
- *The use of credible voices.* Victims and former radicals or terrorists who have walked away from violence can increase credibility and create empathy among young people. Victims' experiences would play a vital role as they would have the chance to show the dangers and real-life results of terrorism and how this has directly affected them, while gaining empathy and helping young people understand how much hurt terrorism can cause. This would, in turn, strengthen the moral principles that can prevent individuals turning to violence to achieve their aims. With regard to former terrorists, their experiences within this field would help to discredit the terrorist message, while at the same time adding credibility to the counter-narrative among the younger generation (which would not necessarily be the case if the source of the message was governmental). For example, the AIDA Foundation in Indonesia is developing a programme in which

[234] 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). At https://www.unodc.org/documents/southeastasiaandpacific/Publications/2016/Radicalisation_SEA_2016.pdf.

victims of terrorist attacks visit schools in order to share their experiences with the children and to explain the outcomes of an attack.[235]

- *Youth as generators of counter-narratives.* Today's youth are not only the recipients or intended audience for a PVE/CVE plan; youth should also be seen as generators of its content. Youth messages possess credibility that governmental experts generally cannot leverage themselves if they are unaware of trends and topics that appeal to young people. One example of youth participation in the field of PVE/CVE is The Asian Youth Council,[236] based in Malaysia. National PVE/CVE strategies should implement frameworks allowing youth groups and CSOs to flourish.
- *Enhancement of critical thinking.* Ultimately, the prevention of radicalization is a task of strengthening society against the impact of terrorist messaging. Youth education enhancing critical thinking will increase the ability to think independently and identify the flaws in exploitative propaganda.

One example of an initiative focused on empowering young people against radicalization is the project known as "Peer to Peer: Facebook Global Digital Challenge." The focus of this project is on collaboration with the private sector and large companies within the sector of social networking.

The project includes a university youth initiative and international competition calling on students to use the power of innovation to challenge prejudice, online hate and extremism.

Participants develop campaigns and social media strategies against extremism that are credible, authentic and believable to their peers and resonate within their communities.

The teams will research their target market and create a strategy designed to best reach and influence their peers. Each team receives a $2,000 (USD equivalency) operational budget plus $400 in Facebook ad credits to design, pilot, implement and measure the success of a social or digital initiative, product or tool that:

- Motivates or empowers students to become involved in countering violent extremism
- Catalyses other students to create their own initiatives, products or tools to counter violent extremism
- Builds a network or community of interest, focused on living shared values, that also counters violent extremism

More than 12 universities and institutes from Bangladesh, Indonesia, Malaysia, Maldives and the Philippines and have participated in this international programme. The Dhaka University project "Think Twice, Act Wise" was awarded first prize in 2016, and recorded over 10 million hits on Facebook in a two-month period.

Further information: https://edventurepartners.com/peer2peer/.

[235] Accessible at http://aida.or.id/8/publikasi.
[236] Accessible at https://www.facebook.com/AsianYouths.

Religious education

This interaction with education centres to reinforce a more moderate interpretation of Islam (as opposed to the extremist interpretation) is necessary and requires the involvement of other partners.

A good example of this interaction in a religious environment is the project launched by the MOVE Foundation in Bangladesh:[237] this is a deradicalization and civic education campaign for youths of different educational institutions and qawmi madrasas across the country. Its key components include:

- Cultural and educational intervention
- Dialogue
- Leadership
- Peace-building training

Community service by madrasas and social leaders

Through this programme, MOVE intends to create an informed and responsible young citizenry with the requisite skills needed to engage in collective action that engenders democratic governance, public accountability, political reconciliation, religious harmony and social transformation.

The Global Movement of Moderates is another important initiative. It focuses on delivering several projects linked to PVE/CVE across South-East Asia.[238]

Delegitimizing the caliphate

Counter-narratives can work to dilute the legitimacy of the caliphate, for example, by exposing the reality of life within it. Counter-narratives can spread factual information about corruption within ISIL leadership, hypocrisy regarding non-Islamic behaviours or miserable living conditions. Delivering these messages utilizing former terrorists who recount their experiences in the first person is an extremely useful measure that has already seen positive results in other parts of Asia.

An excellent example of this strategy is the documentary produced by the Institute for International Peace Building, in Jakarta, called "Jihad Selfie".[239]

Gender-based messaging

A PVE/CVE strategy should plan for and implement gender-based considerations in the development of counter-narratives. For example, narratives need to counter messages that make appeals for women to fulfil traditional gender duties (such as motherhood, or being a wife to "warriors" of the terrorist group). Counter-narratives may also need to demystify messages offering women the chance to experience new roles within society, such as nursing, dissemination of propaganda or recruitment efforts. Potential recruits may thus see involvement in a terrorist group as a method of personal "empowerment" or rebellion, or may believe that the terrorist group is capable of building a "new society" with fewer gender restrictions.

Counter-narratives to these recruitment messages should highlight the dangers of participation in the terrorist group, or the falsehoods of the recruitment message itself. More importantly, PVE/CVE strategies can also seek to directly promote gender equality within society, both for its own sake, and to decrease the attractive force of recruitment messages preying on gender grievances. To that end, local

[237] Accessible at http://move-foundation.com/our-programs/cap-program/.
[238] Accessible at http://www.gmomf.org/about-us/introduction-on-gmmf/.
[239] Accessible at https://prasasti.org/portfolio/film-production-and-screening-jihad-selfie/.

CSOs may study and possess crucial data regarding gender narratives, and may understand the grievances regarding gender inequality within the local community.

4.5 Involvement of society and communities

Benefits of the engagement of civil society organizations

There are many crucial reasons for including CSOs in the PVE/CVE plan:

- *Credibility.* Organizations promoting PVE/CVE messages and activities must be credible. In many instances, PVE/CVE programmes led by governmental agencies do not achieve the desired amount of credibility among the communities at whom they are directed—generally, young people who hold suspicion and even anger against the government. Therefore, it is necessary to rely on the collaboration of CSOs less likely to be rejected or generate suspicion.

  Credibility is essential for CSOs implementing "mentorship" deradicalization and disengagement programmes linked to FTFs and returnees, as successful communication between mentor and mentee relies on a high degree of trust. This trust will no doubt be much higher when the mentor is not associated with government authorities.

  It is highly recommended that the messengers or visible faces of these programmes are credible voices that generate confidence and empathy among the public at whom their messages are aimed. These messengers often require significant logistical support, assistance and training to craft narratives (what to say) and access the target audience (how, when and where to say it). Local civic organizations can provide this assistance more efficiently than regional or national government offices.

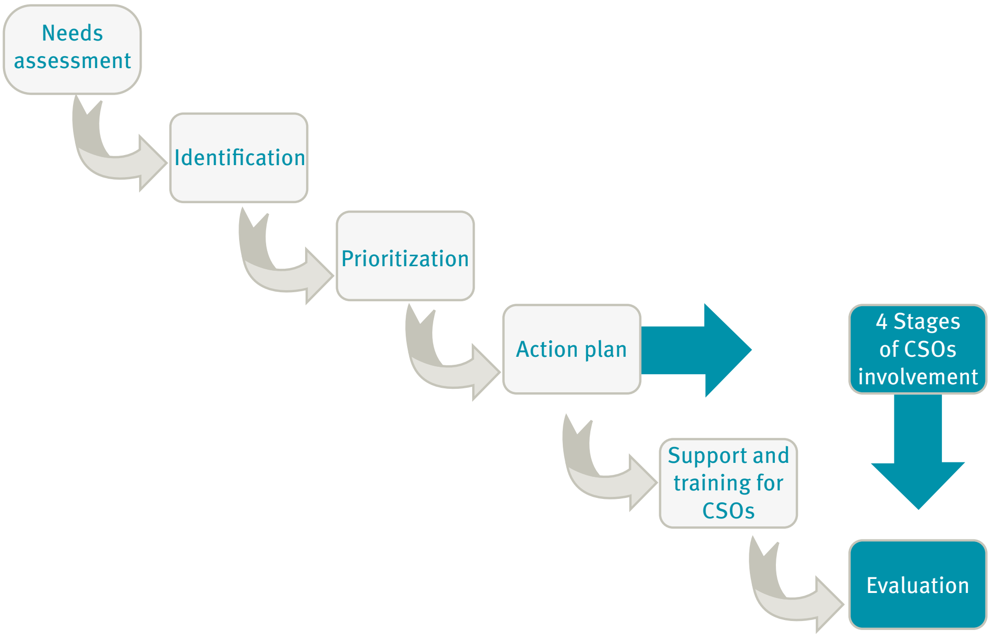
- *Access to CSO networks.* Collaboration with CSOs regarding PVE/CVE leads to the possibility of using their own networks, which will amplify the effectiveness and delivery of messages. Access to certain areas of the community may only be possible through cooperation with specific CSOs and their networks.
- *Access to marginalized groups.* Collaborating with CSOs in PVE/CVE planning facilitates access to a wide range of social groups and individuals who, beforehand, may have had difficulty in direct engagement with authorities without being rejected or ignored. CSOs thus facilitate access to larger audiences.
- *Knowledge of the vulnerable populations.* CSOs can articulate the needs of the local communities where they work. In terms of FTF and returnees' families, local CSOs can obtain information about individual needs, where a governmental authority may otherwise be rejected. This point is extremely important due to the role that families can play in the reintegration process and in building resilience among other relatives exposed to radicalization. The same logical approach should be borne in mind when dealing with children, where specialized teams with the requisite expertise will be essential.
- *Better management of risks to the community reputation of the PVE/CVE programme.* The planning process of implementing a PVE/CVE strategy includes identification of possible threats to the community reputation of the plan. CSOs are often better-placed within the community to identify and mitigate these threats. Thus, CSOs should also be included in the evaluation and monitoring process.
- *Legitimacy of PVE/CVE policies involving law enforcement.* As illustrated in previous points, CSO involvement can raise the credibility of governmental authorities. CSO collaboration with law

enforcement bodies focusing on counter-terrorism can build respect for lawful authority and increase the community's candour with law enforcement, enabling early detection of radicalization and more effective investigations. At the same time, specialized CSOs may work with law enforcement to motivate greater compliance with human rights standards in investigations and prosecutions.

Civil society organizations—community engagement: a methodology

In developing PVE/CVE plans where CSO engagement is desirable, planners can follow the checklist below. This section will explain each step of the process in detail.

Figure 4. Checklist of CSO involvement



Needs assessment. Prior to designing a plan or activity, a needs assessment should be undertaken in order to identify areas that would benefit from the support of, or collaboration with, CSOs. A few simple questions can provide information on specific areas where such collaboration may be beneficial.

Questions include:

- Is the requisite knowledge in place in relation to the section of the public being addressed? For example, understanding of young women from rural areas.
- Is there credibility to effectively reach the target audience and to build a strong bond with that audience?
- Are the necessary legal and logistical structures in place to assist in PVE/CVE implementation?

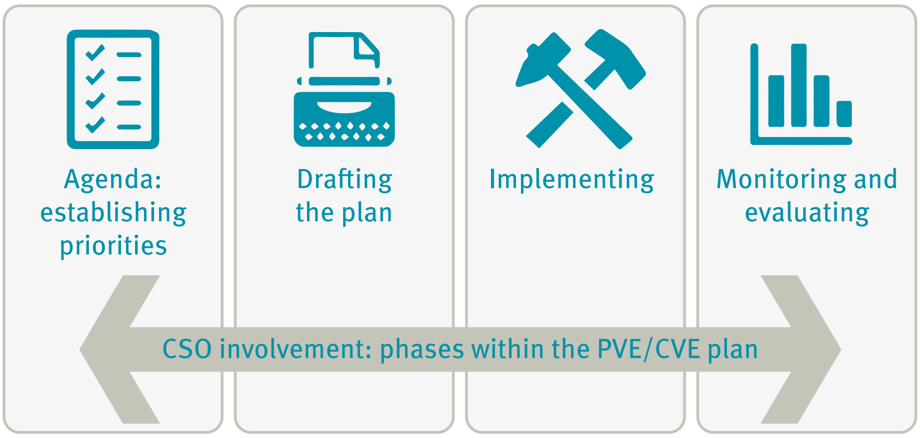
Identification. In order to ensure the correct CSOs are identified for specific activities, it is desirable to have information on their structure, degree of expertise and capabilities. The use of a simple matrix can facilitate the work of the government agency that assumes leadership and coordination of the PVE/CVE plan, as it assists in identifying predefined criteria of the CSO in question.

Prioritization. Once the CSOs have been identified, the process of prioritization should be undertaken in order ensure that each CSO is utilized within the activities to which they are best suited while adhering to the fundamental objectives in the PVE/CVE plan.

For example, where activities are related to interventions within schools through "credible voices", CSOs from the local area that can build relationships with the target audience (school pupils) should be given priority. Additionally, previous experience would suggest that victims' associations, or associations of relatives of radicalized youth, working in coordination with governmental authorities and through their own networks, are often the most effective CSO collaborators for PVE/CVE activities.

Action plan. It is important to identify the model of action and collaboration that will be maintained with the different CSOs that are involved in the PVE/CVE plan—in particular, the stage of involvement of the CSOs. Four stages are described below.

Figure 5. Four main stages of possible CSO involvement


Agenda: establishing priorities
Drafting the plan
Implementing
Monitoring and evaluating
CSO involvement: phases within the PVE/CVE plan

Agenda: establishing priorities. CSOs can be included during agenda planning to take advantage of their in-depth knowledge of the target audience (including trends and community needs). Likewise, their participation can generate credibility and build confidence within society at large, validating future activity in relation to PVE/CVE and counter-terrorism. CSO inclusion in planning should be formalized, thus giving the CSO standing as a partner of the government. This demonstration of official collaboration will help to strengthen the trust of the parties involved, fortifying the working relationship between these parties. The use of informal consultation conferences is also a consideration, as it gauges the atmosphere and approaches between the participating organizations and the general society.

Drafting the plan. Once the priorities of the PVE/CVE plan are identified, drafting the national or regional PVE/CVE plan may require collaboration from CSOs, either from the beginning of the design process or to provide input once that has been completed. Academic centres that have experts in this field, along with CSOs with a profound knowledge of the target population, are partners for consideration for inclusion as collaborators.

Implementing. CSOs can directly implement aspects of the PVE/CVE plan, or the government may finance existing CSO projects that are directly associated with the objectives and national strategy of the PVE/CVE plan.

Monitoring and evaluating. The monitoring and evaluation of the results and effectiveness of a plan or activity can be enhanced by the collaboration of CSOs. In this case, the use of surveys, request reports and workshops with the selected organizations may be a tool that could be used in order to enhance productivity.

Support and training for CSOs. Collaboration and cooperation with CSOs may highlight areas for improvement. Addressing these issues will increase the effectiveness of the PVE/CVE plan. Training activities relating to the use of social networks and the creation of online campaigns, or the simple constitution of forums in which CSO collaboration regarding PVE/CVE are evident, are effective in strengthening these organizations and will reinforce coordination and cooperation within them. Financing of projects is, undoubtedly, another aspect that will enhance these organizations, and therefore positively contribute to the effective implementation of a national or regional plan.

Training given to CSOs, focused on empowering them in their work as government partners in PVE/CVE, may focus on, among other things, developing knowledge in relation to the design, launch and management of online counter-radicalization campaigns.

Evaluation of CSOs. It is also necessary to implement evaluation of the relationship with CSOs. Periodic monitoring meetings between the staff of these CSOs and the governmental agencies to ensure that the adequate degree of communication between both is achieved, is essential. This will ensure that the expectations of both parties in meeting objectives is fulfilled and will provide a platform through which engagement can be modified or adapted to current situations.

Concluding points: successful society and community involvement

These elements are essential for delivering sustainable PVE/CVE activities:

- *Credibility.* The actor promoting the PVE/CVE message, whether governmental, CSO or community-based, must build and hold credibility in the eyes of the target audience.
- *Families.* Families are a key factor in understanding the radicalization process of specific individuals and, in the same way, are critical to facilitating the disengagement process. Families are also in a position to notify authorities of relocation and return of FTFs, as they may have critical information on the needs and plans of those returnees. To guarantee this active involvement, a mutual relationship of trust and understanding must be built with the authorities beforehand. The collaboration of local CSOs is crucial to avoid creating the feeling of being under scrutiny and suspicion, and in order to maintain sustainable and personal contact with relatives. Active engagement will help build the necessary resilience among families to avoid future potential radicalization of other siblings who could feel attracted by the phenomenon.
- *Police.* Local police officers have a special role in terms of community engagement, as they can not only recognize the first signs of radicalization, but also receive information from other local actors or even relatives themselves. In order to improve this police involvement in the community, several practical steps are considered in the box below:

It is essential to deliver specific programmes together with other local organizations in order to create networks of trust in order to gather the correct information about radicalized individuals and/or returnees, and to build the proper local network to support these affected families. Specific protocols to share this information should be recorded.

Providing law enforcement staff with appropriate training in terms of community engagement, approaches, CSO management and how to approach and deal with sensitive situations is essential.

Establishing a personal contact point with the local police team is highly effective in order to build resilience and a solid relationship with the affected families, without the fear that they (the families) are being screened or persecuted.

A “two-way” relationship between families and the local police officer must be established. This should not only be based on receiving information but on providing advice and support during the deradicalization and disengagement processes.

- *Measurement*. A key element of any PVE/CVE strategy is the evaluation and measurement of community engagement. In addition to the measurement of the impact and outcomes of PVE/CVE activity, a thorough measurement plan assesses the design of the activity; the CSOs involved; and the relationship established with those CSOs. Measurement activities should be carried out in collaboration with CSOs.
- Several tools can be used for measurement, depending upon the nature of activity and the nature of the CSO involvement. Generally, the available tools include:
  - *Quantitative research* (data obtained through interviews and surveys). How many people knew about the activity, and how many people eventually participated? For example, how many individuals have asked for support through a hotline?
  - *Qualitative research* (using personal interviews or focus groups). In what ways was the beneficiary community affected by the activity? For example, did a police-community outreach programme mitigate the risk of radicalization of a returnee's sibling? How would one measure this mitigated risk?
  - *A combined method; descriptive analysis of data and statistics.*

Chapter 5

Adult learning and training methodology

5.1 Chapter objectives

This chapter is designed to empower judges and prosecutors in South Asia and South-East Asia to effectively act as trainers, and conceive and deliver effective, tailor-made and goal-oriented training and capacity-building events in the field of foreign terrorist fighters (FTF), preventing and countering violent extremism (PVE/CVE) for the benefit of a variety of audiences, with a special focus on other judges and prosecutors in the countries in the regions.

In particular, having studied and absorbed this chapter, the new trainers should be able to:

- Describe the differences between adult/professional and student learning
- Draw the participant-centred learning cycle model and identify and describe the six steps in the cycle
- Describe the main ways in which a needs assessment on FTF, CVE and PVE may be conducted
- Draft S.M.A.R.T. performance-based objectives for a course on FTF, CVE and PVE
- Conceive a course/module design following the participant-centred learning cycle model
- Describe the role of the facilitator
- Demonstrate correct use of the training equipment (e.g. PowerPoint, etc.)
- Create a list of at least 50 "best practices" that can add professionalism to the planning and delivery of training sessions on FTF, CVE and PVE
- List at least three "best practices" for the organization of practical exercises

5.2 Introduction to the training methodology chapter

Institutions and organizations across the globe tend to appoint trainers whose technical expertise in a particular field is well established and recognized. The assumption is that somebody who knows a topic very well is capable of explaining it. Unfortunately, this assumption often proves to be incorrect: having worked for numerous years in a specific technical field does not automatically translate into being able to effectively train others on the topic.

Being an effective and successful trainer, capable of empowering adult professionals to efficiently carry out their job, requires much more than profound knowledge of the technical subject matter. At times, presentations are simply too long and too boring, sharing far too many details. Other times, they are completely top-down, reproducing the university learning environment where the expert acts as the professor and the participants are viewed as young students. The participants, however, are not students, but probably experienced professionals. On other occasions, it is clear that the presenter possesses profound expertise, but the presentation lacks a rational structure, or the style and approach pose obstacles to learning. These are just some of the instances where an individual with deep expertise would not be able to reach the intended goal of empowering his or her beneficiary audience.

This chapter consists of tools focused exclusively on advanced adult learning and training methodologies to empower experts to become effective trainers, able to organize and deliver relevant and practical training events in field of FTFs and PVE/CVE. The methodology will thus empower the trainers' future trainees (other criminal justice professionals in their respective countries) to effectively handle FTF and PVE/CVE cases.

5.3 Comparing adult learning and student learning

Students and professional adults learn in very different ways. Traditional teaching for students normally implies a professor sitting in the front of the classroom imparting knowledge in a top-down manner. In this context, students often listen and take notes, with minimal opportunities for asking questions and interacting with the professor. They will then be required to study at home to complete their learning process. In other words, students generally play a rather passive role as their input into the learning process is minimal; their opportunities to influence the content of the lessons almost non-existent; and they are required to memorize the information conveyed by the professors with the ultimate objective of passing an exam and obtaining a diploma or a certificate.

On the other hand, the target of this chapter will be adult professionals working in the field of FTFs and PVE/CVE, and in particular other judges, prosecutors, practitioners and criminal justice officers. These individuals need to acquire deeper practical knowledge and skills, not for theoretical purposes, but to effectively combat radicalization leading to violent extremism in their respective countries and at regional level. The context and the aims of the learning are therefore completely different, as compared to students.

The worst mistake that trainers may commit when training other adult professionals is to adopt a completely top-down teaching approach. This creates resistance to learning, as adult professionals may feel that this discredits their own experience, or is simply too boring. In any event, the learning experience would not be maximized. When training adult professionals, trainers should consider themselves as enablers: resource persons that facilitate learning.

Trainers of adult professionals should therefore take into account the following:

- Participants bring to the training a wide range of different and often complementary backgrounds and practical experiences that should be used by the trainer to enhance the learning of all participants.
- The trainer should not only share the necessary knowledge and skills with the participants, and capitalize on the wealth of expertise existing in the training room, but also help participants reflect upon how, where and when they will put such knowledge and skills into practical use.
- Participants don't need theoretical knowledge. They need practical knowledge for immediate use.

- Adults are normally motivated to learn by the realization that they face certain specific knowledge or skills gaps in their job environment. The training should therefore be designed not to provide generic knowledge, but specifically to fill these gaps.
- Adults cannot be forced to learn. They will be motivated to learn only if they recognize that the learning will immediately enhance and/or facilitate their daily professional performance.
- Learn by doing. In other words, after the presentations and interactive discussions on relevant items, a significant amount of time should be devoted to practical exercises designed to allow the learners to put into practice what they have learned.
- The learning process has to be designed on the basis of the specific needs of the future participants, taking due account of their expectations, different needs, levels and types of experience.
- Adult learners have lost the capacity to sit passively for hours, listening to the professors and taking notes. Their learning must therefore be extremely interactive, not only to capitalize on the knowledge and expertise that they may be able to share with the other participants, but also to give them a sense of self-direction and "ownership" of their learning process.
- In other words, traditional formal lectures transmitted by reading a presentation, whether on paper or PowerPoint, are normally not well received and do not yield to optimal results.
- Active learning requires much more than memorizing facts, but the actual development of core competences necessary to carry out specific practical activities linked to job requirements.

The figure below summarizes some of the key elements discussed above:

Figure 6. Features of adult learning

WHY ADULTS LEARN DIFFERENTLY

Cannot sit passively for hours

Bring experience and knowledge to classroom

Motivation to learn

Their time is precious

Need practical knowledge (and not theories)

Need knowledge for immediate use

Learn by … DOING

Training 100% tailor-made to their needs

5.4 Identification of needs

As mentioned above, when organizing a training session for judges, prosecutors or any other criminal justice professionals, it is crucial to ensure that the event meets precisely all the training needs of the participants. In other words, *each training session must be completely customized for the specific needs of a particular group of trainees*. A training session should address the gap between existing knowledge and the knowledge required to perform a certain job—in this context, to effectively handle an FTF case. It is fundamental to analyse the specific needs of the participants: what knowledge enhancement and skill improvements do they need? This analysis is referred to as a "needs assessment".

Trainers should never "jump" into the delivery of training assuming that they know the needs of their participants. The design of any training workshop should begin with a thorough needs assessment to identify the gaps in skills and knowledge of the future participants, as each group contains different people with varying experience and interests. First, the trainer should conduct initial research including consultation with colleagues to determine what resources already exist, and to ask for possible external contacts and solicit advice. Trainers should carry out Internet research to understand current best practices in the topic they are training. The needs assessment should answer the following questions:

The needs assessment will enable the trainer to find out, among other considerations:

- Who the participants are (including their age, gender, professional profile, and possible past experience in counter-terrorism and FTF-related areas)
- What they know (and what they don't know) about the various aspects of FTFs and PVE/CVE
- How much practical exposure they have had to these issues
- If the participants have attended previous practical training on FTFs and PVE/CVE at home or abroad, and on what specific aspects
- If any of the participants has particular or specific needs or problems, including personal issues

Replies to these answers should be sought from multiple sources, and not only from the judges and prosecutors that will attend the future training. At times, in fact, trainees may not be fully aware of their specific knowledge and skill gaps. Information should be acquired from different stakeholders (colleagues, supervisors, users of the trainees' services, other international or regional actors, etc.). Information can be collected through individual and group interviews, surveys, various forms of consultations, and, if possible, inspection of records and work samples. By way of example, when examining the needs of judges in the field of FTFs and PVE/CVE, inputs may be sought also from some of the following categories of stakeholders:

- More senior judges
- Prosecutors
- Policemen
- Private sector lawyers
- Relevant government officials
- Customs officials
- Civil society organizations including users/beneficiaries of their services

Once information is collected, data then need to be examined with a view to drawing conclusions and deciding on the measures to be undertaken through the upcoming training to address the issues identified and fill the knowledge and skill gaps. In larger programmes, consisting of numerous training events and possibly other types of interventions, the findings of the needs assessment should be documented in a written report containing specific recommendations for the necessary interventions. The report may be circulated, if appropriate, among the relevant stakeholders to obtain their buy-in. In addition, this written report will represent the baseline study for the evaluation of the impact of the training, as it will enable the evaluators to compare the situation before and after the training.

If carried out thoroughly, the needs assessment will allow trainers to ascertain the precise content and level at which their new training on FTFs should be delivered, ensuring therefore that the event is customized to meet the concrete needs of the specific group of trainees, and enhancing its impact.

RECYCLING IS GOOD FOR THE ENVIRONMENT, BUT NOT FOR ADULT TRAINING

5.5 Learning objectives

On the basis of the information acquired though the needs assessment, trainers designing a new course on FTFs and PVE/CVE should develop the corresponding performance-based objectives, also known as “learning objectives”.

The learning objectives express what the participants will be able to do by the end of the course or module, in terms of their capacity to effectively handle FTF-related cases. Learning objectives are essential for previewing and framing the content of the course. Learning objectives represent a powerful “marketing” tool to obtain the buy-in of the participants, as the objectives will be built on the specific learning priorities identified during the needs assessment. This explanation of the course’s relevance will encourage active participation and engagement. The learning objectives should be presented to the participants at the beginning of the course/module.

In particular, the learning objectives:

- Should be trainee-focused and not trainer-focused, highlighting what the participants will be able to do by the end of the training (e.g. “By the end of the course/module, the participants will be able to …”).
- Should focus on the improvement of specific capacities to perform FTF and PVE/CVE-related responsibilities.
- Should not be generic but rather very specific (e.g. avoid “soft” verbs such as “will know more about …”, “will be more familiar with …”, and utilize action-related verbs such as “to describe, to outline, to draft, to list…to do”).

- Should enable the trainer, as well as the participants, to assess improvement in performance at the end of the course. Therefore, the use of concrete and possibly numerical indicators is strongly encouraged.
- In sum, use the acronym S.M.A.R.T. Objectives should be **S**pecific (indicating what precise actions the participants will be able to perform); **M**easurable (possibly through numbers); **A**ttainable (the results can be realistically achieved by the participants); **R**elevant (in line with the needs of the participants); and **T**ime-bound (it can be achieved before the end of the course). These objectives will permit both the trainer and the participants to assess if the expected results were achieved or not.

There are two levels of learning objectives: general (for the entire course) and specific (for each module). Courses lasting one or two days may merge these two categories into one unique set of objectives. At the end of the course/module, the trainer should check if the proposed objectives have been achieved. Participants should be asked to review the objectives at the end of each session and at the end of the course, using the objectives as a checklist.

There are different ways to check that the objectives have been met by the end of the training course /module. These include:

- Asking questions orally at the end of the module/workshop (this is also an excellent technique to recapitulate).
- Using evaluation forms for each module.
- Using (if appropriate) pre-questionnaires (forms administered at the beginning of the module/ workshop) and post-questionnaires (forms administered at the end of the module/workshop). This technique consists of asking in the pre-questionnaire a number of FTF and PVE/CVE-related multiple-choice questions corresponding to the main objectives for the module/course. Then, the same questions should be asked again in the post-questionnaire. Comparing the results of the two questionnaires will show the extent of the participants' improvement. This exercise should be carried out anonymously.

LEARNING OBJECTIVES FOCUS ON THE PARTICIPANTS AND NOT ON THE TRAINER

The following are examples of learning objectives potentially appropriate for FTF and PVE/CVE training.

By the end of the module, participants will be able to:

- Define the concepts of FTFs and PVE/CVE
- List at least seven offences linked to FTFs
- Explain the key factors on deciding the jurisdiction for prosecution of FTF cases
- Explain the difference between indicators and proof
- Present at least five best practices in handling digital evidence

- List at least seven general indicators of FTFs
- Outline at least three types of electronically stored information
- List at least 10 best practices to carry out online investigations
- List and describe the three main special investigation techniques
- Outline the difference between "informant" and "secret agent"
- Explain the importance of corroborating and validating FTF indicators
- Describe the two ways in which a device can be allocated an IP address when connecting to the Internet

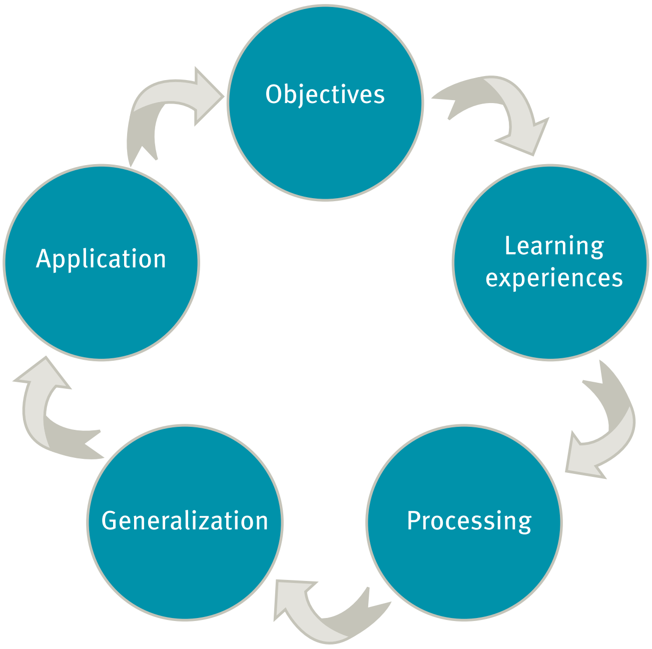
Practical exercise:

Users of this manual should attempt to draft 2-3 SMART learning objectives for future FTF courses.

5.6 Learning cycle

The learning cycle is a very useful planning and delivery tool. It consists of six steps. Each step is designed to increase the level of knowledge retention of adult learners, maximizing their learning experience and the amount of practical knowledge that they will acquire, and bring back to their workplace. The figure below illustrates the learning cycle and its six steps.

Figure 7. The learning cycle



The six steps of the learning cycle are as follows:

1. Objectives

Each module should be devoted to a particular aspect of FTFs and PVE/CVE. In the introduction, the trainer should provide a short overview of the topic, explaining the logical reasons why the subject is relevant to the participants and their professional development. The trainer should also explain how the specific topic of the module fits into the overall theme of the training session. He/she should also link the session topic with previous and subsequent topics. Following this short introduction, the trainer should present the main learning objectives of the learning session and seek buy-in for their validity and relevance.

2. Learning experience

This is the most traditional part of the learning cycle, as it involves the transmission of FTF and PVE/CVE-related knowledge and skills by the trainer to the participants. It is fundamentally important to adopt the most appropriate methods to share the knowledge with participants. Some learning activities are more passive than others. The choice of which method to adopt should depend upon the objective of the session, its duration, and the number and level of knowledge of the participants. There is no one best method for all training situations. Ideally, a well-developed course will take advantage of all relevant learning methods, using different methods for different parts of the course, depending upon the topic and the learning objectives. This has the added advantage of maintaining interest throughout long presentation sessions.

These methods include:

- Lecturettes (short, concise and highly interactive presentations particularly suitable when participants possess very limited or no knowledge in the subject matter). They may be supported by a well-crafted PowerPoint presentation. Lecturettes should focus on a few main points only)
- Videos
- Role plays and simulations (different participants are asked to represent different roles, such as the judge, the prosecutor, the police and the customs official in an FTF and PVE/CVE case)
- Case studies
- Instructional games
- Brainstorming (a highly interactive and useful technique to generate creative new ideas in a group environment, particularly when the group is not too large and members already possess a certain level of practical knowledge of the particular FTF and PVE/CVE issue)

3. Processing

Once the learning experience is completed, the trainer should support the participants in processing and analysing the knowledge acquired during the previous phase. The trainer should help participants reflect upon what they have learned by encouraging them to share their own experiences and personal reactions, and on what new lessons they have captured. There are different ways to carry out the processing phase, including through Q and A sessions and practical exercises aiming at putting in practice the knowledge received from the trainer. By actually carrying out an activity, participants will be able to “learn by doing”, which is the key principle of adult learning.

4. **Generalization**

   The generalization phase is the moment in the learning cycle when participants are invited, through open and participatory dialogue, to draw conclusions and identify best practices and lessons learned from the experiences of the previous two phases. Participants are encouraged to take a step back from the specific analysis of the processing phase and identify important general principles.

5. **Application**

   In this phase of the learning cycle, participants are invited, through questions, to consider how they will apply the knowledge and/or skills acquired during the previous phases to their jobs.

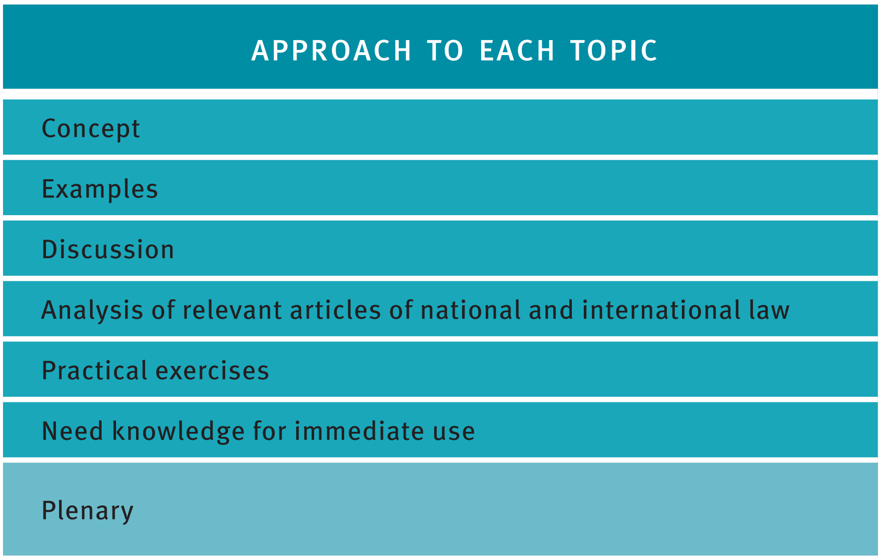
6. **(Back to) Objectives**

   At the end of the session, the trainer summarizes the learning experiences and reviews the key points that were learned, processed and generalized. The trainer resubmits the objectives of the module to the participants to ensure that they have been achieved. This last phase of the learning cycle is often carried out through questions and answers. The trainer should then link the topic's session to the overall programme.

The learning cycle should not be considered as a completely static tool that requires trainers to move inflexibly from one step to the next, always clockwise and at the same pace. On the contrary, the learning cycle allows for flexibility, taking into consideration the circumstances of the specific training event.

The figure below proposes an approach to presenting FTF and PVE/CVE-related topics, which avoids the usual trainer-oriented top-down provision of information.

Figure 8. Proposed approach to FTF and PVE/CVE-related topics



APPROACH TO EACH TOPIC

Concept

Examples

Discussion

Analysis of relevant articles of national and international law

Practical exercises

Need knowledge for immediate use

Plenary

5.7 Course plan

The course plan is a fundamental preparation tool that enables the trainers to make all the necessary substantive arrangements in order to achieve the expected learning objectives. Those arrangements include time allocation and sequencing, which are fundamental for the success of any training event. It is not enough to know “where we are going’”. It is necessary to also know “how we will get there”. The learning objectives will enable the trainer to know what results the training session should achieve; the course plan will enable the trainer to establish the process toward the results.

The course plan for each module should be carefully designed to achieve specific learning objectives. The course plan should recognize which step of the six-step learning cycle is being reinforced. Consideration should be devoted to, for example:

- Which method may be adopted to share the knowledge (e.g. short and interactive lecturette, a video, brainstorming, an exercise)
- Analysis and processing of the knowledge that was shared by determining when and how to carry out practical exercises
- Generalization of the knowledge and consideration of how to apply it in future
- What tools and equipment are necessary during each phase of the training

WATCH OUT FOR TIME MANAGEMENT

The table below may prove to be a useful and practical tool to support new trainers to create their course and module plans. For explanatory purposes, the table schedules the first module of a three-day FTF and PVE/CVE course.

Table 7. Sample module plan

TIME	LEARNING ACTIVITY	ROLE OF THE TRAINER	ROLE OF THE PARTICIPANTS	SUPPORT MATERIALS
8.30 – 9.00	Registration	Welcomes participants	n/a	Registration forms, manual, note pads
9.00 – 10.00	Opening (including speech by VIP, presentation of schedule, objectives, methodology, participants, etc.)	Carries out the opening	Listen, introduce themselves	Banner, welcome slide, photographer, podium
10.00 – 10.30	Interactive PowerPoint presentation on interviewing techniques and short video	Presents, asks questions, replies	Listen, take notes, contribute by asking questions and replying	PowerPoint and video equipment

10.30 – 10.45	Coffee break	n/a	n/a	Tea, coffee, snacks
10.45 – 11.00	Group exercise on main interviewing techniques	Presents the exercise, monitors	Carry out exercise	Photocopied exercises
11.00 – 11.30	Plenary discussion about the exercise	Leads processing discussion	Present outcome of group work, discuss	n/a
11.30 – 11.40	Generalization and application discussion on interviewing techniques	Leads discussion on generalization and application	Discuss and reflect upon general principles and future application	n/a

Learning objective: By the end of this module, the participants will be able to list at least six best practices to carry out face to face interviews of suspects of FTF-related crimes

Practical exercise:

Participants/users of this Manual should attempt to come up with a partial course design relating to 1-2 learning objectives for the future FTF and PVE/CVE courses.

5.8 Logistical arrangements

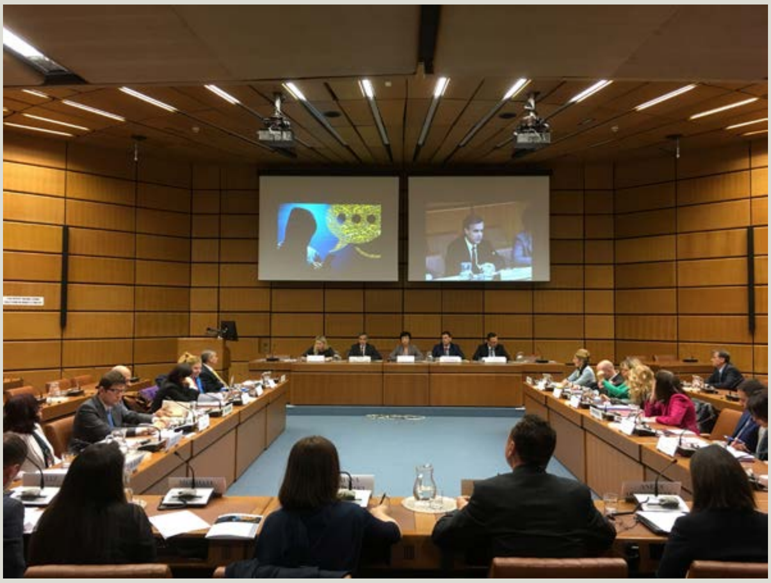
Training room and venue set-up play a fundamental role in facilitating the success of the training session. Some best practices include the following:

- Since all participants in FTF and PVE/CVE training sessions will be adults/professionals, it is essential to avoid organizing the room in any way that resembles traditional university classrooms where students are seated in rows facing the lecturer, thus focusing all attention to the trainer. Tables should instead be arranged in a U-shape where participants can easily see both the trainer and all other attendees. This arrangement significantly enhances the participatory approach and greatly facilitates discussion and interaction both among the participants themselves and with the trainer.
- The room should be neither too big nor too small, and has to comfortably accommodate the required number of participants, up to a maximum of 30.
- Each participant should have a nameplate with his/her name visibly printed to enable the trainer to acknowledge his/her contribution by calling the person by name.
- The precise seating arrangements of the participants should be decided by the trainer, and not left to the participants who naturally tend to sit close to their colleagues and friends.
- It might be useful to also have small break-out rooms for carrying out practical exercises.
- Equipment should be tested and fully functioning.
- Air conditioning should be available in the room and should function without making much noise.
- A flip chart may be useful, but should be easily visible to all participants.
- Spaces for coffee/tea breaks and lunch should be available separately but close by the training room. The organizer should provide lunch at the venue so that participants do not have to leave to eat or go back to their offices.
- Water should be available on the tables in the room throughout the training.

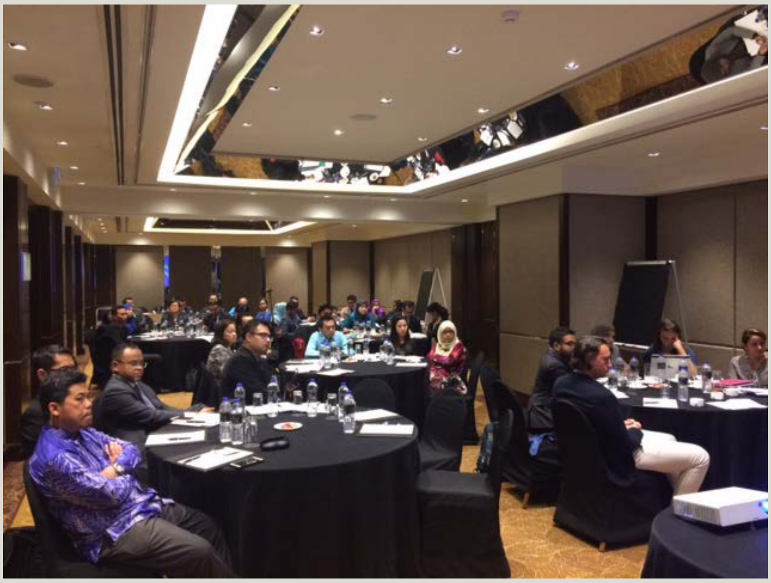
Discussion/reflection point:

Please assess if the following training rooms are in line with the above best practices. What are the positives and negatives of each arrangement?

Training room A



Training room B



Depending on the circumstances, a training session might be held as a residential event, where participants are removed from their daily work environment and are able to concentrate on the course without distractions. This arrangement will also be conducive to establishing professional and personal networks.

5.9 Course opening

The opening speech plays a fundamental role in establishing the foundations of the training session that is about to be implemented. It must include information that, if not communicated during the opening, may cause behavioural and logistical issues throughout the course. Adult trainees may not feel comfortable in situations where they are not fully aware of what to expect.

Often, the opening ceremony is somewhat formal, particularly when special and important guests are involved. In this context, it is important to remember that dignitaries should be given the floor as soon as possible to allow them to leave early, if they so wish.

After the words of welcome and the official opening by dignitaries and/or other guests, the trainer should:

- Present the schedule of the training programme; introduce himself or herself; introduce the other organizers of the course; and introduce the experts who will lead the training on the different modules.
- Present the main learning objectives. This is an opportunity to signal to the participants that the training is about to begin, which will heighten their attention and performance.
- Introduce the practical and interactive training methodology of the event, and possibly the role of the facilitator, if present.
- Ask the participants to introduce themselves. The trainer should specify that each introduction takes a maximum of 30 seconds.
- Present and agree upon a number of ground rules relating to issues such as the use of mobile phones, respect for the schedule (i.e. punctuality), attendance, and so on. The trainer should obtain the participants' agreement to these rules.
- Other possible administrative issues may also be covered (issues relating to per diem, hotel accommodation, transportation, etc.).

Presenting all of these points clearly and effectively during the course opening paves the way for a successful training event.

5.10 Exercises

As Confucius said: "If I hear, I forget, if I see, I remember, but only when I do, I understand". This is the basic philosophical underpinning of professional learning, as adults learn by doing. The most effective way to help adults learn is therefore by providing them with opportunities to put into practice knowledge and/or skills provided by the trainer. As such, practical exercises are at the core of the practice-oriented learning process.

However, creating and managing exercises requires careful advance planning and a number of best practices should be observed:

- While the bare minimum is one exercise per day, very often this may not be sufficient, and a good trainer should be ready to propose other exercises to his/her participants as required. This may become necessary, for example, when the trainer realizes that, either the participants are particularly tired and they need to do something practical and more proactive, or because they did not fully understand a particular point. Five, six or seven short exercises per day may turn out to be an excellent way to ensure active participation and effective practical learning.
- Each exercise on FTFs should be introduced in detail by the trainer so that participants understand exactly what they have to do, by when, how and why they will have to carry out the exercise.
- Time management is fundamental as exercises can be time-consuming. Long exercises should generally be avoided. Even a 10-minute practical exercise will require at least a 20-minute plenary discussion.
- The ideal number of participants per group when carrying out an exercise is three; five is too many, and individual exercises should be avoided.
- The trainer should monitor the groups by approaching each group to ensure that it is working through the exercise in the right direction. If this is not the case, the trainer should provide helpful suggestions and possibly repeat some of the key substantive content of the training.
- The trainer should lead a plenary session where each group presents the outcome of its work and obtain feedback from the expert and/or from other participants.

5.11 Visual aids

Visual communication increases the effectiveness of oral communication. However, there are a number of commonly made mistakes that may be committed when using visual aids.

One of the worst made mistakes is when visual aids become the main source of information, and participants start trusting the PowerPoint presentation more than the trainer. In other instances, slides may contain too many words, with long and convoluted sentences, with the result that participants read through them instead of paying attention to the trainer. Visual aids are more effective when used to reinforce key points and help participants remember important concepts.

PowerPoint is currently the most commonly used visual aid. However, there are different types of visual aids that may be used, such as flip charts, whiteboards, and videos.

PowerPoint

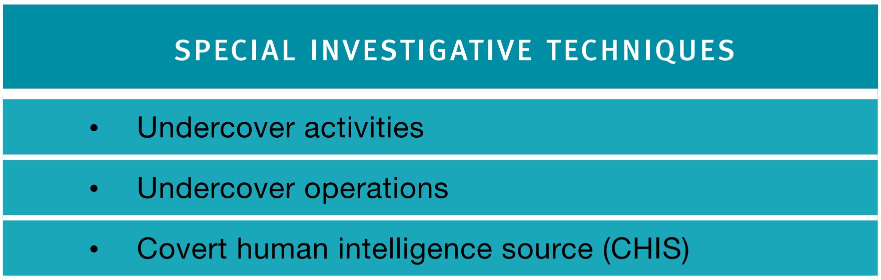
In terms of timing, PowerPoint slides should be conceived only after the actual content of the presentation has been fully developed. Only at this point in fact, will it be possible to establish which key concepts and ideas could be used for training purposes. While good PowerPoint presentations can significantly contribute to the success of the training and the overall learning of the participants, bad PowerPoint presentations may be a source of distraction, limiting the impact of the training. Some best practices when designing PowerPoint presentations include the following:

- Slides should be as simple as possible. Aesthetics is not a criterion that influences the quality of a PowerPoint presentation and the participants' learning.
- Special effects may be used, but within reasonable limits.

- Each slide should focus on one or two important concepts, with text kept to a bare minimum (ideally, seven words at the maximum). Maintaining plenty of blank space in each slide will help participants to focus on the key message. It is up to the trainer to articulate complex information, while the slides should only reinforce the message by highlighting a few key words.
- Long and/or full sentences should be avoided. If possible, replace words with compelling images (and in the area of FTFs, images may be particularly compelling).
- Be consistent with the size and font. Ensure that words are not written in a font smaller than 22 or 24 to allow participants sitting far away from the screen to easily read the presentation.
- Use plain backgrounds. White is ideal. Avoid strong colours, patterns or images that would make the slide difficult to read, particularly for the participants seated far away. Some colour combinations are not suitable for PowerPoint presentations, as they make it difficult for the participants to read the text (e.g. yellow or pink writing on a white backdrop).
- Too many images could distract attention from the main message, instead of supporting the learning.
- Feel free to use various colours provided that they are used for a reason, and not only for aesthetic purposes.
- Lights in the training room should never be turned off, so as to avoid losing eye contact with the participants. The trainer should look at the participants and talk to them at all times, and avoid reading from the screen.
- When not using PowerPoint, the trainer may consider darkening the screen to avoid distracting the participants, or move to a different part of the room. Pressing the B-key during a slideshow turns the screen black.

The following figure is an example of a PowerPoint slide that meets the quality criteria indicated above:

Figure 9. Effective presentation slide

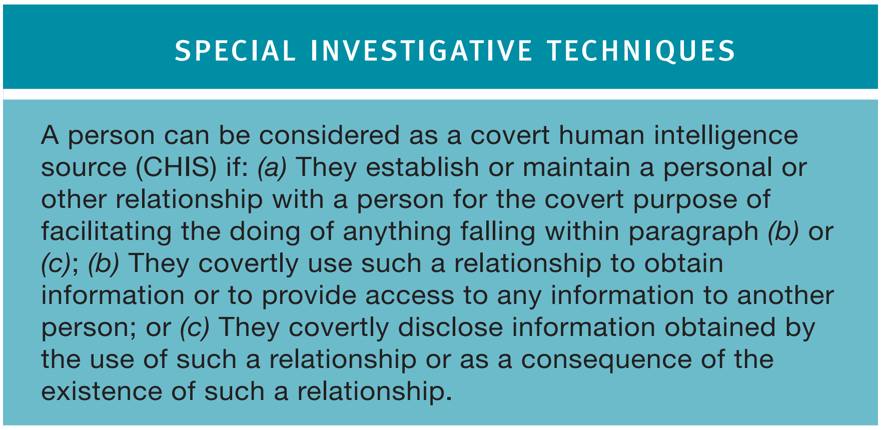


SPECIAL INVESTIGATIVE TECHNIQUES

- Undercover activities
- Undercover operations
- Covert human intelligence source (CHIS)

The following figure is an example of a PowerPoint slide that does not meet the above quality criteria and does not facilitate or enhance the participants' learning:

Figure 10. Ineffective presentation slide



SPECIAL INVESTIGATIVE TECHNIQUES

A person can be considered as a covert human intelligence source (CHIS) if: *(a)* They establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph *(b)* or *(c)*; *(b)* They covertly use such a relationship to obtain information or to provide access to any information to another person; or *(c)* They covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

While traditionally PowerPoint is used to share information with the participants and convey concepts, there are two other ways to effectively use PowerPoint, namely to ask questions or to summarize the discussions had with the participants. Only in the first case, is it possible to distribute paper copies of the PowerPoint to the participants before or during the presentation. In the latter two cases, it is important to distribute paper copies only at the end of the course or module.

Flip charts

Even though it might be perceived as somewhat old-fashioned, flip charts are not only highly effective, but also by far the most participatory form of visual aid. The trainer may write words and ideas that come directly from the participants. Other times the participants may be invited to write on the flip chart and present their thoughts to the group during the plenary session. Conveniently, flip chart pages can be detached and stuck to the wall so that reference can be made to them at a later stage.

Whiteboards

Most of the considerations in relation to the flip charts are applicable also to whiteboards. However, the written text cannot be maintained and has to be erased if other text, images or charts have to be presented on the board.

Videos

A short video can often be used to support instruction or to present information. The advantage of a video is that it can capture immediate interest. On the other hand, there are some important precautions that should be adopted if the trainer decides to show a video. In particular, a video should be:

- No longer than seven minutes
- Completely to the point
- Adequately introduced by the trainer who explains to the participants why they should pay attention to the video, and on what aspects, and for how long
- Followed by a plenary where the salient elements of the video are summarized and discussed

Finally, it should be recalled that videos on FTF issues may contain very sensitive images and information, and may agitate participants. Words of caution should therefore introduce the videos.

5.12 The facilitator

The facilitator is an additional person who is present in the room at all times and supports the delivery of the training, in all its aspects. Facilitators can make sure that the participants have opportunities to think critically, contribute to discussions by sharing their experiences, and understand and absorb all the concepts presented. The following paragraphs describe the fundamental role that could be played by a facilitator. New trainers in the same office should consider acting as each other's facilitators.

Becoming a good facilitator takes time and commitment. However, there are some basic characteristics that a facilitator should possess.

Firstly, the facilitator should launch the upcoming module and introduce the new trainer. Afterwards, the facilitator's role is to create an environment that encourages participatory dialogue, making sure that everyone wishing to contribute feels comfortable to do so. The facilitator helps participants reach consensus, find common ground, or agree to disagree. The best way to achieve this result is to learn to listen to the others and help participants to listen to each other. A good facilitator should be an acute observer, scrutinizing the body language of the participants and taking appropriate measures when he/she realizes that an individual or the entire group is having difficulties in understanding a particular concept, or simply is too tired to pay attention.

When the trainer presents an exercise, the facilitator can help manage the groups. He/she will have to monitor each group to ensure that everyone participates and contributes, and to support the group as a whole to move in the right direction. The facilitator should continue this rule through the plenary discussion after the end of group work.

In general, the facilitator can take steps to enhance the trainer's delivery, particularly if the trainer is not trained in, or not remembering to follow, the techniques and methodology presented in this module. For example, a trainer may be too focused on his/her presentation to go through the six steps of the learning cycle. Should this be the case, the facilitator can ask relevant questions to make the presentation objectives clearer, or motivate participants to summarize specific or general lessons. The facilitator should write key points on a flip chart or whiteboard to summarize the trainer's points, repeat important elements, and draw conclusions. To make meaningful contributions, the facilitator should possess a certain level of knowledge of the subject matter presented by the trainer.

On a practical note, the facilitator should take care of elements which, if neglected, could adversely affect the training event. The facilitator must ensure that there are no obstacles which hinder the participants' learning, such as the temperature, lighting or noise levels in the room, or any other elements that could potentially be a source of distraction.

In sum, the most important characteristic of a good facilitator is flexibility. The facilitator should adjust depending on the type of trainer that delivers a particular presentation. If the trainer is knowledgeable, a good communicator, and perhaps already familiar with the participatory learning methodology presented in this module, then facilitation can be less pronounced. On the contrary, if the trainer is not a good communicator or not familiar with the training methodology, the facilitator must be more engaged to maximize the group's understanding. Needless to say, trainers and facilitators should extensively coordinate prior to commencing the delivery of the course.

Finally, it is up to the facilitator to effectively handle awkward and unpleasant situations, such as:

- A participant not paying attention or falling asleep
- Two or more participants disturbing the class, such as by talking or fighting
- A participant using the phone during the training
- Participant aggression towards any person in the room
- Participants opening discussion about sensitive issues, such as religion, politics, sexuality, etc.
- Problems with the trainer, such as speaking speed and volume, attitude or eye contact

5.13 Public speaking techniques

Speaking in front of a group, particularly when it includes senior judges, prosecutors or investigators, can be an extremely challenging experience. Presenters may fear that:

- Participants may not be attentive or even disrespectful
- Their presentation may not hold the interest of participants
- Their presentation is so complex that he/she might forget specific points
- There is not enough time, or conversely, the presentation finishes too early

The following pages contain some tips and suggestions that might help new trainers enhance their public speaking skills.

Tension/stress

Nobody is completely immune from experiencing a certain level of stress during a presentation this is normal and natural. Some stress, however, can bring about positive results. Tension can help the presenter concentrate and increase the energy that he/she puts into the presentation. There are numerous ways to reduce the fear of speaking in public. These include:

- Thorough preparation of both the content of the presentation and the actual delivery. Repeated rehearsals in front of a group of friends or in front of a mirror can contribute to significantly reducing stress and enhancing delivery of the presentation.
- Making eye contact may prove the most effective technique to reduce stress, as participants will also look back, perhaps nodding or smiling.
- Similarly, establishing personal relationships with members of the audience before commencing the presentation may allow the presenter to see “friendly” faces in the audience and feel supported by their positive attitude.
- Maintaining appropriate posture. By way of example, it is better to avoid having arms crossed in front of the chest, which can not only be perceived as defensive and unwelcoming, but also causes physical tension throughout the body. Instead, remember to breathe slowly and deeply, and move about the room to loosen the legs and calves.
- Being familiar with the premises where the presentation will take place, and being comfortable with the equipment that he/she will use for the presentation.

Reflection point

What would you do if during one of your training events:

- A participant starts talking on his phone or using messenger to communicate with friends?
- Two participants keep on talking among themselves?
- The speaker is boring and monotonous?
- A participant raises his or her hand to take the floor too often?
- The air conditioning breaks down?

Positioning

Interactive training requires the trainer to be approachable. Sitting behind a desk or a podium will not foster a sense of accessibility, and participants may find it boring to see the trainer stay in the same position. Instead, the trainer should ideally deliver his/her presentation while standing, moving around the room, and creating an atmosphere of open interaction.

This may not always be possible in more formal settings. For example, in a conference, presenters may need to deliver their presentations from behind a podium. This is acceptable as conferences are not designed to empower adult professionals to carry out a particular job, but aim at raising their awareness on a particular issue.

Volume and pace

Everyone in the room should be able to hear every word clearly. This requires the presenter to speak more slowly and louder than in an ordinary conversation. Modulation in the tone of voice helps avoid monotony. A good presenter systematically projects his/her voice to the participants sitting at the end of the training room, even when addressing a question asked by an attendee seated beside the position where the trainer is presenting.

Silence

Strategic pauses in public speaking are effective, and very powerful. They are fundamental to giving importance to what has been said, and to what the presenter is about to say. Presenters should not be afraid of silences, as they don't indicate lack of knowledge and confidence, but, on the contrary, add gravitas and project control.

Body language

Hand gestures can be used to add emphasis to a particular point. Body language should not be distracting to the participant, but should be used strategically by the presenter to reinforce his/her messages.

Eye contact

Regular eye contact with all participants maintains their attention and makes them feel like active members of the discussion. Eye contact should be made in a culturally sensitive manner. Smiling at appropriate times often contributes to creating a pleasant and less formal environment.

Preparation and structure

Thorough and careful preparation is fundamental for the success of any presentation. A trainer should have a clear outline of his/her presentation. Presentations should be carefully structured, and this structure should be communicated to the participants in the introduction. The main body of the presentation should take approximately 80 per cent of the allotted time. The introduction and the conclusion should each take 10 per cent of the total time. The body must include adequate time for discussions, and questions.

A golden rule of public speaking is: "Tell them what you are going to tell them; tell them; tell them what you have told them". This rule implies that a presentation should start with a concise introduction, followed by the body of the presentation, followed by a short conclusion revisiting the main points covered in the presentation.

To structure the body itself, it might be useful to group topics in three to five categories. Participants will be psychologically ready to concentrate on three to five main points, which therefore will result in easier absorption of information. It might be useful to have a concise outline listing the main points to be delivered, but a presentation should never be read completely from a paper. A presentation should be given in short sentences; key concepts should be repeated. Concrete examples are fundamental to illustrate a point, and short real-life stories may corroborate an argument.

Interactivity

Refrain from speaking all the time. The trainer should make the presentation as interactive as possible. As a general rule, he/she should never speak for more than 10 minutes without allowing or encouraging active participation from the group.

Be attentive

Finally, an effective presenter should always be cognizant of the needs, feelings and requirements of the participants. This implies being open to listening to their questions and comments, and to draw learning points from them. It can also mean asking the participants particular questions when it is evident that some key points might have been misunderstood.

5.14 Conclusion: key numbers

To conclude, the list below proposes **10** key numbers in adult learning to organize and manage successful events:

Duration:	**2** days minimum, but a week is better
Number of participants:	**25** is good, but not more than 30
Hours per day:	**6**
Sessions per day:	**4** maximum, of 90 minutes each
Modules per workshop:	**5** modules over a 5-day workshop
Duration of each module:	**0.5 to 2** days
Experts per module:	**1**
Exercises per day:	**2** minimum; more is better
Members per group:	**3**
Words per slide:	**7**

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.18-03254