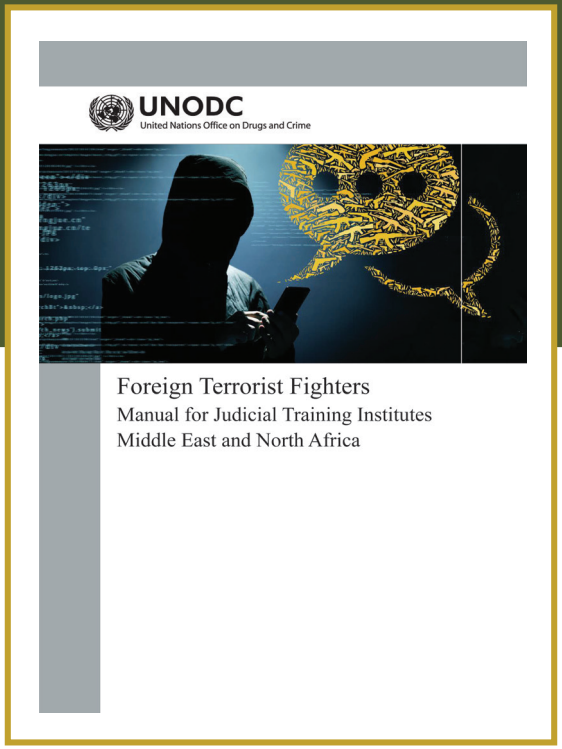
ISSUE
35

التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

INTERNATIONAL
REPORTS



FOREIGN TERRORIST FIGHTERS

MANUAL FOR JUDICIAL TRAINING INSTITUTES

MIDDLE EAST AND NORTH AFRICA

March
2022

International Reports

Monthly Issue - Islamic Military Counter-Terrorism Coalition

Director General

Major General Mohammed bin Saeed Al-Moghedi

Secretary-General of the Islamic Military Counter Terrorism Coalition/Acting

---

Editor-in-Chief

Ashour Ibrahim Aljuhani

Director of Research and Studies Department

FOREIGN TERRORIST FIGHTERS
MANUAL FOR JUDICIAL TRAINING INSTITUTES
MIDDLE EAST AND NORTH AFRICA

ISIS drew attention to the threat of Foreign Terrorist Fighters (FTFs), which preceded the emergence of ISIS; however, ISIS made it a threat to international peace and security. At the very peak of ISIS in Iraq and Syria, and by 2015, about 40,000 individuals from more than 120 countries traveled to Iraq and Syria to join ISIS. The INTERPOL database of ISIS includes 53,000 names, collected from the battlefields in Iraq and Syria. As estimated by the Global Coalition to Defeat ISIS, there were less than 1000 terrorists of ISIS in the area of the said coalition operations by the end of 2017. If the demise of ISIS has come into play, the matter is different for ISIS, which is still active in several countries, such as Yemen, Egypt, Libya, the countries of the Sahel in Africa and elsewhere.

Threats and Risks

Research indicates that about 14,900 FTFs have left Iraq and Syria; some have escaped in disguise during evacuations. Some evacuees might be unwilling to do so because of fear of executive action by law enforcement agencies. Others may instead be prevented from doing so because of removal of citizenship or other sanctions. They may look for refuge in other countries, where they could strengthen the capabilities of local violent groups

How do the MENA countries address such an imminent threat? The UNODC report provides the MENA countries with a reference guide to judicial training institutes to optimally address Returning Terrorist Fighters (RTF). It analyzes FTFs, the legal framework to address such a phenomenon at the regional and international levels and presented best practices for the successful online investigation of FTF crimes.

One key threat facing jurisdictions in the MENA region is the return of FTF to their home countries. Some research studies estimate that about 15,000 individuals from the MENA countries traveled to Iraq and Syria between 2012 and 2017; the number of women and children made up about 35%. The MENA countries are also exposed to the threats of RTFs, as they have suffered greatly as a result of their terrorist attacks.

When ISIS lost control of the territory it had once seized in Syria and Iraq, there were caveats that the FTFs of the MENA countries should gear up for an influx of RTFs, but the number of RTFs, albeit worrying, was much lower than expected. An estimated 30% of FTFs have returned home or have moved to a third country. In November 2017, a United Nations team estimated, according to figures from seventy-nine countries, that about seven thousand foreign fighters had died on the battlefields, while 14,900 fighters had left the conflict areas, of whom 5395 fighters are currently imprisoned, i.e., only 36%. Of them, 6,837 fighters, or 46%, are not subject to the criminal justice system.

FTFs are undoubtedly a glaringly notorious risk across the region; FTFs have combat expertise, aided by exercises to use weapons and explosives. More importantly, many FTFs are still unknown, there is a significant disparity between the total number of FTFs and those considered deaths, detainees, returnees or those relocated.

Why Returnees?

The motives of FTFs to return to their countries vary; some are disappointed by violent extremism, or life in territory controlled by terrorist organizations, and others may be satisfied with their families, or improve social and economic conditions; others may return to seek refuge with their families, improve social and economic conditions. It is critically important to distinguish between foreign fighters who traveled to Iraq and Syria for terrorist purposes and those who traveled for other purposes. Many returnees left Syria before ISIS announced the alleged caliphate in 2014, and most of such returning fighters (first wave) have different motives to travel abroad, such as fighting off the tyrannical Syrian regime or providing humanitarian aid to the anguished and disadvantaged Syrian people.

In any case, it is not easy predict any reaction of any of FTFs over time towards their abroad, or to receive them in their home countries; even if they undergo a strong psychosocial and security assessment, the conditions may prompt them again to search for violent solutions to their problems, especially if they return to the same circumstances.

The political discourse of returning FTFs has focused on the security risks that they may cause. In several cases, ISIS has called on returnees to attack targets in their home countries to preserve the global brand of ISIS. Returning FTFs are believed to be a significant threat for several reasons: returning FTFs may maintain the network of relationships that they have established with other terrorists while operating abroad, and such networks allow terrorists to pool resources for large-scale attacks and provide opportunities for ISIS fighters to direct operatives abroad.

The empirical examination seems to confirm such fears; one of the well-known indicators of terrorist operations carried out in the countries of the Middle East and North Africa (MENA) is the real contact between ISIS and the perpetrators. A research study conducted on about 510 attacks launched by ISIS outside Syria and Iraq, up to October 31, 2017, concluded that FTFs were involved in more than 25% of such attacks, of which 87 attacks were carried out outside their home countries.

In addition to the direct involvement of FTFs in terrorist attacks, they have contributed to the creation of a new

type of terrorist method of action; directed attacks by virtual planners who use secure communications to direct attackers remotely.

However, the security threat to returning foreign fighters should not be overestimated. According to Europol, the attacks on the EU were committed by domestic terrorists who did not travel abroad to join terrorist groups. A research study by the European Parliamentary Research Service concluded that the majority of returning FTFs may not intend to plan terrorist attacks upon their return; very few real cases of FTFs were observed returning with the intention of launching attacks in Europe.

Hence, it can be argued that returning FTFs do not share the same characteristics, as not all of returning FTFs traveled to conflict areas with the intention of engaging in terrorist violence. Some returnees, particularly women and youth, may not have received training in violent combat, or may have committed violent crimes. Upon returning, some of returning FTFs withdrew completely from any extremist activity. Some reports state that the participation of former FTFs has been instrumental to efforts to prevent violent extremism. As such, it is not appropriate to treat all returning FTFs as potential terrorist attackers.

The threat of attacks by FTFs can be classified as high-impact and low-probability. Research reveals that only 18% of the attacks carried out in the West, between June 2014 and June 2017, were by known FTFs. Yet, the attacks they carried out were almost among the deadliest. One attack killed about 35 people.

In the MENA, homegrown terrorist attacks support the UN team's assessment of the threat of FTFs in the MENA as a severe threat. The main challenge for the MENA authorities still detects and follows up on the intentions of returning FTFs.

Legal Framework

At the international level, 19 conventions and resolutions have been adopted to address terrorism over the past 60 years, addressing various topics such as the suppression of terrorist financing, transportation-related terrorism, nuclear and radiological terrorism, hostage-taking, and the suppression of terrorist bombings. Such international instruments are supplemented by the UN Security Council resolutions. Together, they create the obligations of the member states stipulated by international law, which must appear in national legislation, and be strictly implemented. The implementation of such conventions and resolutions

is guided by the guidelines provided by the UN Global Counter-Terrorism Policy, as well as the UN General Assembly resolutions.

In crimes related to FTFs in the international context and the context of the MENA, the UNSC resolutions stand out: Resolutions No. 1373 of 2001, No. 2178 of 2014 and No. 2396 of 2017. The first of these is the most comprehensive of the said resolutions, and subsequent resolutions should be interpreted and understood accordingly and duly. It is the resolution that was adopted in the wake of the terrorist attacks against the US – the 9/11 Attacks of 2001. It is the impetus for a series of international instruments targeting violent extremism and terrorism. Resolution No. 2178 established a definition of FTF, calling on member states to strengthen confrontation methods, according to three categories of measures: criminal laws, sanctions, and preventive measures. Resolution No. 2396 was concerned with the threats of terrorist fighters returning from conflict areas, unlike Resolution No. 2178, which was on FTF travelling abroad.

Global Plan

On September 8, 2006, the UNGA adopted a strategy to address FTFs; although it is not legally binding on member states, unlike the UNSC resolutions adopted under Chapter VII of the UN Charter, it is considered an unprecedented global instrument to strengthen national, regional and international efforts in the fight against terrorism; all member states agreed, for the first time, to adopt such strategy, according to a common approach to counterterrorism, based on four main foundations:

1. Addressing the conditions conducive to ubiquity of terrorism.
2. Preventing and countering terrorism.
3. Building the capacities of states to prevent terrorism and strengthening the UN relevant efforts.
4. Ensuring respect for human rights and the rule of law.

The strategy relies on the two approaches, criminal justice and governance measures, which mutually reinforce each other. The criminal justice approach calls on member states to develop and apply a set of criminal offenses to violent extremism and terrorism practices. The governance approach is used to prevent violent extremism by reducing the conditions conducive to extremism leading to terrorism. It may be difficult to solve political, economic and social problems, which are root causes of violent extremism, with a criminal justice approach; such reasons have a systematic nature and are not attributed to a particular individual or group.

The UNGA reviews and updates its counter-terrorism plan every two years to respond to changing priorities. The UNGA conducted the sixth review of this strategy on June 26 and 27, 2018. The review was conducive to the adoption of the UNGA Resolution No. 72/284 related to the risks of returning FTFs. The said resolution called on Member States to enhance cooperation at the international, regional and bilateral levels to counter the threat of FTFs, including by enhancing operational information sharing, enhancing intelligence support, and capacity building activities in a timely manner.

International Guidelines

In addition to international agreements, UNSC resolutions, UNGA resolutions, and the UN Strategic Plan to Combat Terrorism, the legal framework for confronting FTFs at the international level includes some instruments that made important recommendations, provided best practices, and urged Member States to adopt them to enhance its response to the threat of returning FTFs. Key instruments include:

The Hague-Marrakech Memorandum

It is an initiative launched by Morocco and the Netherlands in 2014, within the framework of the Global Counter-Terrorism Forum. It aims to bring together policy makers and practitioners, from a wide range of countries to share lessons learned and good practices to counter the threat posed by FTFs. The said memorandum identified 19 good practices that direct governments to develop their own policies to address the threat of FTFs. In 2015, an appendix was added to the said memorandum, which included seven recommendations about returning FTFs.

Principles of Malta

It is a joint initiative of the Hedayah Research Center and the International Institute for Justice and the Rule of Law. It was presented in 2016 and included 22 principles. The said principles were developed to guide Member States in their policies and programs for the reintegration of returning FTFs.

Guidelines of Madrid

It is an initiative developed out of a special meeting of the Counter-Terrorism Committee of the UNSC, hosted by the Government of Spain in Madrid on 27 and 28 July 2015. The meeting issued 35 guidelines, which were adopted by the UNSC in December 2015. The said guidelines fall into three themes:

1. Identifying the incitement and recruitment of FTFs, and facilitating, countering and limiting their activities.
2. Imposing travel ban on FTFs by various means, including implementation measures, the use of the history record passenger information system, and measures aimed at enhancing border security.
3. Criminalization and prosecution of returnees, international cooperation, rehabilitation and reintegration of returnees.

With the defeat of ISIS, the attention of the UNSC turned to the continued threat posed by returning FTFs. Th UNSC Resolution No. 2396 of 2017 requested the Counter-Terrorism Committee to review the Madrid Guidelines in light of the threat posed by returning FTFs. A special meeting of the committee on December 13, 2018, in New York State, helped to draw up an addendum to the 2015 Madrid Guidelines, which included 17 additional good practices that assist Member States in their efforts to respond to returning FTFs.

Regional Framework

In the MENA, the legal framework for counterterrorism, developed by the League of Arab States and the Organization of Islamic Cooperation (OIC), is related to the issue of countering FTFs. The League of Arab States approved the basic binding counterterrorism instrument, which is the Arab Convention on Combating Terrorism, April 22, 1998, which entered into force on May 7, 1999. The League approved several recommendations during the twenty-sixth Arab League Summit, held in Egypt in 2015, including but not limited to the establishment of a joint military force to confront the challenges posed by extremist terrorist groups and returning FTFs.

The OIC issued a code of conduct for member states in combating international terrorism and adopted it in 1994. Later, it adopted the OIC Treaty on Combating International Terrorism in 1999, which entered into force on November 7, 2002. The Treaty has some advantages; for example, Article (2) excluded from the scope of the provisions of the treaty the persons participating in what it considers a legitimate armed struggle for self-determination. Recognizing the challenges that hampered the 1999 Treaty, the OIC (2016) staked out its intention to consider proposing additional rules and updating some provisions of the Treaty to enhance current levels of cooperation.

Digital Investigation and Sources

Training via digital investigation supported by the collection of computer evidence has become a priority in the investigation and prosecution of FTFs. Computers, mobile phones, and the Internet have become part of modern investigations into terrorism cases; any of them can be used to commit a crime, which can contain crime evidence; they can be targets of crime.

Crimes involving electronic evidence present a unique challenge to lawmakers, investigators, prosecutors and relevant judges. Once suspects are arrested, most lawsuits draw on the use of digital evidence, including location data, social media posts, text messages, emails, and cell phone call records.

All cross-border cases involving terrorist activities or money laundering require evidence stored in ISPs servers, but these cases are further complicated by the significant differences between countries in legal frameworks, internal procedures, relevant government departments, powers and expertise. Equally important, ISPs vary in performance, practice and level of cooperation when receiving data requests from law enforcement agencies.

The ability to conduct digital investigations is becoming increasingly important; it has become a staple in all prosecutions. Since the time frame for ISPs to retain subscriber data varies, investigators should immediately submit a formal request to service providers to preserve the relevant data until the issuance of the warrant, permit or judicial order that allows the extraction of records. One of the early stages of investigations is tracking IP addresses to identify the data of the Internet Service Provider (ISP) and identify the person in charge who uses that device.

In criminal investigations, the IP address is usually the only information that would link the crime to the individual, but due to the limited number of IPV4 addresses, ISPs use technology to make up

for this shortfall, which could have dangerous results threatening law enforcement investigations, by sharing a single IP address with thousands of subscribers at the same time, making it impossible to identify individual subscribers.

Free online search tools are made available for investigators to consider when gathering open-source intelligence, such as Intel Techniques, Net Boot Camp and Research Clinic, as well as Information Framework. Open-Source Intelligence, which provides an infographic that helps collect information from free tools or sources, as well as the 2018 Guide to Open-Source Intelligence Information, which provides a comprehensive list of tools that help investigators explore information available on social media.

Facebook and Twitter

Facebook is one of the most popular social networking sites in the world, with more than 2,224 billion users (June 2020). The MENA region shows different Facebook users: Egypt (42.4 million), Saudi Arabia (23.72 million), Iraq (22.03 million), Morocco (18.33 million), Tunisia (7,445 million) and Jordan (5.755 million).

Following the publication of a whole host of negative publicity and data protection issues, Facebook removed the graphic search engine, which made it difficult to search freely for users of the website when only email or phone number was available; it was possible to use the Facebook search engine alone to access much information. Even if the person you are looking for has blocked themselves from public view, they can still be found by searching in the friend list, and the person can also be found by searching in the markup language used in the documentation for the page. Some Internet tools allow image search and location in which it was taken.

In the year 2020, the number of Twitter users increased up to 330 million monthly users across the world, and about 42% of them visit frequently the platform daily. The number of accounts on Twitter working for the benefit of ISIS reached about 46,000 accounts in 2015.

Twitter can be seen as a way to send SMS text messages, but on the Internet, which makes searching through so many messages and communications a very tedious task, Twitter provides instructions for investigators on the procedures to obtain recordings. The first thing to understand when conducting investigations with Twitter is that the search results on the website are divided into several sections; it is possible to switch between the following categories within the application itself: people, photos, tweets and videos.

Several free online tools are made available to help Twitter investigators, including Geosocial Footprint, Tweet Beaver, Node XL which is a useful tool for downloading and analyzing Twitter big data. Maltego is one of the most popular and widely used tools for digital investigations.

Evidence Collection

Digitally Stored Information: includes any information created, stored, or used with digital technology, such as speech processing files, e-mail messages, and text messages.

Computer Digital Evidence: means information and data that have value in investigations and are stored in a computer or can be transmitted by it. For this reason, they are latent evidence in the same manner that fingerprints, or DNA are.

Digital Evidence: can be categorized into information and data of value in investigation, stored in a digital device, sent to or transmitted by it. The presence of such evidence is required if data or digital devices are acquired.

Websites and Cookies: any information available on the Internet is stored in the computer system; it can be retrieved by hardware forensics. Some information may be volatile; the content can be changed or deleted, before such devices are located and examined. In such cases, it may be necessary to capture evidence directly from the Internet, during live interaction with the suspect, or by capturing live website content.

Cloud-based systems allow forensic researchers to access text messages and photos from a specific phone and keep 1,000 to 1,500 of the last text messages sent and received from a given phone. Many mobile devices store information about where the device may have moved, along with some information about how much time the owner of the phone has spent in each location. To obtain such information, the criminal investigator can access the last two hundred cellular websites reached by the mobile device.

In all cases, investigation and prosecution of cases that include digital evidence requires special criminal investigation skills, subject-matter expertise, knowledge and experience necessary to apply such

skills, and awareness of all legal requirements and procedures related to the acceptance and rules of evidence at the local and international levels. Investigators can refer to the UNODC document, Basic Guidelines for Investigators and Prosecutors to Request Electronic & Digital Data & Evidence from Foreign Jurisdictions; which contains a set of good practices.

Digital Evidence Collection

One of the main challenges from the perspective of criminal justice is the collection and acceptance of digital evidence in criminal proceedings. Therefore, precautions should always be taken when collecting, preserving and transmitting such evidence to keep it safe. Relevant good practices include:

- Gathering devices and other materials after securing and cordoning off the crime scene, with the legal authority to confiscate evidence.
- Filming or video recording of the crime scene, before extracting anything, as well as all components, including any evidence on site, taking pictures to document any activity on the computer or devices, and recording any information that appears on the screen. If a camera is not available, a diagram of the system is drawn, the ports and wires (cables) are named so that the system can be rebuilt at a later time.
- Extraction of chargers, cables, peripherals and related manuals, as well as data carriers, mobile phones, external hard drives and digital picture frames.
- Documenting any activity on the computer, components or devices by taking a picture and recording any information that appears on the screen to prevent any alteration of digital evidence during collection.

Four principles were considered at the stage of the investigation:

1. No action by law enforcement agencies or their affiliated teams should alter the data of computers or storage media on which the court may subsequently draw.
2. In circumstances where a person considers it necessary to access the original data stored in computers or storage media, such a person must be qualified to do so and be able to provide evidence explaining the relevance of his actions to the case and associated effects.
3. An audit pathway or any other record of all the operations carried out on the computer-digital evidence should be created. Such evidence should be kept. An independent third party should be allowed to examine such processes and come to the same conclusion.

4. The person in charge of the investigation shall bear full responsibility for ensuring full compliance with the law.

Forensic Data Analysis

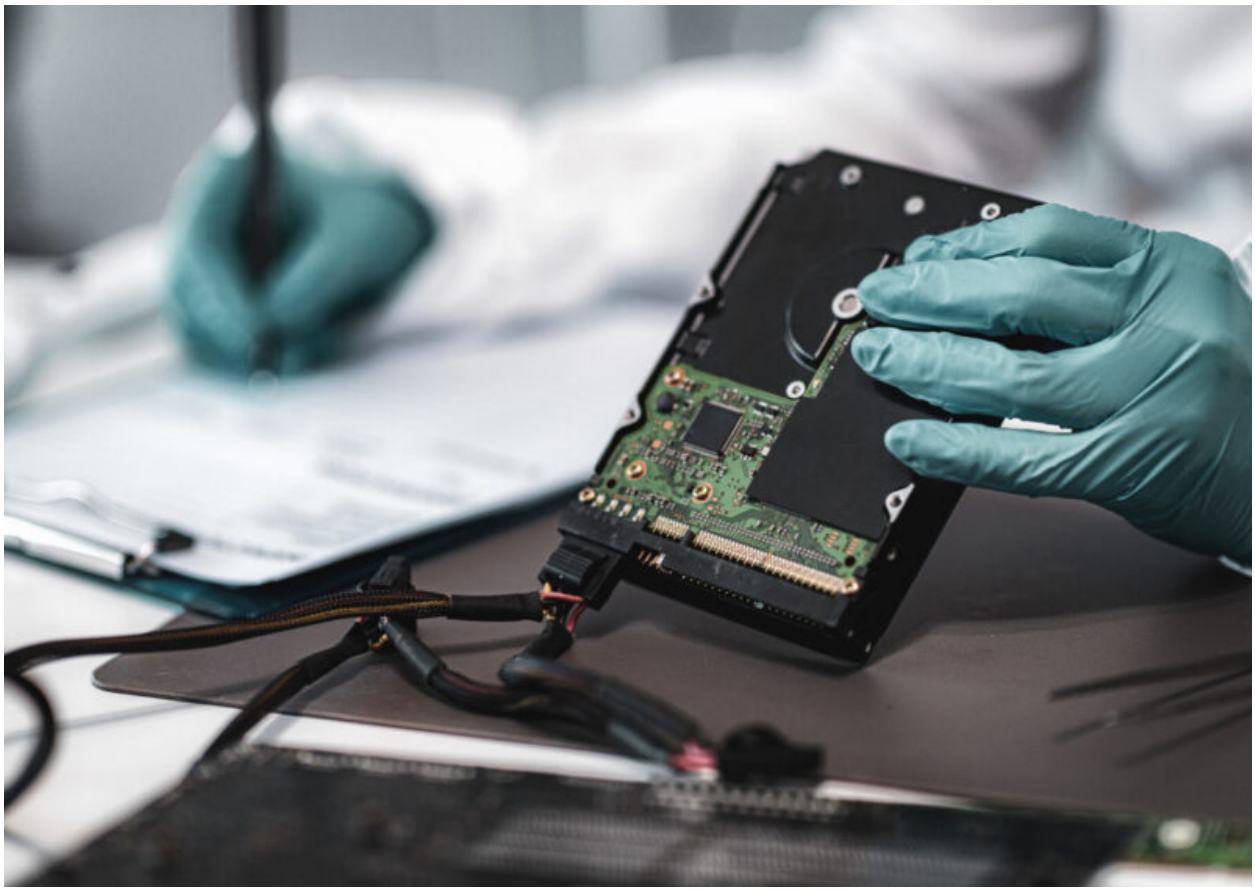
Addressing evidence is one of the most important aspects of computer forensics that is increasingly being used. One of the most recent transformations in addressing evidence is the shift from simply pulling the plug out of the device, which is the first step in collecting evidence, to adopting methods to obtain evidence directly from the suspect's personal computer.

The traditional pull-the-plug approach ignores the huge amounts of volatile data stored in memory that can be lost. Therefore, if a computer is on, an expert in computer forensics is recommended; turning off the computer may lead to the loss of evidence of criminal activity. If the computer is turned on, but it is running a destructive program that deletes, removes or damages information, the power must be turned off from the computer immediately to preserve what is left in the device.

The rapidly changing computing environment has led to challenges that necessitate a change in the collection of digital evidence. It has become possible to install applications from removable media, such as a removable storage device, and then convert it to the default mode in RAM, without leaving any trace on the disk. It is also possible for the malware to be completely present in the RAM, without any trace of its presence on the hard disk. Users can run hidden or secret encrypted files or partitions in hard disk space to hide evidence. Well-known web browsers allowed users to hide their tracks and delete log files of their activity when the browser was closed.

When addressing the said challenges, archiving and analyzing volatile data may offer the only method to find important clues that would not normally be available if the device was turned off. Computer users often do not realize that some services are turned on while they are using the computer. They operate without the user's knowledge; discovering registered drivers may provide investigators with information about peripheral devices associated with a suspect's device.

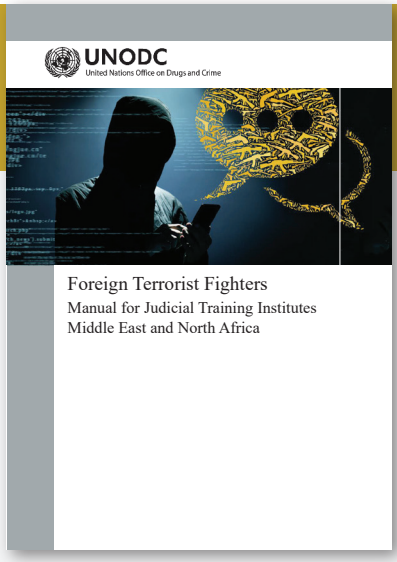
The investigator should not attempt to operate a locked mobile device even if he can remove battery, a switched off phone keeps information about the cell phone tower's location and call log.



Moreover, if the device remains on, or switched on, the evidence on it may be destroyed using remote control commands, without the investigator's knowledge. There are some phones that install and apply updates automatically; such updates may put the phone's data at risk. Therefore, removing battery was the best course of action.

If the mobile phone is in the operating mode, however, it should be kept in this mode for as long as possible; the investigator must keep a set of chargers suitable for different types of devices. He should also try to unlock the screen if possible. The device should be set in flight mode to stop connection to the Wi-Fi, Bluetooth, or any other communication system.

If the mobile phone is turned on, while the screen is off, connecting it to a power source will often force it to synchronize with the cloud services while it is running. This should increase the amount of evidence available in the computing cloud.



FOREIGN TERRORIST FIGHTERS

MANUAL FOR JUDICIAL TRAINING INSTITUTES
MIDDLE EAST AND NORTH AFRICA

Published By

United Nations Office on Drugs and Crime (UNODC)

February 2021


التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

التحالف الإسلامي العسكري لمحاربة الإرهاب

ISLAMIC MILITARY COUNTER TERRORISM COALITION