UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

INTERPOL

Funded by
the European Union

# **Cybersecurity** and **New Technologies**

# Guide for First Responders on the Collection of Digital Devices in the Battlefield

### *Disclaimer*

The opinions, findings, conclusions and recommendations expressed herein do not necessarily reflect the views of the United Nations, The International Criminal Police Organization (INTERPOL), the Governments of the Europe Union or any other national, regional or global entities involved.

The designation employed and material presented in this publication does 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 of its authorities, or concerning the delimitation of its frontiers or boundaries.

Contents of this publication may be quoted or reproduced, provided that the source of information is acknowledged. The authors would like to receive a copy of the document in which this publication is used or quoted.

### *Acknowledgements*

This report is the product of a joint initiative between the United Nations Counter-Terrorism Centre (UNCCT) of the United Nations Office of Counter-Terrorism (UNOCT) and INTERPOL on strengthening capacities of law enforcement and criminal justice authorities to counter the use of new technologies for terrorism purposes. The joint initiative was funded with generous contributions from the European Union.

### *Copyright*

United Nations Office of Counter-Terrorism
S-2716
United Nations
405 East 42nd Street
New York, NY 10017
Website: www.un.org/counterterrorism/

200, Quai Charles de Gaulle
69006 Lyon, France
Website: https://www.interpol.int/en

# Table of Content

# Joint Foreword

Advances in Information and Communication Technologies and their availability have made it attractive for terrorist and violent extremist groups to exploit them to facilitate a wide range of activities, including incitement, radicalization, recruitment, training, planning, collection of information, communication, preparation, propaganda, and financing. Terrorists continuously explore new technological frontiers, and Member States have been expressing increasing concerns over the use of new technologies for terrorist purposes.

During the seventh review of the United Nations Global Counter-Terrorism Strategy, Member States requested the United Nations Office of Counter-Terrorism and other relevant Global Counter-Terrorism Co-ordination Compact entities to “jointly support innovative measures and approaches to building the capacity of Member States, upon their request, for the challenges and opportunities that new technologies provide, including the human rights aspects, in preventing and countering terrorism.”

In his report to the General Assembly on the Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy (A/77/718), the Secretary-General underscores that “[…] new and emerging technology offers unmatched opportunities to improve human welfare and new tools to counter terrorism. […] Despite strengthened and concerted efforts, responses by the international community often lag behind. Some of these responses unduly limit human rights, in particular the rights to privacy and to freedom of expression, including to seek and receive information.”

Through the six reports contained in this compendium – the product of the partnership between the United Nations Counter-Terrorism Centre and the International Criminal Police Organization under the CT TECH joint initiative, funded by the European Union – we seek to support Member States’ law enforcement and criminal justice authorities to counter the exploitation of new and emerging technologies for terrorist purposes and to leverage new and emerging technologies in the fight against terrorism as part of this effort, in full respect of human rights and the rule of law.

Our Offices stand ready to continue to support Member States and other partners to prevent and counter terrorism in all its forms and manifestations and to take advantage of the positive effects of technology in countering terrorism.

**Vladimir Voronkov**

Under-Secretary General
United Nations Office of Counter-Terrorism
Executive Director
United Nations Counter-Terrorism Centre

**Stephen Kavanagh**

Executive Director
Police Services
INTERPOL

# Acknowledgements

This document has been developed through the contributions and review by a wide range of stakeholders. Specifically, the United Nations Office of Counter-Terrorism (UNOCT) wish to acknowledge the contribution made by:

- **Ms. Cecilia Naddeo –** Legal Officer and Criminal Justice Coordinator
  Counterterrorism Executive Directorate (CTED)

- **Mr. Winthrop Wells –** Program Manager
  The International Institute for Justice and the Rule of Law (IIJ)

- **Ms. Marie Paulus –** Staff Officer, Emerging Security Challenges Division, Counterterrorism Section
  NATO

- **Mr. Adrien Vincart –** Digital Forensic Expert
  UNITAD

# Terms and Definitions

**Artificial Intelligence**

Generally understood to describe a discipline concerned with developing technological tools exercising human qualities, such as planning, learning, reasoning, and analyzing.

**Battlefield**

For the purpose of this document, battlefield refers to the description of an environment in which counterterrorism actions take place and in which military personnel might be the first responders due to ungoverned or under-governed aspects of the area.

For the purpose of this document, the use of battlefield illustrates the difference between a regular crime-scene and the special circumstances under which first responders need to operate and adjust their activities in line with their original mandate. The use of the term "battlefield" in this document does not intend to affect any definitions used by national or regional organizations and legislations.

**Chain of custody**

Chronological records of how the evidence was seized and handled. Any record should at least include what information was seized, when, and by whom, who handled the information, and when it was transferred to law enforcement agencies or a court.[1]

[1] CTED Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences (2019) https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_military_evidence_guidelines.pdf

| | |
|---|---|
| **Criminal justice process** | A legal process to bring about terrorism charges against an individual or an entity and the legal court hearing, ruling or judgement of the case and sentencing of the conviction |
| **Digital devices** | Electronic devices that store or process information electronically. Examples of digital devices include but are not limited to smartphones, laptops, tablets, external hard drives, remote storage, unmanned aerial systems, shipborne equipment. Digital devices may contain various types of electronic information, such as documents, images, videos, audio recordings, system information, logs and meta data. |
| **Digital forensics** | A branch of forensic science that focuses on identifying, acquiring, processing, analyzing, and reporting on information stored electronically. The main goal of digital forensics is to extract data from electronic device, process it into actionable intelligence and present the findings for prosecution. All processes utilize sound forensic techniques to ensure the findings are admissible in court.[2] |
| **Electronic evidence** | Evidence is a formal term for information that forms part of a trial in the sense that it is used to prove or disprove the alleged crime. All evidence is information, but not all information is evidence. Information is thus the original, raw form of evidence.[3] Electronic form of evidence is any information electronically stored that can potentially be used as evidence in court or legal proceedings. |
| **Faraday bags** | A Faraday bag is an enclosure made of a conductive material, such as metal mesh, that blocks electromagnetic fields. This makes it ideal for protecting electronic devices from radio frequency interference. Faraday bags are often used to protect mobile phones, laptops, and other sensitive devices from being hacked or tracked. |
| **First responders** | Individuals or groups of designated bodies who arrive to a scene of a terrorist attack after or together with emergency personnel and are designated to collect digital devices or who are designated to collect digital devices as part of their counterterrorism mandate. This term does not apply to emergency personnel, including firefighters and medical personnel.<br>For the purpose of this document, the first responders are any military or civilian personnel of a national, regional or international governmental organization who are the first to arrive on a terrorism crime scene and whose mandate allow for the collection of digital devices. Personnel of non-governmental organizations can also be present in the battlefield and collect digital devices, but they are not considered as first responders for the purpose of this document. |
| **Intelligence** | The product resulting from collection, development, analysis, interpretation and dissemination of information gathered from a wide range of sources, in accordance with the fundamental human rights principles, to inform decision makers for planning purposes and to take decisions or actions on strategic, operational or tactical level. |
| **Investigations** | The process of collecting information (or evidence) to determine if a crime has been committed; identify the perpetrator and to provide evidence to support the prosecution in legal proceedings. |

[2] INTERPOL – Digital Forensics https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics

[3] CTED Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences (2019) https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_military_evidence_guidelines.pdf

| | |
|---|---|
| **Law enforcement actions** | Typically describes law enforcement actions, based on legal authority, taken against a threat, which may include detaining individual(s), disrupting threat actor activities (i.e. content removal, asset seizures), etc. |
| **Live triage** | For the purpose of this document, the process of on-site evaluation, assessment, and prioritization of digital devices or storage media for further examination and analysis by accessing and digitally searching information stored on a working device on-site, in order to copy relevant information stored on it or determine if this data container is relevant to the counterterrorism investigation, without fully copying all the data stored on the device. |
| **New technologies** | While the new technologies terminology covers a wide range of different technologies[4], for the purpose of this document new technologies refer to the use and abuse of such new technologies as the Internet, social media, cryptocurrencies, facial recognition and darknet.[5] |
| **Prosecution / adjudication** | A legal process to bring about terrorism charges against an individual or an entity and the legal court hearing, ruling or judgement of the case and sentencing of the conviction. |
| **Rehabilitation** | In a criminal justice context, the term "rehabilitation" is used to refer to interventions managed by the corrections system with the aim to change the offender's views or behaviour to reduce the likelihood of re-offending and prepare and support the reintegration to society. |
| **Reintegration** | A comprehensive process of integrating a person back into a social and/or functional setting. |
| **Triage** | The process of on-site evaluation, assessment and prioritization of digital devices or storage media for further examination and analysis. This is often the first step on-site for a digital forensic investigation and assists investigators in finding relevant data containers quickly.<br>For the purpose of this document, triage involves identification and prioritization of digital devices in the battlefield for collection based on factors such as their value for counterterrorism investigations and the value of stored data.<br>For the context of this document, triage does not include live processes or access to the data on the device by first responders.[6] |
| **Terrorism** | For the purpose of this document, terrorism is defined as criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism. |
| **Zettabyte** | One zettabyte is equal to one billon terabytes. |

[4] Artificial intelligence, Internet of things, block chain technologies, crypto-assets, drones and unmanned aerial systems, DNA, fingerprints, cyber technology, facial recognition, 3D printing.

[5] CT TECH Project Document – Annex I Description of the Action.

[6] For more details on live triage with on-site access to the data of a device, see INTERPOL Guidelines for Digital Forensics First Responders, March 2021 https://www.interpol.int%2Fcontent%2Fdownload%2F16243%2Ffile%2FGuidelines_to_Digital_Forensics_First_Responders_V7.pdf. For more information on the evolution of digital triage, see Carrier, B. (2011). Digital triage forensics: A field guide for first responders, Syngress.

# Executive Summary

Battlefield requires personnel to operate in complex and constantly evolving environments. The dynamics of the battlefield are often characterized by urgency, uncertainty, chaos, and high levels of risk. Battlefield illustrates the difference from a regular crime-scene and the special circumstances under which first responders operate and adjust their activities in line with their original mandate. For the purpose of this report, first responders are understood as any military or civilian personnel of a national, regional or international governmental organization who are the first to arrive on a terrorism crime scene and whose mandate allow for the collection of digital devices. Personnel of non-governmental organizations can also be present in the battlefield and collect digital devices, but they are not considered as first responders for the purpose of this document.

Counterterrorism in the battlefield presents a range of key challenges for first responders. Collection of digital devices in the battlefield for evidentiary purposes is one of such new and unfamiliar challenges.

If first responders lack knowledge and awareness of the risks and good practices of collecting digital devices, their actions during collection and handling of digital devices in the battlefield may cause potential harm to their safety, safety of other people and surroundings, and may harm criminal proceedings against terrorist offences.

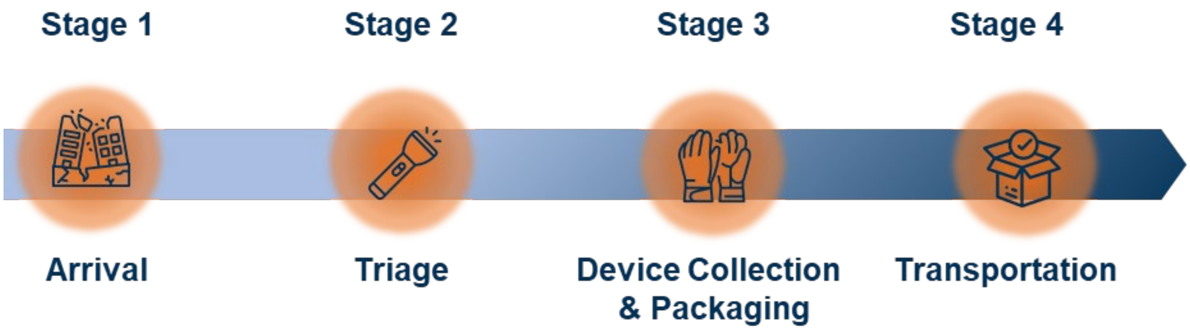
The purpose of this document is to provide practical guidance for first responders on collection of digital devices in the battlefield for investigation, prosecution and adjudication of terrorist offences. The document outlines practical and technological aspects and principles that the first responders should know and adhere to in order to maintain their safety, the safety of others, and to ensure authenticity and reliability of the digital devices as evidence.

The document outlines the actions that first responders need to take in the battlefield to ensure that their safety and security as well as the safety and security of others is maintained, digital devices found at the scene are handled and collected, and the required actions are taken before devices arrive at a forensic laboratory for further exploitation, in a way which ensures that information and data contained in devices is admissible as evidence in criminal proceedings.

This practical guide is targeted at first responders, who have a very limited knowledge or expertise in collection of digital devices or in digital evidence but are tasked with collection of digital devices in the battlefield for counterterrorism purposes.

The guide is structured around four stages related to collection of digital devices in the battlefield for criminal proceedings: (1) arrival at the scene; (2) triage of digital devices; (3) collection and packaging of digital devices; and (4) transportation of the devices out of the scene.

FIGURE 1



To assist first responders, the document provides a list of suggested actions for each stage, along with specifications and appendix templates.

# [ I ]
# Background

## 1.1 Overview

United Nations Member States attach great importance to addressing impact of new technologies in countering terrorism. During the seventh review of the of the United Nations Global Counter-Terrorism Strategy (A/RES/75/291)[7] in July 2021, Member States expressed their deep concern about *"the use of the Internet and other information and communications technologies, including social media platforms, for terrorist purposes, including the continued spread of terrorist content,"* and requested the Office of Counter-Terrorism and other Global Counter-Terrorism Compact entities *"to jointly support innovative measures and approaches to build the capacity of Member States, upon their request, for the challenges and opportunities that new technologies provide, including the human rights aspects, in preventing and countering terrorism".* Security Council resolutions 2178 (2014)[8] and 2396 (2017)[9] call for Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology and communications for terrorist acts. Security Council Resolution 2396 (2017) also encourages Member States **to enhance cooperation with the private sector, especially with information communication technology companies**, in gathering digital data and evidence in cases related to terrorism.

In its 30th Report to the United Nations Security Council[10], the Analytical Support and Sanctions Monitoring Team noted that "*Many Member States highlighted the evolving role of social media and other online technologies in the financing of terrorism and dissemination of propaganda*", with platforms cited by Member States include Telegram, Rocket.Chat, Hoop and TamTam, among others. **ISIL supporters using platforms on the darknet** for storing and accessing training materials that other sites decline to host as well as **for acquiring new technologies** were also cited in the report.

Countering the use of new and emerging technologies for terrorists purposes was discussed at the dedicated special meeting of the United Nations Security Council's Counter-Terrorism Committee's

[7] The United Nations Global Counter-Terrorism Strategy: Seventh Review Resolution (A/RES/75/291), N2117570.pdf (un.org)
[8] Security Resolution 2178 (2014), S/RES/2178%20(2014) (undocs.org)
[9] Security Resolution 2396 (2017), http://undocs.org/S/RES/2396(2017)
[10] Thirtieth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2610 (2021) concerning ISIL (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities S/2022/547 (undocs.org)

(CTC), which took place on 28-29 October 2022 in New Delhi and resulted in the adoption of a non-binding document, known as the Delhi Declaration[11].

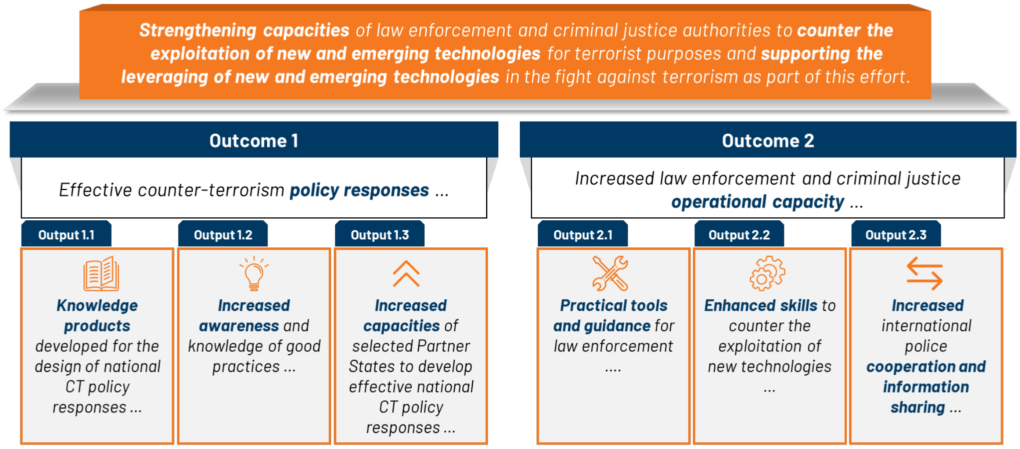
The CTC noted "***with concern the increased use, in a globalized society, by terrorists and their supporters of the Internet and other information and communication technologies****, including social media platforms, for terrorist purposes*" and acknowledged "***the need to balance fostering innovation and preventing and countering the use of new and emerging technologies, as their application expands, for terrorist purposes***", while emphasizing "***the need to preserve global connectivity and the free and secure flow of information*** *facilitating economic development, communication, participation and access to information*".

## 1.2 CT TECH Initiative

CT TECH is a joint UNOCT/ UNCCT and INTERPOL initiative, implemented under the UNOCT/UNCCT Global Counter-Terrorism Program on Cybersecurity and New Technologies. It is aimed at strengthening capacities of law enforcement and criminal justice authorities in selected Partner States to counter the exploitation of new and emerging technologies for terrorist purposes, as well as support Partner States' law enforcement agencies in leveraging new and emerging technologies in the fight against terrorism.

To achieve the overall objective, the CT TECH initiative implements two distinct outcomes with six underpinning outputs.

**FIGURE 2**


Strengthening capacities of law enforcement and criminal justice authorities to counter the exploitation of new and emerging technologies for terrorist purposes and supporting the leveraging of new and emerging technologies in the fight against terrorism as part of this effort.
Outcome 1
Effective counter-terrorism policy responses ...
Output 1.1
Knowledge products developed for the design of national CT policy responses ...
Output 1.2
Increased awareness and knowledge of good practices ...
Output 1.3
Increased capacities of selected Partner States to develop effective national CT policy responses ...
Outcome 2
Increased law enforcement and criminal justice operational capacity ...
Output 2.1
Practical tools and guidance for law enforcement ....
Output 2.2
Enhanced skills to counter the exploitation of new technologies ...
Output 2.3
Increased international police cooperation and information sharing ...

[11] The Delhi Declaration, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_special_meeting_outcome_document.pdf

Table 1: CT TECH Outcomes and Outputs

| Outcome 1: Effective counter-terrorism policy responses towards the challenges and opportunities of new technologies in countering terrorism in full respect of human rights and rule of law. | |
|---|---|
| **Output 1.1** | *Knowledge products developed for the design of national CT policy responses to address challenges and opportunities of new technologies in countering terrorism in full respect of human rights and rule of law is developed.* |
| **Output 1.2** | *Increased awareness and knowledge of good practices on the identification of risks and benefits associated with new technologies and terrorism in full respect of human rights and rule of law.* |
| **Output 1.3** | *Increased capacities of selected Partner States to develop effective national CT policy responses towards countering terrorist use of new technologies and leveraging new technologies to counter terrorism in full respect of human rights and rule of law.* |

| Outcome 2: Increased law enforcement and criminal justice operational capacity to counter the exploitation of new technologies for terrorist purposes and use of new technologies to prevent and counter terrorism in full respect of human rights and rule of law. | |
|---|---|
| **Output 2.1** | *Practical tools and guidance for law enforcement on countering the exploitation of new technologies for terrorist purposes and use of new technologies to prevent and counter terrorism in full respect of human rights and rule of law is developed.* |
| **Output 2.2** | *Partner States' law enforcement and criminal justice institutions have enhanced skills to counter the exploitation of new technologies for terrorist purposes and use of new technologies to counter terrorism in full respect of human rights and rule of law.* |
| **Output 2.3** | *Increased international police cooperation and information sharing on countering terrorist use of new technologies and using new technologies to counter terrorism.* |

# 1.3 Document Purpose and Use

The purpose of this document is to provide practical guidance for first responders on the collection of digital devices in the battlefield for subsequent investigation, prosecution and adjudication of terrorist offences. The document outlines practical and technological aspects and principles that the first responders should know and adhere to in order to maintain their safety, the safety of others, and to ensure authenticity and reliability of the digital devices as evidence.

## 1.3.1 Scope

The document outlines the actions that first responders are recommended to take in the battlefield to ensure that:

- their safety and security as well as the safety and security of others are maintained;
- any digital devices left in the battlefield are detected and adequately collected; and

- any collected devices are adequately handled until arrival at the forensic laboratory for further exploitation.

The overall aim is to ensure that information and data contained in devices is admissible as evidence in criminal proceedings.

Legal frameworks related to the use and admissibility of information collected in the battlefield as evidence in national criminal courts for terrorist offences' prosecution are addressed in the "*Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences"*[12] and should be developed to meet all the necessary legal conditions.

The document is not intended to be used by first responders as a reference guide for digital forensics methodology or as a framework of the chain of custody principles. The aim is to support first responders who are not experienced in collection and handling of digital devices by guiding them on how to collect and transport digital devices from the battlefield to a dedicated forensics laboratory.

### 1.3.2 Target Audience

This practical guide targets first responders, who have none or very limited knowledge or expertise in collection of digital devices or in digital evidence but are tasked with collection of digital devices in the battlefield for counter-terrorism purposes.

It is highly advisable to include digital forensics professionals as part of the first responders' teams, but the document considers a professional and technological gap that many Member States face and targets all personnel who might be tasked with first responders' functions and collection of digital devices in the battlefield.

### 1.3.3 Benefits

This document provides first responders with a clear and structured process to follow for collection of digital devices in the battlefield to support investigation, prosecution and adjudication of terrorist offences within criminal justice chain. Specifically, this guide can improve first responders' skills and preparedness by familiarizing them with the basic principles and requirements for collection of digital devices for evidentiary purposes, at the same time reducing the risks associated with personnel safety and security. By following the guidelines, first responders can increase their efficiency and compliance with the principles of the chain of custody, increase admissibility of the digital devices and digital information as evidence in counter-terrorism proceedings and successful prosecution of terrorist offences.

[12] Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences, developed by the Counter-Terrorism Committee Executive Directorate, 2019, cted_military_evidence_guidelines.pdf (un.org)

### 1.3.4 Limitations

This document does not provide guidance on the legal aspects related to collection of digital devices in the battlefield. The document assumes that all necessary legal conditions have been met and that first responders are acting in full respect of the rule of law. It is the court which determines the final admissibility of any evidence, including collected from digital devices found in the battlefield.

[ II ]

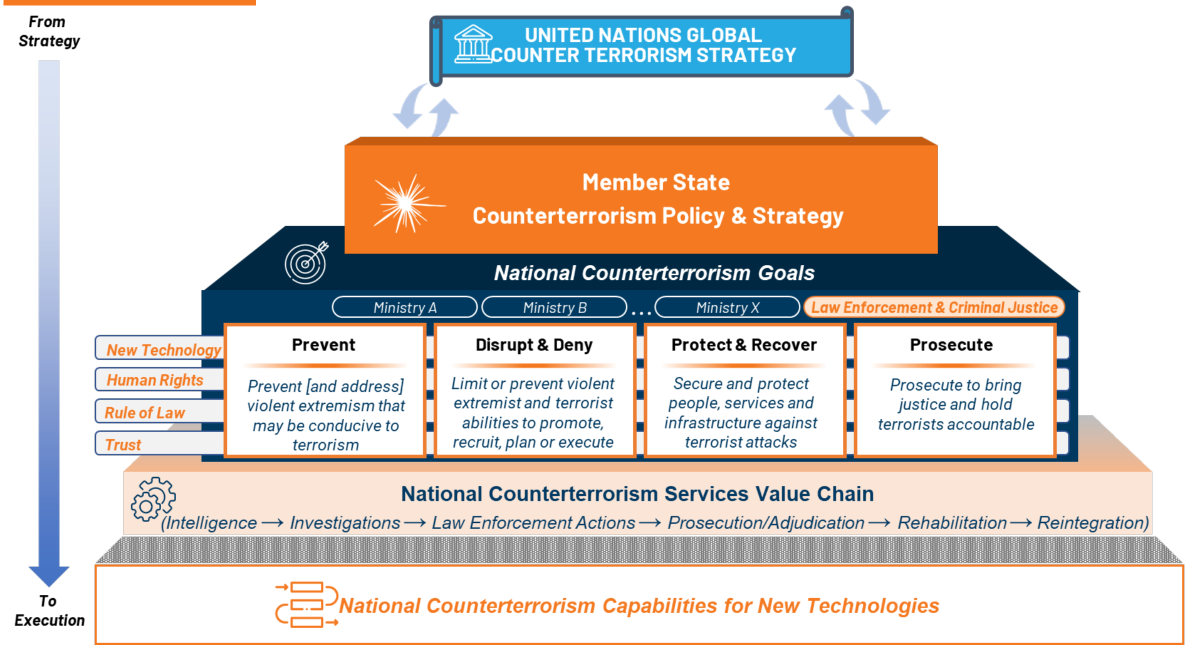
# Approach

## 2.1 Overview

The report seeks to support and enable Member States in finding an effective range of offered solutions for digital devices collection in the battlefield, which are aligned to the United Nations Global Counterterrorism Strategy and in full respect of human tights and the rule of law.

## 2.2 Guiding Framework

FIGURE 3


From Strategy
To Execution
UNITED NATIONS GLOBAL COUNTER TERRORISM STRATEGY
Member State Counterterrorism Policy & Strategy
National Counterterrorism Goals
Ministry A
Ministry B
...
Ministry X
Law Enforcement & Criminal Justice
New Technology
Human Rights
Rule of Law
Trust
Prevent
Prevent [and address] violent extremism that may be conducive to terrorism
Disrupt & Deny
Limit or prevent violent extremist and terrorist abilities to promote, recruit, plan or execute
Protect & Recover
Secure and protect people, services and infrastructure against terrorist attacks
Prosecute
Prosecute to bring justice and hold terrorists accountable
National Counterterrorism Services Value Chain
(Intelligence ⟶ Investigations ⟶ Law Enforcement Actions ⟶ Prosecution/Adjudication ⟶ Rehabilitation ⟶ Reintegration)
National Counterterrorism Capabilities for New Technologies

The guiding framework is a conceptual model that is intended to guide, align, and inform the development of the report. It seeks to ensure coherence from strategy to execution between the United Nations Global Counter Terrorism Strategy (GCTS) and a Member State's National Counterterrorism Policy and Strategy goals and outcomes, services, and capabilities from a law enforcement and criminal justice perspective, regarding new technologies.

The United Nations GCTS, adopted by the General Assembly, sets out broad actions for Member States to address terrorism threat, which are set out across four key pillars:

**Pillar I:** Measures to address the conditions conducive to the spread of terrorism

**Pillar II:** Measures to prevent and combat terrorism

**Pillar III**: Measures to build States' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in this regard

**Pillar IV**: Measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism

Member States are encouraged to develop their respective national counter-terrorism legal and policy frameworks in alignment with the United Nations GCTS. They must ensure that their respective counter-terrorism laws, policies, strategies and measures comply with their obligations under international law, including international human rights law, international refugee law and international humanitarian law. A Member State's national counter-terrorism legal and policy framework should broadly seek to prevent and address violent extremism that may be conducive to terrorism, prevent or limit terrorist activities, take appropriate measures to protect persons within the State's jurisdiction, services and infrastructure against reasonably foreseeable threats of terrorist attacks, and ensure that terrorists are held accountable for their actions.

To achieve the counter-terrorism outcomes and goals, Member States' national law enforcement and criminal justice authorities have a set of tools at their disposal. These include, but are not limited to:

**Table 2: High-level National Law Enforcement and Criminal Justice Services for Counterterrorism**

| Services | Description |
|---|---|
| ***Criminal justice process*** | *A legal process to bring about terrorism charges against an individual or an entity and the legal court hearing, ruling or judgement of the case and sentencing of the conviction.* |
| ***Intelligence*** | *The product resulting from collecting, developing, disseminating, analyzing, and interpreting of information gathered from a wide range of sources, in accordance with international human rights law, to inform decision makers for planning purposes to take decisions or actions – strategic, operational or tactical level.* |
| ***Investigations*** | *The process of collecting information (or evidence) to determine if a crime has been committed; identify the perpetrator and to provide evidence to support criminal justice proceedings.* |
| ***Law enforcement actions*** | *Typically describes law enforcement actions taken against a threat, which may include detaining individual(s), disrupting threat actor activities (i.e., content removal, asset seizures), etc.* |
| ***Rehabilitation*** | *In a criminal justice context, the term "rehabilitation" is used to refer to interventions managed by the corrections system with the aim to change the offender's views or behaviour to reduce the likelihood of re-offending and prepare and support the reintegration to society.* |

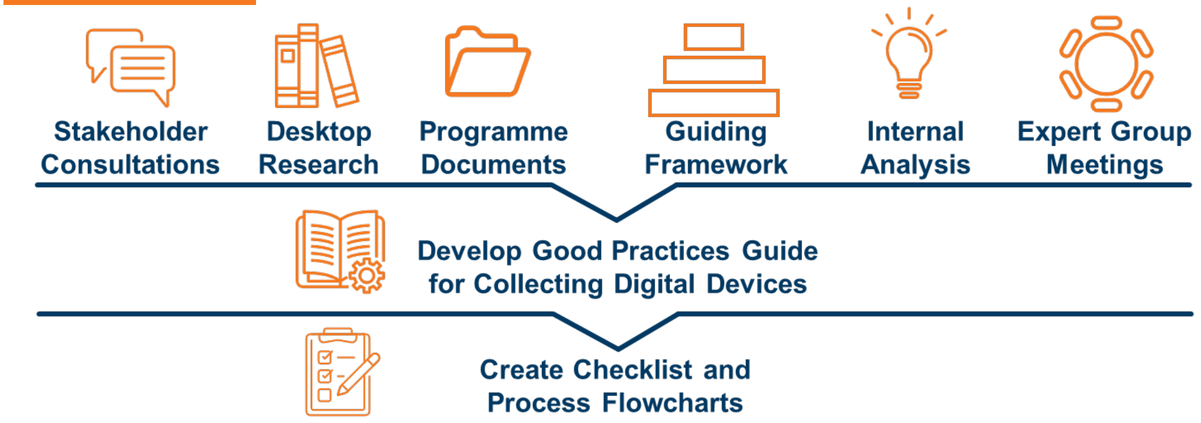
| | |
|---|---|
| ***Reintegration*** | *A comprehensive process of integrating a person back into a social and/or functional setting* |

The effective use and deployment of such services and tools is dependent on a set of underlying capabilities. The required capabilities to enable and deliver services are often defined and represented in a capability model. A capability model represents a functional decomposition of key functions into a logical and granular grouping which supports the execution of services and activities. The capability model informs the requirements across people (structure and skills), processes, technology, infrastructure, and finance.

The guiding framework serves to ensure alignment between strategy and execution from both 'top-down' and 'bottom-up'.

## 2.3 Methodology

FIGURE 4


Stakeholder Consultations
Desktop Research
Programme Documents
Guiding Framework
Internal Analysis
Expert Group Meetings
Develop Good Practices Guide for Collecting Digital Devices
Create Checklist and Process Flowcharts

This document was developed and informed by a wide range of inputs which include CT TECH project documents, stakeholder consultation, internal analysis, desktop research, expert group meetings, co-ordination with the United Nations Global Counter-Terrorism Co-ordination Compact entities, and the guiding framework as described above in section 2.2.

### 2.3.1 Expert Group Meetings and Consultation

This guide has been developed with inputs by experts through the Expert Group Meeting (EGM) sessions as well as individual consultations and review. The EGM brought together a group of experts and practitioners from counter-terrorism and law enforcement agencies, human rights, private sector, academia and civil society to discuss how to counter use of new technologies for terrorist purposes and use new technologies as part of this effort, identify good practices in this regard, and also discuss risks, challenges and not so good practices that require attention and caution. The guide was further refined through engagement with the United Nations Global Counter-Terrorism Coordination Compact and its Working Group on Emerging Threats and Critical Infrastructure Protection, which promotes coordination and coherence to support the efforts of Member States to prevent and respond to emerging terrorist threats, with respect for human rights and the rule of law as the fundamental basis, in line with international law, including human rights, humanitarian and refugee law.

### 2.3.2 Reference Document Review

The development of this guide was informed by, took into consideration, built upon, and complemented existing research, guidelines and publications – which includes the following:

**Table 3: References**

| | |
|---|---|
| **1** | *UN Counter-Terrorism Committee Executive Directorate (CTED), Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences ("Military Evidence Guidelines"), December 2019* |
| **2** | *The Global Counterterrorism Forum (GCTF), Abuja Recommendations on the Collection, Use and Sharing of Evidence for Purposes of Criminal Prosecution of Terrorist Suspects, September 2018* |
| **3** | *INTERPOL, Guidelines for Digital Forensics First Responders, Best Practices for Search and Seizure of Electronic and Digital Evidence, March 2021* |
| **4** | *Eurojust, Memorandum on Battlefield Evidence, September 2020* |
| **5** | *Eurojust, Casework on Counter-Terrorism: Insights 2020 – 2021, December 2021* |
| **6** | *Council of Europe, The Recommendation of the Committee of Ministers to Member States on the Use of Information Collected in Conflict Zones as Evidence in Criminal Proceedings Related to Terrorist Offences CM/Rec (2022)8, 30 March 2022* |
| **7** | Christian Braccini, Teemu Väisänen, Michal Sadloň, Hayretdin Bahşi, Agostino Panico, Kris van der Meij, Mario Huis in ‘t veld, NATO Cooperative Cyber Defence Centre of Excellence, Battlefield Digital Forensics Digital Intelligence and Evidence Collection in Special Operations, 2016 |
| **8** | US Department of State, Department of Justice, and the Department of Defense, US Non-Binding Guiding Principles on Use of Battlefield Evidence in Civilian Criminal Proceedings |
| **9** | The Geneva Academy of International Humanitarian Law and Human Rights, and the International Committee of the Red Cross (ICRC), Guidelines on Investigating Violations of International Humanitarian Law: Law, Policy, And Good Practice, September 2019 |

# [ III ]

# Introduction

## 3.1 Overview

As advancements in technology continue to accelerate, terrorists increasingly exploit these innovations to further their destructive agendas. The rapid proliferation of communication platforms, social media networks, encryption techniques, and emerging technologies pose significant challenges for law enforcement agencies. As terrorists increasingly leverage technology for communication, recruitment, and planning, digital footprints become valuable sources of information in uncovering their activities. Digital forensics involves the systematic collection, preservation, analysis, and presentation of digital evidence, allowing investigators to reconstruct events, identify perpetrators, and dismantle terrorist networks. This guide seeks to provide guidance on the collection and handling of digital devices in a manner that minimizes the disruption of such device in its current state that may contain valuable information. This proactive approach not only aids in preventing terrorist attacks but also supports the prosecution of individuals involved in terrorist activities.

## 3.2 New Technologies and Counterterrorism

Today, the advancements of digital technologies, data, and the Internet have led to a hyperconnected world where information is accessed, shared, and received nearly instantaneously. As of 2022, nearly 70% of the global population uses the Internet[13], of which over 93 percent are social media users[14]. Globally, it is estimated that in 2022 over 97 zettabytes[15] of information was generated[16]. Whilst such technology advancements provide the opportunity to transform society for the greater good, terrorist actors are taking advantage of the same technology for their own nefarious purposes. Use of new technologies for terrorist purposes poses significant challenges to Member States in countering terrorism – in particular – the use of technologies that allow for anonymity and the ability to coordinate and operate remotely.

[13] ITU Global Connectivity Report 2022, https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/index/
[14] Domo Data Never Sleeps, Data Never Sleeps 10.0 | Domo
[15] 1 zettabyte equals to 1 billion terabytes.
[16] Statista, Total data volume worldwide 2010-2025.

On the other hand, new technologies present significant opportunities as a capability multiplier for counterterrorism and law enforcement agencies. For example, such technologies can enable law enforcement agencies to do more with less, fast track timely decision making, generate new insights, and conduct disruptive operations remotely.

Countering the use of new technologies for terrorist purposes hinges on understanding how terrorist actors are using new technologies, developing effective legal framework and policy responses, and building operational capacity to counter use of such technologies for terrorist purposes, to include leveraging and adopting the use of new technologies.

### 3.2.1 Challenges –Use of New Technologies for Terrorist Purposes

Advances in Information and Communication Technologies and their availability have made it attractive for terrorist and violent extremist groups to exploit the Internet and social media to facilitate a wide range of activities, including incitement, radicalization, recruitment, training, planning, collection of information, communication, preparation, propaganda, and financing. For their purposes, terrorist groups also expertly exploit and manipulate gender inequalities, norms and roles, including violent masculinities. For example, Da'esh skillfully recruited women through social media, adapting their messages to appeal to women speaking different languages and living in different social, economic and cultural contexts in Western Europe, Central Asia, and Middle East and North Africa, often tapping into women´s experience of gender inequalities. Terrorists also use encrypted communications and the darknet to share terrorist content, expertise, such as designs of improvised explosive devices and attack strategies, as well as to coordinate and facilitate attacks and procure weapons and counterfeit documents. Meanwhile, developments in the fields of artificial intelligence, machine learning, 5G telecommunications, robotics, big data, algorithmic filters, biotechnology, self-driving cars and drones may suggest that once these technologies become commercially available, affordable, and convenient to use, they could also be misused by terrorists to expand the range and lethality of their attacks.

### 3.2.2 Opportunities – CT Law Enforcement

New technologies present endless opportunities for law enforcement agencies to effectively counter terrorism while upholding responsible practices with respect to international human rights law. Law enforcement can harness new technologies to detect, investigate, prosecute, and adjudicate terrorist activities in new and more effective ways.

Open-source intelligence enables quick collection of information about targets of interests, which can make law enforcement activities more effective. Advanced data analytics and artificial intelligence (AI) capabilities allow for the processing and analysis of vast amounts of information, enabling law enforcement to identify patterns, detect potential threats, and preemptively respond to terrorist activities. Advanced surveillance systems, including facial recognition and biometric technologies, aid in the identification and tracking of suspects, enhancing the efficiency of investigations, preventing potential attacks, and prosecuting terrorists. Furthermore, digital forensics tools assist in extracting critical evidence from electronic devices, enabling law enforcement to uncover hidden connections, disrupt terrorist networks and prosecute terrorists.

Leveraging new technologies can help prioritize limited law enforcement resources in a more effective way. However, it is crucial that these technologies are employed ethically and with strict adherence to privacy, human rights, and rule of law. Transparency and accountability measures must be in place to ensure responsible use and prevent any potential misuse of these powerful tools. Additionally, comprehensive training programs should be implemented to equip law enforcement personnel with the necessary skills to leverage new technologies effectively and within the boundaries of legal and ethical frameworks. By leveraging new technology responsibly, law enforcement can significantly enhance their counter-terrorism efforts and safeguard the safety and security of communities.

### 3.2.3 Human Rights and New Technologies

Terrorism poses a serious challenge to the very tenets of the rule of law, the protection of human rights and their effective implementation. It can destabilize legitimately constituted governments, undermine pluralistic civil society, jeopardize peace and security, and threaten social and economic development. States have the obligation to take appropriate measures to protect persons within their jurisdiction against reasonably foreseeable threats of terrorist attacks. States' duty to safeguard human rights includes the obligation to take necessary and adequate measures to prevent, combat and punish activities that endanger these rights, such as threats to national security or violent crime, including terrorism. All such measures, must themselves be in line with international human rights law and rule of law standards.

In the context of employing new and emerging technologies to counter terrorist activities , States have to ensure that relevant laws, policies and practices respect rights such as the right to privacy, the rights to freedom of expression, freedom of association, freedom of thought, conscience and religion, the right to liberty and security of the person, the right to fair trial, including the presumption of innocence as well as the principle of non-discrimination. States must also uphold the absolute prohibition of torture and cruel, inhuman or degrading treatment or punishment.

The UN, Interpol and the EU have repeatedly underlined the interrelationship between new technologies, counter-terrorism, and human rights, including gender equality. The UN Global Counter-Terrorism Strategy and various General Assembly and Security Council resolutions underscore Member States' obligations under international human rights law, international humanitarian law, and international refugee law when countering terrorism. In particular, the UN's counter-terrorism strategy recognizes that "effective counter-terrorism measures and the protection of human rights are not conflicting goals, but complementary and mutually reinforcing" and requires measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism. Specifically, the Strategy encouraged Member States to address the use of the Internet and other information and communications technologies, including social media platforms, for terrorist purposes, including the continued spread of terrorist content while respecting international law, including international human rights law, including the right to freedom of expression.

# [ IV ]

# Collection of Digital Devices in the Battlefield

## 4.1 Overview

This chapter introduces the concept of battlefield digital information and provides a practical guidance to first responders on how to collect and handle digital devices in the battlefield and transport them to a forensic lab in such a way that ensures safety and security of first responders, other people and surroundings as well as evidentiary value of the devices (and information retrieved from them) for potential use in criminal proceedings.

As technology continues to evolve rapidly, it is essential that the potential impact of new advancements on the practices and procedures suggested in this document are considered by first responders in the application of this guide.

The guide is structured around four stages required for the adequate collection of digital devices in the battlefield to enable their admissibility in subsequent criminal proceedings: (1) arrival at the scene; (2) triage of digital devices; (3) collection and packaging of digital devices; and (4) transportation of the devices out of the scene.

Each stage includes a list of suggested actions for first responders and their descriptions:

- Actions marked as **MUST** are mandatory for first responders in order to preserve the evidentiary value of digital device or when the action needs to be completed before moving on to the next action.
- Actions marked as **SHOULD** are recommended actions and best practices to be followed by first responders to fully comply with digital forensics methodologies. Exceptions can be made when the time required to perform these actions might endanger first responders or other personnel.

- Actions marked as, **IF POSSIBLE**, are suggested best practice to be followed by first responders but are not mandatory and will not affect admissibility of digital devices as evidence in criminal proceedings.

By following the recommendations provided by this guide, first responders will ensure that digital devices collected in the battlefield and their output can be used in criminal proceedings as evidence.

These guidelines should be implemented in accordance with security or safety protocols that the first responders follow. If the team suspects the existence of explosives or booby-trapped devices on-site, the team MUST obey their protocol for actions on explosion hazard scene.

## 4.2 Battlefield Digital Information

The rapid proliferation of digital devices and advancements in information and communication technologies have provided terrorists and terrorist organizations with new tools for recruitment, financing, training, planning, and executing attacks, including cyber-attacks. These actions frequently leave digital traces on the devices used, documenting their activities, including their activities on the Internet and communication activities.

Digital information can help to prevent terrorists acts and terrorist activities, identify perpetrators, uncover evidence of their activities, identify their supporters and bring them to justice. Member States are encouraged to use digital information collected in the battlefield as digital evidence for investigation, prosecution and adjudication of terrorist offences. Guidelines and recommendations have been developed to facilitate collection, use and sharing of such evidence, including, but not limited to the Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences ("Military Evidence Guidelines")" [17], developed by the United Nations Counter-Terrorism Committee Executive Directorate (CTED) and the Global Counterterrorism Forum (GCTF) Abuja Recommendations on the Collection, Use and Sharing of Evidence for Purposes of Criminal Prosecution of Terrorist Suspects ("The Abuja recommendations")[18].

Information and evidence contained in digital devices is volatile, easily altered, damaged, or destroyed, it is also time-sensitive, and not bound by territorial jurisdictions. Digital information can be easily manipulated or deleted without any trace.

Battlefield environment presents additional challenges when it comes to collecting, handling and preserving digital devices and ensuring that information contained in them can be used and be

[17] UN Counter-Terrorism Committee Executive Directorate (CTED), Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences ("Military Evidence Guidelines"), 09 December 2019.

[18] The Global Counterterrorism Forum (GCTF), Abuja Recommendations on the Collection, Use and Sharing of Evidence for Purposes of Criminal Prosecution of Terrorist Suspects, September 2018.

admissible as evidence in courts, especially when digital forensics expertise is not available and there are safety and security risks involved.

First responders' actions related to collection and handling of a digital device found in the battlefield are especially important and, in many cases, determine whether information contained in a device is admissible as evidence in criminal proceedings on counter-terrorism cases.

The Abuja recommendations recognize this particular challenge of ensuring that the information retrieved by the military and other acknowledged actors in (post-) conflict situations meet the legal thresholds to be allowed as evidence in criminal proceedings, according to the legal system of different states. The strict legal criteria that are laid down in the national criminal codes, which include the admissibility of evidence, preservation of the chain of custody and evidence, and respect for fair trial principles, need to be met.[19]

This chapter introduces to the unique circumstances and challenges related to the collection of digital devices by first responders in the battlefield, and the use of the information contained in those digital devices as admissible evidence for legal proceedings related to terrorism offences.

### 4.2.1 Battlefield and Digital Devices

Battlefield requires personnel to operate in complex and constantly evolving environments. The dynamics of the battlefield are often characterized by urgency, uncertainty, chaos, and high levels of risk. Counterterrorism in the battlefield is characterized by the need to quickly identify and neutralize terrorist threats while minimizing collateral damage and preserving the safety of civilians and the surroundings, in full respect of human rights and the rule of law. Sometimes, it also entails collection of digital devices found in the battlefield, which may contain data and information important or relevant for investigation, prosecution and adjudication of terrorist offences.

### 4.2.2 Battlefield Actors

For the purpose of this document, battlefield is understood as an environment in which counterterrorism actions take place and in which military personnel might be the first responders due to ungoverned or under-governed aspects of the area. First responders often include military personnel, but can also include civilian personnel of national, regional and international organizations mandated to counter terrorism. Personnel of non-governmental organizations can also be present in the battlefield.

Battlefield illustrates the difference from a regular crime-scene and the special circumstances under which first responders operate and adjust their activities in line with their original mandate.

For the purpose of this report, the first responders are understood as any military or civilian personnel of a national, regional or international governmental organization who are the first to arrive on a

[19] *ibid*, p.17 on V. Recommendations on the Collection, Use and Sharing of Evidence by the Military

terrorism crime scene and whose mandate allow for the collection of digital devices. This term does not apply to emergency personnel, including firefighters and medical personnel.

First responders' actions and role in collecting digital devices in the battlefield are of paramount importance to ensure that devices collected are admissible as evidence in criminal justice procedures and they need to be aware of consequences related to mishandling collection and transportation of digital devices on and from the battlefield.

### 4.2.3 Informational Value – Intelligence vs Evidence

Digital information has become a crucial source of intelligence for military and evidence for law enforcement agencies. Digital information collected in the battlefield can be used as intelligence driving counterterrorism efforts and as evidence in criminal proceeding against terrorists.

Use of digital information for intelligence or other military purposes does not involve the criminal justice system and does not fall within the scope of this report. This document focuses on the use of digital information as evidence in criminal proceedings against terrorist offences and legal thresholds that should be met, including the admissibility of evidence, preservation of the chain of custody and evidence, and respect for fair trial principles.[20]

### 4.2.4 Key Challenges

Counterterrorism in the battlefield presents a range of key challenges for first responders. Collection of digital devices in the battlefield for law enforcement and legal proceeding purposes is one of such new and unfamiliar challenges.

If first responders lack knowledge and awareness of the risks and good practices of collecting digital devices, their actions during collection and handling of digital devices in the battlefield:

- may cause potential harm to their safety, safety of other people and surroundings, and
- may affect the admissibility of information contained in digital devices as evidence in criminal proceedings against terrorist offences.

For example, Unmanned Aircraft Systems (UAS) are digital devices, which first responders may be tasked to collect in the battlefield. Terrorists can booby-trap an UAS to target first responders who are trying to open the device in the battlefield or can use it for a secondary attack once first responders had arrived at a blast site. In 2016, an UAS blew up when military personnel tried to process it after it allegedly crashed to the ground, which killed two soldiers and injured two more.

First responders must be aware of the potential risks associated with digital devices left in the battlefield, such as explosion hazards, adversaries tracking capabilities, and other means that can compromise their safety.

[20] *ibid*, p.17 on V. Recommendations on the Collection, Use and Sharing of Evidence by the Military

For the information extracted from digital devices collected in the battlefield to be used as evidence in criminal proceedings, first responders need to adhere to a set of digital forensics requirements to maintain the chain of custody and to ensure its admissibility as evidence.

Proper documentation of the scene, of the digital device and the actions taken to collect and handle the device until it is handed for preservation or to a forensics lab ensures maintenance of the chain of custody and admissibility of the digital device and information as evidence.

First responders operating in the battlefield often lack training, experience and resources to address proper documentation requirements and may tamper with digital devices and render them inadmissible as evidence. For example, switching a digital device on or off or accessing its content would alter the source of the evidence.

## 4.3 Guiding Principles

These guiding principles form the core of the document and the guidance developed for collection of digital devices in the battlefield.

Table 4: Guiding Principles

| Guiding Principles | |
|---|---|
| ***Cause No Harm*** | *To maintain the safety of the team, its surroundings, the device and investigative systems, act with caution when approaching, touching, altering or connecting the digital device found in the battlefield to networks or investigation systems.* |
| ***Reliability*** | *For a digital device to be admissible as evidence, one should demonstrate that the information retrieved from it can be re-generated. Therefore, actions made on a digital device onsite can affect its reliability and change dates or other artifacts stored on the device. For example, "unread messages".* |
| ***Integrity*** | *For information retrieved from a digital device to be considered as evidence, one should demonstrate that the data has not been tampered with or modified in any way that would alter its meaning or context.* |
| ***Authenticity*** | *Authenticity refers to the assurance that the digital evidence has not been tampered with or altered in any way, and that it is what it purports to be. This is an important part of the admissibility of the device and the information stored in it. In some cases, alteration of the device is necessary to collect the digital device, and the procedure and actions must be documented.* |
| ***Credibility*** | *Trustworthiness and believability of the digital evidence in the eyes of the court or the jury. Credible evidence is one that is supported by other facts and evidence and can be accepted as truthful.* |

| | |
|---|---|
| ***Respect to the Chain of Custody*** | *Admissibility of a digital device as evidence refers to whether the evidence collected from a digital device meets the legal requirements for admissibility in court. Admissibility criteria may vary by jurisdiction, but generally, the evidence must be relevant, material, obtained legally, and the chain of custody must be maintained.* |

[V]

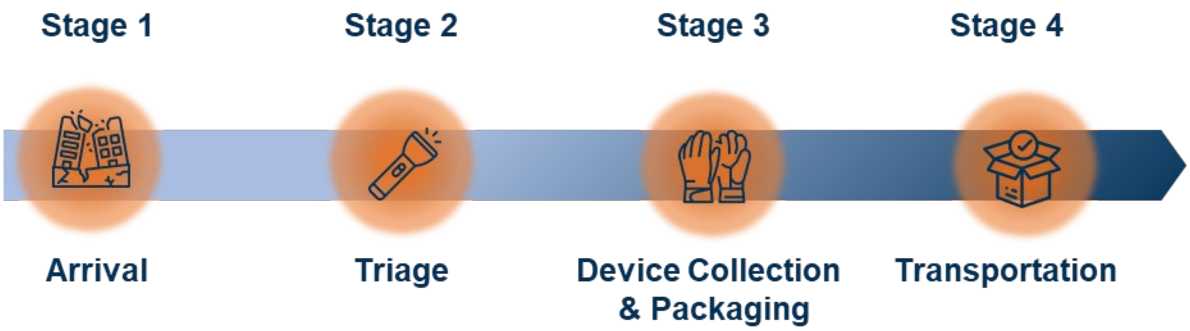
# Collection of Digital Devices in the Battlefield

## 5.1 Overview

This chapter will provide practical guidelines to first responders for the collection of digital devices in the battlefield in such a way that is minimizing disruption and ensuring the integrity of digital devices that may contain valuable information, including potentially incriminating evidence, that court can find admissible in the legal proceedings. The guide will cover four key stages:

- Stage 1 – Arrival at the Scene
- Stage 2 – Triage
- Stage 3 – Device Collection and Packaging
- Stage 4 – Transportation

FIGURE 5



## 5.2 Stage 1 – Arrival at the Scene

### 5.2.1 Planning and Preparation

Advance planning can significantly improve the ability and the efficiency of first responders collecting digital devices in the battlefield and improve the triage of digital devices at the scene. Preparations can increase productivity of first responders in collecting digital devices and reduce time required to spend on site and to be exposed to security threats.

**If possible**, during planning and preparation, first responders define priorities in terms of what relevant digital devices shall be collected first, identify technical support available on-site and what additional technical personnel and equipment might be required. For a list of a priority digital devices to be collected please refer to Annex I.

### 5.2.2 Arrival at the Scene

Upon the arrival at the scene, first responders **MUST** take a few quick actions that are imperative to their safety and safety of other people, and which are sometimes referred to as "site exploitation":

First responders **MUST** scan the site for potential hazards, and identify real-time transmitting digital devices and.

It is **RECOMMENDED** to document the scene, unless there is an imminent danger to safety and security of first responders, other people and surroundings and conduct a quick assessment of it.

Table 5: Summary Actions

| Action | Purpose | Level of Importance |
|---|---|---|
| *1. Scanning the site* | *Security Measure* | *MUST* |
| *2. Identify real-time transmitting digital devices* | *Security Measure* | *MUST* |
| *3. Documentation* | *Documentation* | *SHOULD* |
| *4. Quick Scene Assessment* | *Handling* | *SHOULD* |

### 5.2.3 Scanning the site

Box 1

**This action MUST be completed before entering the site and shall be the first action upon arrival.**

**Note:** Scanning the site can be combined with the next action of identifying real-time transmitting digital devices (see 5.2.4 below).

Digital devices left on the scene by terrorists might pose a physical threat to personnel working at the scene and its surroundings. There have been cases when terrorists planned a tandem attack, which targeted the team working on-site, their platforms and technology tools.

Digital devices can be boobytrapped and be exploded by terrorists using sensors that recognize the team's approach, by physical contact with a digital device, when first responders touch or lift the device, or by remote control, when the area or the device is monitored by the terrorists. Quickly locating electronic data storing devices can be valuable for further exploitation.

A non-exhaustive list of devices to scan the site for include:

- Cameras (active or non-active)
- UAS (flying, on or off)
- Sensors
- Network equipment: routers, servers, network cables
- Computers
- Tablets
- Cellular phones
- Memory cards
- Thumb drives
- Digital storage devices

#### a. Purpose

- To ensure security and safety of first responders, other personnel, individuals, and surroundings.
- To understand the number of digital devices to be collected.

### b. Actions

Visually scan or screen the site to locate visible digital devices without actually entering the scene.

### c. Results

After completion of the scanning of the site, first responders will be able to identify safety and security hazards stemming from digital devices left on the scene, their technological complexity and possibility of remote site monitoring by terrorists. The presence of cameras, UAS, sensors and network devices would be an indication of possible remote activation of the devices located and first responders should not enter the scene before it is cleared safe for entering by relevant personnel.

Also, first responders will understand an amount and type of digital devices to be collected on the scene.

## 5.2.4 Identify real-time transmitting digital devices & booby-trapped devices

Terrorists can remotely monitor sites in the battlefield and take action against first responders remotely, without awareness of first responders. This poses a threat to safety of first responders, other people and surroundings and to the data that can be found on-site. Real-time transmitting digital devices, which are connected and active in the battlefield, might alert terrorists of the arrival of the first responders to the scene and allow them to execute an attack.

Online data storing digital devices, such as cellphones, tablets, and computers can also be remotely manipulated by terrorists and exploded, or terrorists may remotely connect to them to delete or encrypt data.

Flying UAS can be an indication that its operator is nearby. As part of the “Quick assessment” action (see 5.2.6 below), the team **SHOULD** consider calling an UAS expert and perform a proximity search to locate the real-time UAS pilot.

Please note that as technology progresses, this indication of a nearby operator should be reassessed and not taken for granted.

Transmitting cameras can record the first responders’ actions and be used against them not only in real-time but also as a measure to learn about the team’s tactical actions and must be avoided. Searching for active cameras is advised before the team enters the scene, although cameras may be hidden or concealed.

Concealment of camera lenses does not affect digital material but might affect other forensic measures such as DNA collection. Concealing camera lenses is suggested, **IF POSSIBLE**, to be done by using anti-static gloves.

If first responders prioritize collection of DNA samples from the site and devices, the team **SHOULD** use anti-static gloves, and disconnect the camera device from its power supply to stop its transmission faster and to prepare for its collection.

When disconnecting the cameras from its power supply, the team **SHOULD** make sure it does not affect the full or partial power supply of the site and does not affect power-supply to a nearby DVR or storage device. This can be done by carefully assuring the disconnected power supply goes directly to the right camera and visibly only to the camera, if its battery operated, remove it. This stage is meant for safety considerations, on the next stage of "Quick Assessment" (see 5.2.6 below), the team can consider wider power-supply shutdown or network disconnection.

The use handheld short-range wireless jammers[21] can stop transmitting device sending the recordings to remote location. Stopping the connectivity of the devices can prevent booby-trapped remote-operated devices from exploding and prevent remote-monitoring of the first responders' actions on-site.

## a. Purpose

- To ensure security and safety of first responders, other personnel and people, and surroundings.
- To identify connected digital devices on the scene that might pose threat to personnel safety and security and stop the transmission, if possible.
- To identify connected devices that might be remotely manipulated by terrorists and prevent them from doing it.

## b. Actions

1. First responders **MUST** identify working cameras and UAS and assess their connectivity.

   The parameters that would indicate that the digital device is connected are:

   - Device is working, seemingly in flying mode, blinking.
   - Device is using cable or wireless connection devices (Wi-Fi, cellular, satellite, etc.).

2. First responders **SHOULD** cover their faces to conceal themselves from active photography or recording by connected devices.

3. **IF POSSIBLE**, stop the transmission and recordings and digitally isolate the site.

   Connectivity can be stopped by:

   - Using transmission jammers for networks and signals, including GPS.

[21] Battlefield Digital Forensics Digital Intelligence and Evidence Collection In Special Operations, Christian Braccini, Teemu Väisänen, Michal Sadloň, Hayretdin Bahşi, Agostino Panico, Kris van der Meij, Mario Huis in 't veld, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2016, See Page 39.

- Disconnecting the entire site from cable networks, turning off routers and wireless generating or expanding devices.
- Disconnecting the devices from its power source.

### c. Results

After completion of the scanning of the site, first responders will be able to identify safety and security hazards stemming from digital devices left on the scene, their technological complexity and possibility of remote site monitoring by terrorists. The presence of cameras, UAS, sensors and network devices is an indication of possible remote activation of the devices located and first responders should not enter the scene before it is cleared safe for entering by relevant personnel.

## 5.2.5 Documentation

Box 2

**This action SHOULD be taken before moving on to the next phase.**

Documentation is a key element in preserving the chain of custody. At this stage, documentation is also beneficial for:

- Supporting decision making on-site, especially regarding the digital device and whether it is exploitable and needs to be collected.
- Supporting further exploitation of digital devices in digital forensics lab. Documentation can assist lab in understanding irregularities the digital forensics experts find in the digital device, identify the owner of the digital device, etc.
- Documenting first responders' interventions at the scenes, if challenged during legal proceedings.

For documentation, first responders can use video cameras to record the scene and devices. Video recording can provide all or most of the information required for documentation at a later stage. Alternatively, first responders can sketch the scene.

Any changes made by first responders at the scene should be for safety reasons only, and video recording in real-time can support the credibility of actions and chain of custody of digital devices.

If the video recording could not be made for all changes made by first responders, it is recommended to supplement the recording with a written report. If video recording is not available, the team can perform documentation in writing, using the template provided in Annex B1.

### a. Purpose

- To preserve a chain of custody and support future digital forensic activities.

### b. Actions

1. First responders **SHOULD** document in writing or by video recording the surroundings of the site and digital devices found.

2. Documentation at this stage **SHOULD** include:

   - Site overall description
   - Location of the device
   - Device description and state – working, in flying condition, blinking
   - Device identified connectivity – the presence of network transmissions – indication of connectivity by cable or by wireless connection devices (Wi-Fi, cellular, satellite, etc.,)
   - Actions made to isolate the online transmitting device and the scene – documenting the use of jammers, power-supply cut-off, etc.
   - On-screen information on the device found
   - A registered list of all witnesses that are present at the scene upon the arrival of the team - name, surname, any indication of suspicion – a visible state of mind.

3. Please refer to Documentation upon Arrival at the Scene Template in the Annex B1.

### c. Results

Documentation or video recording of a scene, describing the site, location, description and state of devices, device connectivity status, first responders' actions to disconnect devices, witnesses present at the scene.

## 5.2.6 Quick Scene Assessment

Box 3

**This action SHOULD be taken before moving on to the next stage to fully comply with digital forensics methodologies. Exceptions can be made when staying longer on the scene will endanger first responders or other personnel.**

This phase is the last phase for the arrival stage and initiates the next stage of triage of digital devices. It is limited to disconnection of cameras and UAS from their power supply or network, as they pose the highest risk of remote monitoring.

Some information may be lost when disconnecting a digital device from power or network, but it is not a primary consideration for cameras and UAS.

Isolating the site is essential for the safety of first responders. Digital isolation is performed by disconnecting digital devices from their power-supply and network.

If on-line cameras or flying UAS are located at the scene, it is recommended to contact or call a digital forensics expert on-site.

First responders should mark all UAS for collection. Stationed cameras typically do not store a lot of data, and the camera itself is less important than its data storage computer (DVR/NVR).

Cameras are a low priority item for collection.

If first responders assess that the scene is monitored or booby-trapped, their decision to leave or enter the scene **MUST** be made in accordance with the applicable safety and security protocols.

### a. Purpose

- Isolate the scene from visible remote monitoring.

### b. Actions

1. First responders **SHOULD** decide which digital devices to be disconnected from power or network.

2. First responders **SHOULD** decide if an expert needs to be called on-site (for example, digital forensics, UAS, explosive ordinance device).

3. First responders **SHOULD** identify digital devices for triage.

### c. Results

Digital devices are disconnected from power or network and identified for triage. Relevant experts are called on scene, in secured or permissive environment.

## 5.3 Stage 2 - Triage of Digital Devices

Triaging is an important element of the process of collecting digital devices by first responders. Triage entails on-site evaluation, assessment and prioritization of digital devices or storage media for collection for further examination and analysis. It helps first responders to focus their efforts and save time.

For the purpose of this document, triage involves identification and prioritization of digital devices in the battlefield for collection based on factors such as their value for counter-terrorism investigations and the value of stored data.

During this stage, first responders **MUST** find all digital devices on-site and **SHOULD** determine which devices to collect for further exploitation and analysis, in what order of priority, **SHOULD** document their actions and conduct a quick assessment of the scene.

It must be noted that not all digital devices contain data that has a high probability to assist in criminal counter-terrorism proceedings. Some data stored on digital devices may not be relevant, therefore collection of digital devices should be prioritized accordingly to all circumstances and priorities of the team.

For the context of this document, triage does not include live processes or access to the data on the device by non-professional first responders.[22]

Table 6: Summary of Actions

| Action | Purpose | Level of Importance |
|---|---|---|
| *1. Find all digital devices on-site* | *Handling* | *MUST* |
| *2. Decide which digital devices to collect* | *Documentation* | *SHOULD* |
| *3. Documentation* | *Documentation* | *SHOULD* |
| *4. Quick Scene Assessment* | *Security Measures* | *SHOULD* |

### 5.3.1 Locating Digital Devices On-Site

First responders should look for all digital devices placed on-site, including hidden and concealed devices. A non-exhaustive list of the most relevant digital devices, which store a lot of data and contain files, which can be used as evidence in criminal proceedings of terrorist offences are:

- Cellular phones
- Computers – stationery and laptops
- Servers
- Tablets
- USB thumb drives
- Digital storage devices
- Memory cards
- SIM cards

[22] For more details on live triage with on-site access to the data of a device, see INTERPOL, Guidelines for Digital Forensics First Responders, Best practices for search and seizure of electronic and digital evidence, March 2021. For more information on the evolution of digital triage, see Carrier, B. (2011). Digital triage forensics: A field guide for first responders. Syngress.

- Cameras
- UAS

When first responders find a stationed camera on-site, they **MUST** search and find the computer (NVR/DVR) that the cameras are sending information to. This computer stores all the data the cameras were recording until they stopped and should be nearby, in some cases connected by cable to an Internet device and following the cables can assist in finding all Internet cable connected digital devices. These types of computers usually store the recorded data for a brief period and re-writes over prior recordings. Another method is to search for the storage computer of the camera by following power-supply cables to find more digital devices that are connected to power.

Identifying the status of a digital devices helps to decide on measures required to collect the device. At this phase, the team **MUST** only check the state of the device. Documentation will be done during the next phase (see 5.3.3 below).

The core element of triage is deciding which devices should be collected and their priority. First responders **SHOULD** refrain from conducting searches inside the devices if they do not have a dedicated digital forensics expert on the team. To decide which devices to collect and in what order of priority, first responders **MUST** assess potential relevancy of the data stored in a digital device for counter-terrorism investigations and the state of a digital device.

**Table 7: Summary Considerations**

| Parameter | Factors to Consider | Relevancy | Urgency |
|---|---|---|---|
| *Potential relevancy of the data stored in a digital device for counter-terrorism investigations* | *The owner or user of the device is suspected to be involved in terrorist activities* | *High relevance for further examination and data exploitation* | - |
| | *Data on the digital devices contains files, user activity, user data, communication* | *High relevance for further examination and data exploitation* | - |
| *The state of the digital device* | *Damaged, password protected, encrypted* | *More complex for data exploitation* | - |

| | | | |
|---|---|---|---|
| | *Turned off, not damaged* | *Easier to collect* | *Not urgent* |
| | *Turned on, password protected, suspected to be encrypted* | *Call a digital forensics expert* | *Very urgent* |

The overall relevancy score of a digital device will assist the team in determining which digital devices need to be addressed first, at a later stage, or not touched at all.

If there are suspicions that there are IEDs or booby-trapped devices on-site, first responders **MUST** adhere to relevant safety procedures and protocols.

## a. Purpose

To locate all digital devices left on-site and prioritize their collection.

## b. Actions

1. First responders **MUST** search the scene and locate all digital devices.

2. If first responders find a stationed camera on-site, they **MUST** search and find the computer (NVR/DVR) the cameras are sending information to.

3. First responders **MUST** identify the status of digital devices found on-site:

    - Working
    - Turned off
    - Connected to/ disconnected from a network
    - Connected to/disconnected from a power-supply
    - Damaged
    - Encrypted
    - Password protected.

4. First responders **MUST** assess the relevancy of the device for investigation, prosecution and adjudication of terrorist offences

## c. Results

(1) All digital devices are located on the scene.
(2) their status is identified, prioritized in terms of their relevance for investigation, prosecution and adjudication of terrorist offences.

### 5.3.2 Deciding which Digital Devices to Collect

First responders **SHOULD** always collect mobile phones, UAS and their remote controller, laptop computers, stationary computers that are turned off, storage repositories such as USB thumb drives, memory cards and hard drives, as they are usually light weighted and may contain a lot of digital material relevant for investigation and prosecution of terrorist offences. Peripheral devices, such as keyboards, mouses, printers, computer screens are usually not of interest for digital exploitation and digital evidence.

**Box 4**

**Digital devices left in the battlefield can have other investigative value aside from digital information. They can store DNA information, fingerprints, or explosive materials residue, which could be relevant for investigation and prosecution of terrorist offences and must be considered when deciding on which digital devices to collect.**

If servers or stationary turned-on computers are found on-site, first responders **SHOULD** consult (remotely) with a digital forensic expert before collecting them. At this point of triaging, a consultation should be enough, and can provide basis for calling the digital forensics expert on site for the collection. Determining the relevancy of servers requires triage of the stored information, where such action may harm the evidentiary value of the information that will be collected from it. The triage decision should be based on the relevancy of the digital device to investigation and prosecution of terrorist offences, and by the first responders' ability to secure the scene and wait for a digital forensics' expert to arrive.

Turning off a working computer or a server will likely have an effect on the ability to recover the data that is stored on them and **SHOULD** be avoided, if a digital forensics expert can arrive to the scene.

If there is no digital forensics expert to consult, first responders **SHOULD** disconnect the digital device from the network but **SHOULD** keep it in working state until some advice from a digital forensic expert is received. If first responders must urgently leave the scene or if remaining on-site is not an option because of safety and security concerns, first responders **SHOULD** turn working computers or serves off and collect them anyway. Leaving working computers and servers on-site is the least recommended option.

**IF POSSIBLE**, first responders should look for damaged digital devices and consider their relevance for collection. Damaged digital devices are devices that look broken, burnt, not intact, etc.

First responders should look whether the data storage unit of a damaged digital device looks intact. If a digital device is visibly in bad shape, for example, shattered into pieces, completely burnt, first responders will not be able to determine if the data on this device is still intact. When digital devices are completely broken, the reconstruction of the device is not practical, and the device **SHOULD** be left on-site.

For prioritization of collectable digital devices, first responders **SHOULD** consider the relevancy of its data for the teams' missions, and its relevancy for counterterrorism investigations and prosecution, along with the device's potential for reconstruction, if a digital device is damaged or broken, its physical weight, required packaging and its transportation measures.

While triaging, first responders **SHOULD** label digital devices that are decided to be collected and those digital devices that will be left on-site. Labeling of digital devices while triaging will help in distinguishing between the different items found on-site and may assist in documentation of the scene, the place where the digital device was originally found and their surroundings.

**Box 5**

**IED's can sometime look like neglected or damaged devices. First responders SHOULD use all security precautions to locate explosives on site and follow their security protocols for explosion hazard scenes.**

## a. Purpose

To decide which digital devices will be collected and in what order or priority

## b. Actions

1. First responders **SHOULD** always identify for collection.

   - Mobile phones
   - UAS and their remote controller
   - Laptop computers
   - Stationary computers that are turned off
   - Storage repositories such as USB thumb drives, memory cards, hard drives
   - SIM cards

2. **IF POSSIBLE,** first responders should identify for collection:

   - Servers
   - Stationary computers that are turned on

3. **IF POSSIBLE**, first responders should assess damaged devices

4. First responders **SHOULD** label devices for collection

### c. Results

Collectable digital devices are identified or labelled for collection

## 5.3.3 Documentation

Documenting the triage helps to understand decision-making process on-site at a later stage and assists in tracing missing components when the digital device is exploited at the lab. First responders **SHOULD** document the triage only if doing so does not compromise team's safety and security. If a digital forensics expert is among first responders and performs a live triage, all actions **MUST** be documented in accordance with digital forensics methodologies.

This documentation will be relevant if digital devices collected from the scene are challenged in court or are needed for later judicial review. Triage can also be documented at a later stage. First responders SHOULD label all digital devices planned for collection by simple stickers. It can be any type of simple small sticker that is visible, and the team acknowledges its meaning.

### a. Purpose

- To document the scene and all digital devices found on-site and label digital devices for collection.

### b. Actions

1. First responders **SHOULD** document the scene by photographing it, and all the digital devices that were found, including those that would not be collected.

2. First responders **SHOULD** label with stickers devices to collect.

### c. Results

All digital devices found on-site are documented and labelled for collection.

## 5.3.4 Conducting a Quick Assessment of the Scene

Box 6

**This action SHOULD be taken before moving on to the next stage to fully comply with digital forensics methodologies. Exceptions can be made when staying longer on the scene will endanger first responders or other personnel.**

First responders **SHOULD** assess the need for calling other experts before they start collection of digital devices. These decisions must be made in accordance with the time the team can stay on the scene, and if the circumstances allow it.

If a working computer or server is found, turning off the device will likely impact digital forensics team ability to recover data stored on this device. Therefore, first responders **SHOULD** consider calling a digital forensics expert on-site to collect information from working computers or servers to ensure that procedures for digital forensics are strictly followed and the chain of custody is maintained.

Collecting information from a computer or searching through a cell phone, without proper training and equipment, can harm both the data and the device, will impact reliability, integrity, and authenticity of the evidence, and render it inadmissible to criminal proceedings and should never be pursued by first responders, who are not trained in digital forensics.

If a working computer or server is found, first responders, **IF POSSIBLE**, should call for a digital forensics expert to arrive on-site for digital forensics live triage and copying of information. If first responders suspect that some digital devices might be booby-trapped, they should call for EOD experts or units.

At the end of triage, first responders know which digital devices will be collected and can assess whether they have sufficient resources to package and transport all collectable digital devices. If first responders lack resources, they would need to request for more resources to be delivered on side or modify the triage. First responders **SHOULD** be aware of threats stemming from IED’s or booby-trapped digital devices. Relevant safety and security protocols **MUST** always be followed.

## a. Purpose

- To call for additional expertise before digital devices are collected and assess the team’s physical capacity to collect all collectable digital devices.

## b. Actions

1. First responders **SHOULD** decide if there is a need for consultation with or arrival on-site of a digital forensic expert.

2. First responders **SHOULD** decide if other experts shall be consulted or called on-site.

3. First responders **MUST** assess their physical capacity to collect digital devices on-site by assessing whether they have sufficient packaging equipment and transportation capabilities.

## c. Results

(1) Digital forensics experts or other experts are called on-site as needed before digital devices are collected; and (2) first responders have sufficient resources to package and transport collectable devices.

## 5.4 Collection and Packaging of Digital Devices

In the battlefield, first responders have significantly less time for collection of digital devices. Therefore, first responders should always collect computers and digital devices in the cases they are found and never open them on-site.

Digital devices should be collected with caution for non-contamination and preservation. For example, the use of adequate anti-static gloves by first responders will increase chances for recovery of fingerprints from digital devices using traditional forensics means.

**Table 8: Summary Actions**

| Action | Purpose | Level of Importance |
|---|---|---|
| *1. Handling* | *Handling* | *MUST* |
| *2. Documenting the scene* | *Documentation* | *MUST* |
| *3. Packaging* | *Handling* | *MUST* |

### 5.4.1 Handling

**Box 7**
**This action MUST be taken before moving on to the next stages.**

“Digital isolation of a device” is an action aimed preventing a digital device from sending and receiving signals.

First responders **MUST** disconnect all digital devices from the network. It can be done by pulling out the cable, changing device to “flight mode”, or by disabling its network connectivity. All these actions will isolate the digital device from distant surroundings.

After disconnection from the network, first responders **MUST** continue to consider that a digital device continues to transmit signals. Even on flight-mode, a cellular device continues to send GPS signals and may point to the exact location of first responders or a digital forensics lab that first responders are delivering the device to.

To ensure blockage of signals, first responders **MUST** pack all collectable digital devices into a faraday bag as soon as possible, after they have been disconnected from the network (for more information, see Packaging 5.4.3 below). To prevent any confusion between devices and in some cases between different scenes, first responders should label devices with stickers and package them in separate individual bags.

Labelling **MUST** include:

- A notification of "DIGITAL DEVICE"
- Date and time of collection
- Unique identifying number of the digital device
- Full name of the team member who collected the device
- Unique and precise definition of the site where the device was found
- A mark to suggest if this device should be cloned or copied.

When handling working devices that contain cameras, first responders **SHOULD** always divert the camera away from their faces. This will prevent the recording of first responders by terrorists by automatic means, which usually sends photos to distant locations as well. First responders **MUST** ensure that a small concealing sticker is placed on the camera of the mobile device as soon as the device is approached.

If a cellular phone is turned on and is open, first responders **SHOULD** cancel digital device's password to make it accessible at a later stage.

All phone models after 2013 should be considered as encrypted and **SHOULD** be handled accordingly on-site (see section 5.3.4 above). **IF POSSIBLE**, first responders should not shut down the cell phones they are collecting and collect them in the working state that they were found. **IF POSSIBLE**, first responders need to keep cell phones active by using an alternative power source (external power-bank) until the digital device reaches the lab for further exploitation.

When there is no nearby lab, first responders **SHOULD** call a digital forensics expert for on-site exploitation of the device (see 5.3.4 above ).

If first responders know or manage to cancel the password for a digital device, they can shut it down. If a collected cell phone is expected to reach the lab days after collection, **IF POSSIBLE,** first responders should label the device by writing its password and shut it down before packaging.

Breaking a cell phone encryption requires resources of an advanced digital forensics lab. When such a lab is not available, first responders **SHOULD** seek to identify the device's user and to find the device's password. These actions **MUST** be in accordance with the rule of law, and if needed, be accompanied with a judicial review or warrant.

Cell phones **SHOULD** be collected with their charging cables, if found on-site.

When an UAS is found at the scene, whether in a working state or shut-down, first responders can approach the UAS for quick information. However, examining the UAS **MUST** be done by a digital forensics' expert, who **SHOULD** be called on-site (see section 5.3.4 above).[23]

When a data storage device is suspected to be encrypted, first responders **SHOULD** search for the password at the scene and question relevant witnesses. All actions **MUST** be performed in accordance with the rule of law and human rights principles. If the situation is urgent, any non-voluntary provision of password information must be subject to judicial review.

If the device is a working computer with encrypted data storage, first responders should, **IF POSSIBLE**, photograph information displayed on the device and call a digital forensics expert for consultation (see section 5.3.4 above). Device's information may not be accessible after it shuts down. First responders **MUST** consult digital forensics experts before shutting down the device or computer or disconnecting its power supply.

Computer screens are large and hard for transportation, and they commonly do not contain digital information of relevance to counter-terrorism investigations and prosecution. If it is a regular computer screen, first responders **SHOULD NOT** collect it and leave it on-site. First responders **SHOULD** make sure that the screen is not an "all-in-one" computer.

"All-in-one" screen **MUST** be considered as a computer and first responders **SHOULD** collect them if it is turned off or consult with a digital forensics expert if it is turned on.

When smart TV screens are found on-site, first responders **SHOULD** consult with a digital forensics expert to decide whether a smart screen should be taken or not.

Printers usually do not store any extra information. Most of data on printed documents is stored on the sending device and first responders **SHOULD** be collecting other digital devices, such as computers or cell phones and collection of printers **SHOULD** be on low priority. But sometimes printers store data of the last documents printed. The document stored on the printer can be partial, without a specific time and date or without reference to the user who sent the document for print. First responders **SHOULD** collect printers only if no other digital devices are available.

Before touching or lifting a digital device, first responders need to make sure that they are not attached to a power source or an explosive material.

## a. Purpose

[23] Also see INTERPOL, Guidelines for Digital Forensics First Responders, Best practices for search and seizure of electronic and digital evidence, March 2021, pp.41-42.

- To ensure integrity, authenticity and credibility of collected digital devices, maintain the chain of custody of the information or the device and ensure its admissibility as evidence in courts.

### b. Actions

1. First responders **MUST** digitally isolate the device.

2. First responders **MUST** label all digital devices.

3. First responders **MUST** collected digital devices with caution for non-contamination and preservation.

### c. Results

Digital devices are collected from the scene for packaging and transportation to a forensics lab or a dedicated site.

## 5.4.2 Documentation

Box 8

**This action MUST be taken before moving on to the next stages.**

The first touch of a digital device is the most crucial phase in digital forensics procedures. Documentation of this stage is crucial for the integrity, authenticity, and credibility of the device and for the chain of custody of evidence. And it is a **MUST** to ensure its admissibility as evidence in criminal proceedings.

Each collected digital device should have the following documented information attached to it along every stage of the chain of custody, including in storage, at a lab, and when being further examined.

Mandatory documentation can be supplemented with pre-labelled stickers, video recordings, on-site notes, template reports, checklists, and more.

As shown in the Table 9 below, some of the documentation can be completed at a later stage and not on-site, as long as it can be retrieved before first responders handover the digital device to another team. First responders **SHOULD** document the following specifications:

Table 9: Summary Actions

| Documented Information | Suggested measures |
|---|---|
| *1. **Date and time of collection**. This should be as accurate as possible.* | *A structured form to write date and time. Can be filled at a later stage* |
| *2. **Team member's full name and ID** of a person who handled the digital device for triage, collection, packaging and transportation.* | *Each team member can be supplied with "identification stickers" that can be used for labeling and documenting on all phases and documented at a later stage.* |
| *3. **Place:** region, site, location of the digital device on-site, connected devices or cables* | *The device can be photographed before collection and the details can be inserted at a later stage* |
| *4. **Description:** Type of digital device, manufacturer or model, color, label no.* | *The device can be photographed before /during collection and the details can be inserted at a later stage by using OCR, attaching the photo to the form or by filling out the details.* |
| *5. **State of digital device**: on/off, transmitting yes/no, locked/open, physical condition* | *A structured form will assist first responders in in tagging the description from a pre-structured list.* |
| *6. **Actions taken on-site:** changes that first responders made to the digital device, such as removal of password, turn off, connection to power-bank, disconnection from network.* | *Textual field to describe all changes made to the collected device, to maintain its chain of custody. It is possible that the described actions will alter the device and may affect its authenticity or may have other unintended consequences.*<br>*This should be filled as soon as possible.* |
| *7. **Details:** known owner, time and date on the device, suspected materials to look for.* | *This can be filled out at a later stage and will assist further investigation and material exploitation.* |

## a. Purpose

- To ensure integrity, authenticity and credibility of collected digital devices, maintain the chain of custody of evidence and ensure its admissibility as evidence.

## b. Actions

1. First responders **MUST** document all actions performed on the device for collection

### c. Results

All collected digital devices are documented to ensure its admissibility as evidence.

## 5.4.3 Packaging

Before packaging any digital device, first responders **MUST** ensure all collected devices are properly and uniquely labelled with a sticker (see 5.4.2 above).

Every digital device **MUST** be packed separately from other digital devices but together with their cables or other add-ons connected to them when found.

When collecting computers, first responders **SHOULD** collect them along with their cases they were found in and **SHOULD NOT** disassemble them on site.

To prevent electrostatic discharge that may harm the digital device or its surroundings or even cause self-explosion, first responders **SHOULD** use anti-static bags. Anti-static bags are cheap and weightless and should be considered as part of the first responders' kit. Paper bags or envelopes that can be sealed can be used in lieu of anti-static bags.

First responders **SHOULD** be aware that cellular devices continue to send GPS signals even when on flight mode and can pinpoint a terrorist to the exact location of first responders on-site, in transit and to a location of a forensic lab. To prevent digital devices from transmitting signals, Faraday bags are recommended as packaging material.

First responders need to make sure that previously used Faraday bag is working properly before arrival on-site. As an alternative, first responders can use aluminum foil to wrap the digital device (at least 3 times) after packing the device in an anti-static bag.

To prevent shaking and physical harm to collected digital devices, first responders need to pack them in a padded storage. Any kind of padding can be used, as long as digital device is wrapped in antistatic bags.

**IF POSSIBLE**, first responders should pack digital devices in their original package.[24]

All digital devices **MUST** be packed together with the documentation suggested in section 5.4.2.

First responders **MUST** seal the package with a tape to ensure that documents, cables or accessories packed with the device are not lost.

First responders must label the packages and the labelling **MUST** include:

[24] Also see INTERPOL, Guidelines for Digital Forensics First Responders, Best practices for search and seizure of electronic and digital evidence, March 2021, p.20.

- A notification of “DIGITAL DEVICE”
- A notification of a “DEVICE IN WORKING STATE”, if applicable
- A notification of “EXPLOSION HAZARD – CONTAINS BATTERY” when the device is packed with an external power-bank or contains a battery
- Date and time of collection
- The unique identifying number of the device
- Unique and precise definition of the site where the device was found
- The place or name of the first responders’ team
- The final destination for a package

Use of an alternative source of power (external power-bank) to transport a digital device in a working state can be hazardous and increases the risk of battery explosion.

The use of an external power bank and transporting a device on a working state **SHOULD** be made known and considered by all personnel addressing the device, always.

If a digital device in a working state with or without an external power bank is transported, it **MUST** not be exposed to extreme temperatures.

Before deciding whether a digital device should be transported with an external power bank, first responders **MUST** consider their expected travel time to digital forensics lab, expected temperature, and estimated time of arrival.

## a. Purpose

- To package all collected digital devices in preparation for transportation

## b. Actions

1. First responders **MUST** wrap all small digital devices in a separated anti-static bag.

2. First responders **MUST** use faraday bags, when needed.

3. First responders **MUST** wrap all digital devices, which do not have protective cases (that is inside the anti-static bag) in a padded wrap.

4. First responder **MUST** package all wrapped digital devices in a box/ envelope/ bag.

5. First responders **MUST** package digital devices before concealment a copy of documentation.

6. First responders **MUST** seal the package before transportation.

7. First responders **MUST** label the package before transportation

### c. Results

All collected digital devices are uniquely labeled and properly packaged.

## 5.5 Transportation

Collected digital devices need to be transported as soon as possible out of the battlefield to a safe location for storage and further material exploitation.

Digital devices can be transported by first responders themselves or by another team. Considering that not all digital devices can be transported directly to a digital forensic laboratory, devices shall be transported to a storage facility and then, as soon as possible, to a digital forensics lab for exploitation. When digital devices are transported for storage, first responders **MUST** prepare all necessary documents before transportation. Collected digital device **MUST** never be left unattended.

The documentation prepared during previous stages of these guidelines **MUST** be always attached to the relevant devices.

Digital devices **SHOULD** be transported inside padded packages, closed, and as far from the transport team as possible to minimize the possibility of being recorded by active recording devices.

**Table 10: Summary Actions**

| Action | Purpose | Level of Importance |
|---|---|---|
| 1. Documentation | *Documentation* | *MUST* |
| 2. Digital Devices in-Transit | *Security Measure* | *MUST* |
| 3. Handover | *Handling* | *MUST* |

### 5.5.1 Documentation

**Box 9**

**This action MUST be taken.**

Transportation **MUST** be documented in terms of documenting the different team members that have touched the digital device, and the specific destination such as forensics lab, storage, etc.

Documentation **SHOULD** include a short description of the digital device and the objectives of its transport to assist the receiving party in quickly handling the device.

The device must be accompanied with a copy of the documentation first responders prepared during collection.

### 5.5.2 Digital Devices in-Transit

While in transit, the transport team should be aware of the risks of transmitting digital devices. The transport team **MUST** never unpack the collected digital devices since they can expose themselves to terrorists who might continue track the devices. Unpacked digital devices can transmit signals and expose transport location, record conversations and transmit data to an unknown hostile location. This, in turn, can lead to targeted attacks, exposure of the transport route and facilities location.

Unpacking cell phone, which have not been concealed, could record team's faces and transmit this data to the cloud.

The transport team should also be aware of a risk of self-exploding devices such as batteries, power-banks, cellular phones etc. and take necessary precautions.

Digital devices **SHOULD** remain packed all the time and never be placed on a team member's lap.

Transportation temperature should be monitored to prevent overheating of digital devices. Overheat might happen in some extreme weather conditions or when a digital device is placed near a heat source in transport.

### 5.5.3 Handover

The chain of custody **MUST** be maintained and the handover of collected digital devices **MUST** be documented and attached to the device.

The handing team **MUST** brief the transporting teams on safety and transportation mechanisms, and make sure that all documentation and labeling are attached to the device prior to its handing. This is necessary to prevent breaking the chain of custody and to prevent loss of devices, future misunderstandings and confusions.

# [ Appendix A ]
# Basic Equipment Checklist

## A.1 Checklist

Below is a suggested list of basic equipment for first responders.

□ Video Camera

□ Anti-static Gloves

□ Labeling stickers – personnel unique stickers or writeable stickers.

□ Permanent Markers (for labeling)

□ Small stickers for camera cover

□ Handheld transmission jammers including Wi-Fi, Cellular and GPS

□ Anti-static bags, zip-lock bags or paper envelopes with seal

□ Seal equipment

□ Faraday bags or aluminum foil bags or aluminum foil wrapper

□ Bubble wrap packaging

□ Padded packages

□ Packaging carton boxes

□ Documentation templates:

  - Documentation on arrival
  - Digital collection documentation

# [ Appendix B ]
# Documentation Template

## B.1 Template – Documentation upon arrival at the scene

First responders should document in writing or by video recording the surroundings of the site and digital devices found.

**To be completed for each site of collection:**

**Date and time of arrival:**

| | | | |
|---|---|---|---|
| Date | | Time | |

**Site Details**:

| | | | |
|---|---|---|---|
| Region | | Site | |

Overall description

**Documenting officer:**

Full name and ID of the team member filling the form, and commander on-site

| | | | | | |
|---|---|---|---|---|---|
| Full name | | ID | | Description | |
| Full name | | ID | | Description | |

**Device description and State**:

| **No** | **Device description and state**<br>**On/ Off/ Broken/ Flying** | **Connectivity status of the device** | **Location on site** | **Is digital Forensics expertise needed for the collection of the device?** |
|---|---|---|---|---|
| | | ☐On<br>☐Off | | ☐Yes<br>☐No |
| | | ☐On<br>☐Off | | ☐Yes<br>☐No |
| | | ☐On<br>☐Off | | ☐Yes<br>☐No |
| | | ☐On<br>☐Off | | ☐Yes<br>☐No |
| | | ☐On<br>☐Off | | ☐Yes<br>☐No |
| | | ☐On<br>☐Off | | ☐Yes<br>☐No |

**Actions taken on-site**:

State any changes the team made to the site in terms of isolating network, transmission, devices. Including any handling of a device such as remove password, turn off, connect to power-bank, disconnect from network, etc.,

**Witnesses**:

| | | | | | |
|---|---|---|---|---|---|
| Full name | | ID | | Description | |
| Full name | | ID | | Description | |
| Full name | | ID | | Description | |
| Full name | | ID | | Description | |

Notes

- Device description and state – On screen information on device found. Please state is the device working, in flying condition, blinking, etc.,
- Device identified connectivity - The presence of network transmissions – Indication of connectivity by cable or by wireless connection devices (Wi-Fi, cellular, satellite, etc.,).
- Actions made to isolate the on-line transmitting device and the scene – documenting the use of jammers, power-supply cut-off, etc.,
- A registered list of all witnesses that are present at the scene upon the arrival of the team - name, surname, any indication of suspicion – a visible state of mind.

# B.2 Template - Documentation on Collection of Digital Devices Template

Devices should be collected with caution for non-contamination and preservation. This template is aimed to document each collected device. Some of the details on this template can be completed at a later stage and not on-site, as long as it can be retrieved before the first responders team handover the digital device to another team.

Handling

Documenting

Packaging

***Attach this filled form to the collected device and pack with the device.***

**Documentation is needed for each digital device collected:**

**Device No. as issued upon arrival or its labeling**

**Make sure the number matches the labelling on the device**

**Date and time of collection:**

date time

**Handling officer:**

Full name and ID of the team member that handled the device, made changes or picked for triage, collection, and packaging.

| | | | | | |
|---|---|---|---|---|---|
| Full name | | ID | | Action | |
| Full name | | ID | | Action | |
| Full name | | ID | | Action | |
| Full name | | ID | | Action | |

**Place of collection**:

Region site

Location of the device on-site

Attached devices or cables

**Description of the collected device**:

Type of device

Manufacturer or model

Color Label no.

**State**:

on □ off □

Transmitting - yes □ no □

locked □ open □

Physical condition

**Actions taken on-site**:

State any changes the team made to the device such as removed password, turned off, connected to power-bank, disconnected from network, etc.

**Details**:

Known owner

Time and date on the device

Notes

https://www.un.org/counterterrorism/ct-tech-initiative

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)