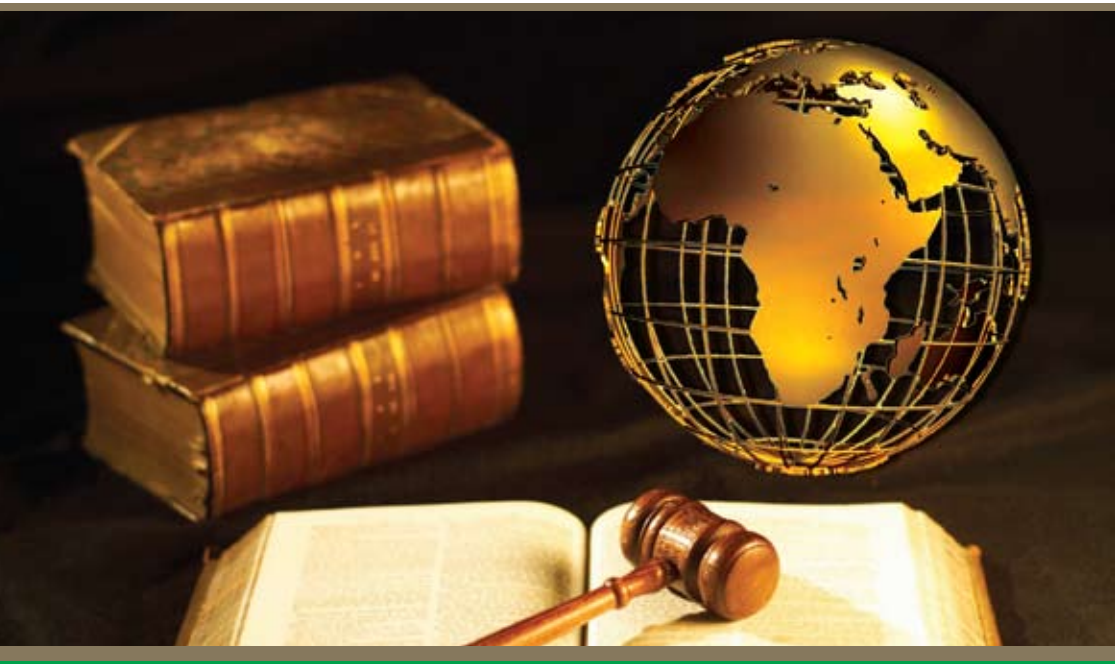


Africa Prosecutors Association Counter-Terrorism Manual

for Prosecutors

Contents

Foreword

Adv. OM Imalwa
President of the Africa Prosecutors Association (APA)

The idea behind the counter-terrorism manual was first mooted at the 8th annual conference of the Africa Prosecutors Association that was held in Cape Verde during 2013. The tenth year of the existence of the Africa Prosecutors Association is a historic moment in the history of the Association it also marks an important milestone for us to be launching this manual. What makes this occasion so special is that the manual was written by prosecutors from Africa, for prosecutors. When we came together in Mozambique to officially launch the Association one of the ideas behind its formation was to strengthen the collective capacity of prosecutors throughout the continent. We believed at the time that capacitating Africa`s prosecutors with knowledge and skills, will enable them to better deliver justice to our people on the continent.

The emergence of terrorism has had devastating effects on our people. No country has been immune to the consequences that this crime brings. From Cape to Cairo, Nigeria to Kenya its horrific impact has been felt and it has left a stain on the collective psychic of our people. It is with this in mind that prosecutors on the continent had resolved to be proactive in response to this phenomenon by empowering themselves with an aid and becoming more vigilant and prepared when confronted with the scourge of this type of an offence.

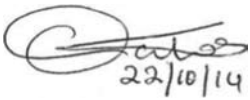
At one of our executive meetings held in Maputo, Mozambique the Institute for Security Studies together with the Strategic working committee of the APA under the able leadership of Adv. Shaun Abrahams was mandated to work hard at ensuring that the first ever and by no means the last manual on the subject be finalised. I am therefore confident that with this new tool, prosecutors would be

better equipped to respond to the threat posed by the emergence of this crime. I am also convinced that by the creation of this manual, Africa`s prosecutors are moving in the right direction and ever more closer towards realizing the objectives as enumerated under the aims and objectives of the Association`s constitution.

It is with sincere appreciation that I thank our donor the United States of America for its prompt assistance in this regard. Your generosity has gone a long way in capacitating Africa`s prosecutors to better respond to the growing threat posed by the emergence of this crime. Your contribution not only serves as a shining example for others to follow but it will forever be held in great esteem by both prosecutors and the judiciary alike. It is my desire that our Association should soon embark upon working on a second manual that would focus on corruption. Corruption needs the attention and specialization of all prosecutors. Corruption undermines and destroys the economies of our respective countries and creates poverty among our citizens.

In conclusion, my heartfelt appreciation to everyone who was involved in the compilation of this counter-terrorism manual. Your dedication and commitment will always be remembered and your contribution will always be felt when prosecutors in search of new techniques pick up this manual to read. To all the prosecutors who would be making use of the manual I am certain that you would find the manual more than helpful as a practical tool to aid you in the execution of your prosecutorial duties, as the cases referred to in the manual are real life cases that were dealt with by prosecutors on the job.

I thank you.



22 October 2014

Acknowledgements

The APA wishes to express its sincere gratitude to all those who contributed to the successful development of this manual and especially to Shaun Abrahams who ably led the process to its successful end.

To the Prosecutors who contributed to the different chapters in the manuals as authors and/or contributors there to. The following persons deserve mention:

Haruna Isa Alabi	FMJ	: Nigeria
Prosper Mwangamila	NPSA	: Tanzania
Monica Chipanta Mwansa	NPA	: Zambia
Vanusa Cemina dos Reis Aurbiiz de Sousa	NPA	: Angola
Rolanda L Van Wyk	Office of the Prosecutor General	: Namibia
Daisy Otchere Darko	NPA	: RSA
Fikile Mdhluli	NPA	: RSA
Collin Brian Chitsime	SAA	: Malawi
David Charles Ali Bilal	Ministry of Justice	: South Sudan
Luvuyo Mfaku	NPA	: RSA
Anneli Botha	ISS	: RSA
Uyo Salifu	ISS	: RSA
Shaun Abrahams	NPA	: RSA
Arvinder Sambei	GCSS	: UK
Martin Polaine	GCSS	: UK
Dawood Adam	OWP	: RSA
Chris Macadam	PCLU	: RSA
Chris Ndzengu	AFU	: RSA
Jason Jordan	Consultant	: RSA

The APA EXCO created an enabling environment for the work to happen seamlessly. We say Thank You.

Gratitude also goes to the members of the APA Strategic Committee who co-ordinated the whole process duly assisted by members of the ISS. To you I say well done.

I thank you

Compiled by:
Adv Thoko Majokweni-Sipamla
Special Director of Public Prosecutions: National Prosecuting Authority of South Africa
Office of the APA Treasurer General

Preface

The development of the APA Counter-Terrorism Manual for Prosecutors has been inspired by the realisation of the pivotal nature of the role of the prosecutor in crime fighting and the administration of justice. Central to this, is the instilling and maintenance of the rule of law in the continent.

It is important that the capacity to deal with crimes that have a negative impact in the application of the rule of law must be developed on an ongoing basis. It is also quite important to ensure that minimum standards are set in the development of the said capacity and resultant capability.

The manual is intended to be both a learning tool to be used in training all prosecutors but also as a desk reference for those prosecutors with less ability to access information and knowledge in the prosecution of crimes of terrorism and related offences like financing of terrorism and cyber-crimes for example.

It must therefore be a living document stimulating intellectual debate and conversation among prosecutors. It should have no national or regional boundaries so that prosecutors from all over the continent can share experiences on its implementation. It must inspire and enrich legal dialogue. It will be updated from time to time as the need arises and as the environment of its application demands.

We need to act strategically when we approach those offences and strengthen how the criminal justice systems in our different countries and regions become deterrents because of their effectiveness, efficiency and expeditiousness of case management.

The APA has resolved to prioritise three areas of criminal law, which are the following:

- Organised crime including environmental crime
- Sexual and gender-based violence including trafficking in persons

- International and trans-national crimes including terrorism

It is hoped that prosecutors would benefit from it and be better at their business of prosecuting offenders terrorism because of it.

Compiled by:

Adv Thoko Majokweni-Sipamla
Special Director of Public Prosecutions: National Prosecuting Authority of South Africa
Office of the APA Treasurer General

Acronyms and abbreviations

3D	three dimensional
APA	Africa Prosecutors Association
AQIM	al-Qaeda in the Islamic Maghreb
AU	African Union
CLA	Caprivi Liberation Army
CT	counter-terrorism
CTC	Counter-Terrorism Committee
CTED	Counter-Terrorism Committee Executive Directorate
CPAT	Commonwealth Plan of Action on Terrorism
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DoS	denial of service
DRC	Democratic Republic of the Congo
ECHR	European Convention on Human Rights
ECOWAS	Economic Community of West African States
EMP	electromagnetic
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
EU	European Union
FATF	Financial Action Task Force
FLEC	Front for the Liberation of the Enclave of Cabinda
FBI	Federal Bureau of Investigation

FIU	financial intelligence unit
GCTF	Global Counterterrorism Forum
GIABA	Inter Governmental Action Group against Money Laundering in West Africa West Africa
GPS	Global Positioning System
IAP	International Association of Prosecutors
ICC	International Criminal Court
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
ICTR	International Criminal Tribunal of Rwanda
ICTY	International Criminal Tribunal for Yugoslavia
IED	improvised explosive device
ISP	Internet service provider
ISS	Institute for Security Studies
IGAD	Intergovernmental Authority on Development
IMF	International Monetary Fund
IT	information technology
IP	Internet protocol
MEND	Movement for the Emancipation of the Niger Delta
MLA	mutual legal assistance
MoU	Memorandum of Understanding
NPA	National Prosecuting Authority
NDPP	National Director of Public Prosecutions
OAU	Organization for African Unity
OWP	Office for Witness Protection
PCLU	Priority Crimes Litigation Unit
PIL	public international law
POCDATARA	Protection of Constitutional Democracy against Terrorist and Related Activities Act 2004

RF	radio frequency
SADC	SADC
SARPCCO	Southern African Regional Police Chiefs Cooperation Organisation
SCADA	supervisory control and data acquisition
SMS	Small Message Service
UAE	United Arab Emirates
UCTI	universal counter-terrorism instruments
UK	United Kingdom
UN	United Nations
UNCAC	UN Convention against Corruption
UNODC	UN Office on Drugs and Crime
UNTOC	UN Convention against Transnational Organized Crime
US	United States
VBIED	vehicle-born improvised explosive device
VoIP	Voice over Internet Protocol

Part 1

Introduction to terrorism in Africa

Anneli Botha and Uyo Salifu
Institute for Security Studies (ISS)

Index

Aim and objective

The aim and objective of this module is to provide a conceptual understanding and overview of terrorism in the absence of a universally accepted definition thereof. The scope of this overview includes the threat of terrorism in Africa; the motives behind terrorism; its means of perpetration; different types of terrorism; explosives; children as terror suspects; and suicide bombers.

This will enable prosecutors to:

- Understand what terrorism is
- Comprehend the threat of terrorism on the African continent
- Understand conditions conducive to terrorism
- Understand the motives behind terrorism
- Differentiate among the different types of terrorism
- Recognise and distinguish various types of explosives and nuclear and chemical biological instruments, and the manner of delivery commonly used by terrorists
- Understand cyberterrorism
- Understand terror financing

Chapter 1

Overview of the history of terrorism

Terrorism has always formed part of violent human behaviour. Thus, if we understand the historical development of terrorism, we may be able to determine why it is so difficult to define the concept in modern history, and why terrorism remains a valuable tactic.

The word 'terror' is derived from the Latin word *terrere*, which means 'to frighten'. Throughout history this concept and term were used to explain the use of violence as a tactic – from the campaign of Ivan the Terrible in 16th-century Russia to periods of violent political turbulence, such as the Reign of Terror during the French Revolution. In 1789–99 in France, for example, terrorism involved the use of violence against the state as well as violence perpetrated by the state.

Before the 1900s, the Anarchist anti-establishment movement presented itself as an organisation for the masses (or the working classes) against their exploitation by governments. One of the best-known incidents in the history of the Anarchist movement occurred in 1886 in Chicago when eight policemen were killed in a bomb attack during the Haymarket riot. This period also witnessed a number of assassinations, including those of General Martinez Campos in Barcelona, Spain in 1892; Sari Carnot, the president of France, in 1894; Empress Elisabeth of Austria-Hungary in 1898; King Umberto of Italy in 1900; and United States (US) president William McKinley in 1901. Although the perpetrators were categorised as 'anarchists', all of them acted alone, without the support or knowledge of the groups to which they belonged.

Terrorism was also included in the strategy of nationalist groups in the Middle East, Africa and Asia. During the 1960s, the 'terrorism' label was used to describe acts

of violence directed at the state by subnational groups and ethnic, ideological and religious insurrectionist movements; acts of terrorism were incorporated in guerrilla warfare in both remote and urban areas.

During the Cold War the Soviet Union assisted and trained national liberation movements in an attempt to spread traditional Marxist-Leninist thinking, while the US covertly supported the 'other side' of these conflicts. This period led to the development of the concept of 'international terrorism'. It is important to note that during this period terrorist groups learned from one another through their growing interaction and shared training camps in the Middle East, Europe and Africa.

The 1970s saw an increase in issue-motivated terrorism in the US with the advent of animal-rights organisations; white supremacy organisations such as The Order, and The Covenant, the Sword and the Arm of the Lord; and black militant movements such as the Black Panthers. The civil rights debate led to the development of both white supremacist and black militant movements. Government counter-measures and limited public support saw a decrease in the activities of white supremacy organisations during the 1980s. The 1990s, however, witnessed an increase in right-wing extremism, with Ruby Ridge in 1992 and the Federal Bureau of Investigation (FBI) siege of the Branch Davidian compound near Waco, Texas in 1993, leading up to 19 April 1995 when Timothy McVeigh bombed the Alfred P Murrah Federal Building in Oklahoma City. Although issue-motivated terrorism continued through anti-abortion and environmental groups, the attack on the World Trade Centre in New York on 11 September 2001 introduced a new phase in the threat and manifestation of terrorism.

Probably the most unfortunate aspect of terrorism is that it has become a label that is (mis)used in the following ways:

- Affected states label violent dissident groups as 'terrorists' to justify the use of extraordinary measures against them.
- Dissident groups, in turn, describe the violent repression they might encounter at the hands of state forces as 'terrorism'.

Ultimately both sides, to justify their cause as legitimate, label their opponents as 'terrorists'. When using violence, particularly when it is indiscriminate (targeting civilians and non-combatants), it is from an observer's point of view more a question

of loyalty (to a particular side of the conflict) in deciding who is a 'terrorist' and who is a 'freedom fighter'. The aphorism 'one person's terrorist is another person's freedom fighter' is legally and morally part of an emotional debate over which side is 'wrong' or 'right', which can be a serious obstacle to understanding terrorism. This argument should never be about when it is just to take up arms against a corrupt or unjust government or occupying force.

Chapter 2

What is terrorism?

Several attempts have been made to define terrorism. Despite all these definitions, the international community has thus far been unable to agree on one definition, due to:

- Emotion and labelling (what is right and what is wrong) in the freedom fighter vs. terrorist debate.
- The ever-evolving nature of terrorism as a tactic and the fact that it remains a favoured strategy. The motivation behind the resort to terrorism as a tactic and the manner in which it is used are constantly changing. This has contributed to the success of terrorism as a tactic, as those who are planning future attacks can adapt and include new technical advances. However, this has also had an impact on the formulation of a satisfactory definition.

Despite the inability to decide on one definition, all existing definitions have three common elements:

- **Method:** Violence or the threat to use violence
- **Target:** Civilian, government and, according to some definitions, non-combatants
- **Purpose:** Most importantly, to intimidate or instil fear to force change

Chapter 3

Terrorism as a crime

Because of the differences that impede the formulation of a single definition, it may be more appropriate to define an act of terrorism. Since most countries classify terrorism as a crime, providing the different elements of an act of terrorism can help those involved in criminal justice to prosecute those involved in the offence without becoming involved in the philosophical debate about the justification for the offence.

As a crime, terrorism is criminalised when the state involved passes laws to that effect. Crimes related to terrorism are also described in international, regional and national instruments. In this regard, the following activities, often referred to as 'terrorism', are frequently outlawed:

- Hijacking of airplanes and ships
- Attacks on ships and ports
- Targeting of diplomatic personnel
- Hostage-taking
- Bombings
- Financing of terror groups
- Endangering nuclear material, etc.

Instruments to assist prosecutors in addressing these acts are discussed in Part 2 of this manual.

Chapter 4

Organization for African Unity definition of terrorism

In recognition of the need to address the scourge of terrorism, the Organization for African Unity (OAU) defined those acts constituting terrorism in the 1999 Convention on the Prevention and Combatting of Terrorism:[1]

(a) any act which is a violation of the criminal laws of a State Party and which may endanger the life, physical integrity or freedom of, or cause serious injury or death to, any person, any number or group of persons or causes or may cause damage to public or private property, natural resources, environmental or cultural heritage and is calculated or intended to:

  (i) intimidate, put in fear, force, coerce or induce any government, body, institution, the general public or any segment thereof, to do or abstain from doing any act, or to adopt or abandon a particular standpoint, or to act according to certain principles; or

  (ii) disrupt any public service, the delivery of any essential service to the public or to create a public emergency; or

  (iii) create general insurrection in a State;

(b) any promotion, sponsoring, contribution to, command, aid, incitement, encouragement, attempt, threat, conspiracy, organizing, or procurement of any person, with the intent to commit any act referred to in paragraph (a) (i) to (iii).

As mentioned before, there remains no universally agreed definition. However, the criminality of terrorist acts and the violation of state laws provide a basis for the prosecution of these acts.

The origins of Boko Haram in Nigeria

Boko Haram's roots can be traced to al-Sunna wal Jamma or 'Followers of the Prophet', the group responsible for an armed uprising in December 2003 in Yobe State when it attacked police stations in Kanamma and nearby Geidam, killing two policemen. The group then retreated to a primary school in Kanamma where it hoisted the flag of Afghanistan and became known as the 'Nigerian Taliban'.

Analysis of the incident revealed that the group had operated in Nigeria for some time; it had a cell network of members that included highly educated people trained in the use of weapons. Residents of Kanamma, a small town in Yobe State in north-eastern Nigeria, also mentioned 'strangers' who had set up camp on the town's outskirts near the Niger border at the end of 2002 and beginning of 2003. These 'strangers' had come into town to preach about the attainment of Islamic purity. According to security officials, the group had an extensive network of cells that recruited members from afar, including Lagos in the south-west and neighbouring Niger. The fact that residents mentioned 'strangers' raised the possibility that foreigners were responsible for the establishment of the group and that it might have received external financial and logistical support (including weapons). Information gathered during investigations increased concerns among security agencies about the activities of certain Islamic preachers whom they feared were radicalising Muslims in parts of the north. Many were suspected of having links to terrorist groups and foreign organisations. These concerns deepened when the group attacked a police patrol on 8 October 2004 near Kala-Balge, close to the north-eastern border with Cameroon.

The members of the group were university students who sought to create a Taliban-style state. Small extremist groups such as this one tapped into a wider atmosphere of frustration and feelings of neglect, and tried to impose what they called 'purification of Islam' on the communities where they had set up military-style camps. The group has since attacked various local and federal government targets, causing death and destruction.

Chapter 5

Types of terrorism

5.1 Distinctions based on areas of operation

5.1.1 Domestic terrorism

Domestic terrorism refers to acts of terrorism that are confined within national boundaries and do not include targets or agents from abroad. The underlying reasons for domestic terrorism are diverse – the only shared aspect is that individuals become frustrated with the status quo and gradually begin to implement a campaign of systematic violence, often against civilians, as part of a strategy to put pressure on the government of the day and to emphasise its inability to govern.

In Africa, the following countries have seen sporadic acts of domestic terrorism:

- In Nigeria, Boko Haram is a serious challenge to security. The bombing of a bus station in Nyanya on 14 April 2014, for instance, killed more than 70 people in yet another example of the group's ruthlessness.
- In Egypt, the bombing of a church in Alexandria just after midnight on 1 January 2011 left 21 people dead and a reported 97 people injured. The attack was an indication of growing sectarian marginalisation and frustration.
- The Lord's Resistance Army has made sporadic attacks against civilians in northern Uganda, southern Sudan and the western Democratic Republic of the Congo (DRC).

It is important to acknowledge that domestic terrorism occurs as a result of domestic circumstances. African countries are therefore encouraged to address issues that not only have an impact on their vulnerability to domestic terrorism but also increase their vulnerability to transnational terrorism. Since the two are interrelated, in addressing related domestic circumstances countries will make it

difficult for domestic and transnational agents of terrorism to operate, justify the use of terror tactics and recruit new followers to their cause. This is part of a long-term strategy and requires the involvement of security forces and intelligence agencies within the framework of a broader objective.

State terrorism is part of domestic terrorism when state actors (police, the military, etc.) resort to acts of terror against their own nationals, often through a third force, frequently to justify harsher action against political opponents.

5.1.2 State terrorism

State terrorism implies that governments use terrorism to achieve a strategic objective for a number of reasons:

- It is inexpensive
- It has limited consequences
- States can distance themselves from culpability in a terrorist attack; they can cover their involvement, disclaim responsibility, or even escape reprisal attacks
- It can be successful
- Weaker states can use asymmetric warfare (acts of terrorism) to their advantage
- States can use proxy wars to their advantage

Briefly, the following categories of support are available to states:

- Ideological support
- Financial support
- Military support
- Operational support
- Support to execute acts of terrorism
- Direct involvement in the execution of acts of terrorism

State-sponsored terrorism therefore includes the following:

- Moral support, particularly through ideological guidance
- Technical support through logistical assistance

- Selective participation
- Active participation through joint operations

5.1.3 International terrorism

International terrorism comprises acts – instigated by a third party – that have clear international consequences. These acts include incidents where terrorists cross national borders to strike at foreign targets or select victims or targets because of their connections to a foreign country (for example, diplomats or local executives). International terrorism is broadly associated with the Cold War, when acts of terrorism were carried out by individuals or groups controlled by a sovereign state.

5.1.4 Transnational terrorism

Transnational terrorism is the use or threat of any act of violence, for political purposes by any individual or group, whether acting for or in opposition to established governmental authority, when such action is intended to influence the attitudes and behaviour of a target group wider than the immediate victims and when its ramifications transcend national boundaries, whether through the nationality or foreign ties of its perpetrators, its location, the nature of its institutional or human victims, or the mechanics of its resolution.

In contrast to international terrorism, where state actors commit acts of terrorism, autonomous non-state actors, irrespective of support from sympathetic states, carry out acts of transnational terrorism. Terrorism is transnational through the nationality or foreign ties of its perpetrators, and when its location, victims, mechanics of resolution and/or ramifications transcend national boundaries.

Africa's role in transnational terrorism is receiving increasing attention due to the involvement of African nationals in transnational terror networks and the use of African countries to facilitate attacks in others.

The US embassy bombings in Dar es Salaam and Nairobi on 7 August 1998, the Westgate Mall bombing in Nairobi, and the bombing of the United Nations (UN) headquarters in Abuja are some of the best-known examples of acts of transnational terrorism on the continent. These are, however, not the only incidents where targets extended beyond domestic terrorism – that list is extensive.

5.2 Distinctions based on motivation

5.2.1 Political ideology

Political terrorism can broadly be defined as the use or threat of terror by a state or a group outside government in pursuit of a set of ideological objectives. Essentially, political terrorism embodies violence or the threat of violence against the state, its representatives or those associated with it, in order to achieve political goals. Terrorism used as a modus operandi by political groups reflects their inability to achieve their political objectives through legitimate means. Both left-wing and right-wing groups form part of this spectrum.

5.2.2 Religion

'Religious terrorism' can broadly be described as the use of terrorism for a religious purpose. Religiously motivated terrorist groups believe they know what is 'good' (or what is sanctioned by their god or beliefs), and that this knowledge obligates them to destroy the evil and the unjust, according to their own perceptions of good and evil – in other words, the use of violence is religiously sanctioned and justified. Religion-based terrorism is far more violent than non-religious or secular terrorism, since religion is used to legitimise or justify the use of violence.

Religious groups have considerable impact on socio-political issues: religion can be used as a vehicle or ideology of opposition and as a justification to protect the spiritual and even material interests of a particular community. The manner in which acts of religious terrorism are committed varies from religion to religion and culture to culture.

5.2.3 Ecoterrorism

The term ecoterrorism points to coordinated acts of violence directed to achieve environmental or ecological objectives. Many developed countries have experienced forms of ecoterrorism. For example, multinational corporations such as Tarmac, Costain and ARC (a unit of the Hanson conglomerate) have been targeted by eco-activists. Companies not only face financial threats from highly sophisticated, well-organised eco-organisations but are also subject to terrorist tactics, such as bomb threats and the intimidation of their staff. British police, for example, investigated the tactics used by underground eco-groups, which distribute leaflets with instructions on how to assemble homemade explosives. In the US, Earth First was established

in the 1980s, focusing on nuclear facilities and associated electrical systems. In 1986, this group was responsible for a successful attack on the Palo Verdes nuclear facility's transmission lines in the US. An increase in radical environmental movements, and the acts of terrorism associated with them, can be expected, particularly in light of the impact of global warming on the environment.

5.2.4 Issue-motivated terrorism

Groups that coalesce around various social issues (such as racial equality, pro- and anti-abortion, animal rights and nuclear issues), environmental concerns, land and economic rights and other matters impinging on the public conscience, generally operate within the bounds of legitimate democratic dissent. However, in certain cases these pressure groups exceed the bounds of legitimate protest. This form of terrorism can be considered the least serious form of random violence against the public. In some cases issue-motivated terrorism may also include elements of religiously motivated terrorism, with reference to fundamental interpretations of religious doctrines.

5.2.5 Narco- or crime-related terrorism

Crime-related terrorism involves the systematic use of terror to secure a group or organisation's hold on material gain. The primary manifestations of force in this form of terrorism include kidnapping, extortion, assassination and murder. When a member of the state apparatus is selected, it is either for direct personal gain or to reduce interference by governmental authorities in their efforts to put an end to criminal activity. Bombings and assassinations initiated by the drug cartels in Colombia or the mafia in Sicily serve as examples.

5.3. Other distinctions

5.3.1 Cyberterrorism

The concept 'cyberterrorism' was originally used to describe the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives. In other words, cyberterrorism refers to the use of computer equipment to intimidate and infiltrate private, public and government computer infrastructure through the

use of viruses or code breaking, with the intention to disrupt services and/or to compromise or destroy data. For further information on cyber terrorism, see Part 7 of this manual.

5.3.2 Lone wolf or lone offender terrorism

Lone wolf terrorism speaks to the growing trend of individuals committing terrorist attacks without direct support from a particular group. Although the individuals may adopt similar political, religious or ideological viewpoints as particular terrorist groups, the attacks they carry out are independent and not as a result of instructions from a group. Lone wolf terrorists may be involved in domestic, transnational or international terrorism, but their autonomous planning and preparation sets their acts apart from other types of terrorism. A prominent example of this trend is when Anders Behring Breivik killed 77 people in two consecutive attacks in Norway on 22 July 2011.

Chapter 6

Tactics and targets of terrorism

6.1 Tactics

It should be noted that not all types of threats and scenarios will be presented or discussed in this section. In summary, prosecutors involved in terrorism cases should pay attention to a few basic elements:

- The type of attack and weapon used will be determined by the objective of the attack and the availability of material – in other words, instead of using a chemical or biological agent (although not excluded) a terrorist could opt for a more accessible and cost-effective modus operandi.
- Terrorists' success lies in their ability to change or adapt at will old and new tactics to their operations. In preparing for a potential act of terrorism, security forces often prepare for the outrageous (which is necessary because terrorists need to think and plan 'outside the box' to successfully execute their attacks and stay ahead), while even a lesser device or threat could result in massive damage, for example, by causing panic that could lead to a stampede.
- The attack could come in the form of discriminate or focused attacks directed at athletes or high-ranking government officials, including heads of state, or indiscriminate attacks intended to cause mass casualties and damage.

Conventional tactics and weapons include:

- Improvised explosive devices (IEDs): These may be delivered by suicide bombers or planted and then detonated later. Bombs are probably the most common indiscriminate tactic for two primary reasons: they pose a low risk to the group/structure when compared to the benefits, and the physical and psychological impact on the target may be substantial.

- Firearms: Their use may be discriminate (for example, specific targets selected in the case of assassinations) or indiscriminate, in which gunmen indiscriminately shoot and kill.
- Knives: Particularly used in decapitation. The use of this tactic by the Armed Islamic Group in Algeria was particularly devastating and effective in intimidating the population, especially people living in smaller towns and villages.
- Kidnapping: This tactic is used to achieve a number of objectives, from extorting ransom (money to fund the organisation and other activities – not for personal financial gain) to propaganda purposes (particularly when hostages are executed and the video material is distributed on the Internet).
- Hijacking methods of transport, including airplanes, ships and boats: The propaganda value of this due to the resultant media coverage was realised early in the development of international/transnational terrorism, as a result of which the first international conventions dealing with terrorism concentrated on the hijacking of airplanes.

Although the use of explosives is often the preferred modus operandi, Africa also has seen the use of firearms in acts of terrorism. This is explained by the availability and flow of illegal firearms as a result of lack of control, inter- and intrastate warfare and instability. The Cold War, the conclusion of civil wars in most African countries, and the fall of Muammar Gaddafi's regime in Libya have contributed to the prevalence of extensive stockpiles of used and unused weapons. Kidnapping for ransom has also seen an increase on the continent, primarily due to the need to finance terrorist organisations.

Unconventional tactics and weapons include:

- The use of a manned intentional aircraft, or the use of remote-controlled airplanes entering the airspace above the venues of major events
- The use of chemical, biological and nuclear weapons
- Cyber weapons and the intentional use of information technology to further terrorist objectives

6.2 Targets

Targets are strategically selected in line with terrorist objectives and means. Before attacking a specific target, those planning the attack will evaluate and analyse valuable and potential targets. Certain factors contribute towards making a good target:

- **Symbolism:** This can be defined as 'something that stands for or suggests something else; especially a visible sign of something invisible'. Keeping in mind that attacking a specific target is a form of communication, deciding on a specific target is, among others, also driven by symbolism: the greater the symbolic value of the target, the more publicity the attack brings to the terrorists and the more fear it generates. For example, in attacking Independence Day celebrations in Nigeria, the Movement for the Emancipation of the Niger Delta (MEND) not only ventured outside its normal area of operation (the Niger Delta) and its traditional target selection (oil companies), it also attacked the Nigerian state, its unity and its accomplishments.
- **Vulnerability:** How protected and secure is the target?
- **Feasibility:** Is the target accessible? Will the intended level of destruction be achieved? How difficult and expensive will it be to rebuild and recover?
- **Impact:** In attacking the target, will the required impact be achieved on its intended victims and those watching the attacks?
- **Risk:** What is the risk of detection and capture? In other words, is the risk worth the effort?
- **Reputation following the attack:** How will the terrorist or terrorist group be perceived after the execution of the attack, considering that 'overkill' (resulting in more than the expected casualties) will reflect negatively on the group or individual?

Valuable targets include:

- Buildings occupied by a large number of people, which causes not only more casualties but also a greater impact on the people experiencing or witnessing the attack
- Vital and/or high-use infrastructure
- Structures that have historical, symbolical, strategic or functional value to a country, or a religious or ethnic group

- Structures that will be difficult to replace
- Structures holding sensitive, historic or rare items
- Structures containing dangerous items, for example explosives, or nuclear facilities

Possible targets include:

- **Government**
  - Office buildings
  - Courts
  - Offices of international agencies or organisations
  - Embassies
- **Public safety**
  - Law enforcement facilities, vehicles and employees
  - Emergency facilities, vehicles and employees
- **Commercial**
  - Hotels
  - Shopping centres
  - Financial and investment centres
  - Corporate headquarters of transnational companies
- **Communication facilities**
  - Radio and TV broadcast facilities
  - Telephone lines
  - Newspapers
- **Industrial**
  - Factories
  - Warehouses
- **Infrastructure**
  - Power plants
  - Transmission lines
  - Generating stations
  - Dams
  - Water reservoirs and distribution facilities

- **Transportation**
  - Bridges
  - Tunnels
  - Buses and terminals
  - Airports and airplanes
  - Subway and railway stations, trains and tracks
  - Major roads
- **Coastal facilities**
  - Cruise and cargo ships and terminals
  - Docks, ports and harbours
  - Shipping containers and facilities
- **Petroleum**
  - Oil wells and platforms
  - Oil pipelines and refineries
  - Oil tankers
  - Natural gas lines and storage tanks
- **Strategic**
  - Military bases
  - Nuclear and toxic waste sites
- **Symbolic**
  - National monuments
  - Sites of historic value
  - Political parties
- **Religious**
  - Synagogues, mosques and churches
  - Religious organisations
  - Cultural centres
- **Entertainment**
  - Stadiums
  - Tourist attractions
  - Resorts
  - Movie theatres
- **Outdoor venues and events**
  - Parades and festivals, including national day celebrations
  - Concerts
  - Sport tournaments
  - International events

Movement for the Emancipation of the Niger Delta

In Nigeria, the 'oil curse' indirectly led to the recourse to violence, including terrorism, against foreign oil companies. With the establishment of MEND, the extent and sophistication of attacks have increased markedly. These attacks are also not limited to foreign oil workers. For example, on 19 April 2006, MEND detonated a car bomb at Bori Camp military base in Port Harcourt that resulted in the death of two people. Although not associated with al-Qaeda, the organisation's leadership has referred to Nigeria as a potential theatre to target the economic interests of the 'Crusaders' (i.e. the US and Western Europe). The strategy is therefore to manipulate and transnationalise a domestic conflict.

On 1 October 2010, Nigeria's Jubilee Independence Day celebrations gave effect to an earlier threat: MEND had sent an email message to media houses warning of its plan to disrupt festivities. Part of the message read: 'With due respect to all invited guests, dignitaries and attendees of the 50th independence anniversary of Nigeria being held today, Friday, October 1, 2010 at the Eagle Square Abuja … MEND is asking everyone to begin immediate evacuation of the entire area within the next 30 minutes. This warning expires after 10:30. Several explosive devices have been successfully planted in and around the venue by our operatives working inside the government security services. In evacuating the area, keep a safe distance from vehicles and trash bins.'

Police confirmed that two car bombs detonated outside the justice ministry in Abuja, while a third, smaller explosion targeted the venue, Eagle Square. In this attack 10 persons were killed and 36 injured, including 11 policemen. The blasts also destroyed six vehicles and damaged 18.

Chapter 7

Conditions conducive to terrorism

As a first step before introducing measures, instruments and policies to prevent and combat terrorism, policymakers and analysts need to understand why an individual decides to commit acts of terrorism and what contributes to this decision. Recognising the importance of identifying and addressing the conditions that might lead to individuals becoming involved in acts of terrorism, the then secretary-general of the UN, Kofi Annan, in his report titled 'Uniting against terrorism: recommendations for a global counter-terrorism strategy', provided the background to the UN Global Counter-Terrorism Strategy adopted on 20 September 2006. Through this initiative the UN introduced a new phase in its counter-terrorism efforts, in that all member states agreed to a common strategic and operational framework to fight terrorism. The strategy presents a basis for a concrete plan of action that rests on four pillars:

- To address the 'conditions conducive' to the spread of terrorism
- To prevent and combat terrorism
- To take measures to build state capacity to fight terrorism
- To ensure the respect of human rights while countering terrorism

The strategy builds on the unique consensus achieved by world leaders at the September 2005 summit to condemn terrorism in all its forms and manifestations.

Essentially, root causes, or 'conditions conducive', refer to external factors (which have an impact on how a person interprets the world around them). Table 1 addresses the key conditions conducive to terrorism.

Table 1: Conditions conducive to terrorism

Category	Elements conducive to terrorism
Political circumstances	Poor governance and rule of law, political exclusion, lack of civil and political liberties and abuses of human rights
Economic circumstances	Economic deprivation and lack of employment, interacting with harmful ideologies to create a potent mix that radicalises elements of the population and creates foot soldiers for terrorist groups
Sociological circumstances, with reference to religious and ethnic discrimination	Perceived ethnic and or religious marginalisation and the fight for self-determination
Counter-terrorism and its impact	Victimisation of elements of the population perceived to breed terrorists and government or security forces' crackdown on these groups
Perceived injustice and international circumstances	Sympathy for persons perceived to be treated unjustly in other countries and the protest against their maltreatment
Geo-strategic conditions	Long, porous borders and other border vulnerabilities that provide access to terrorists

Chapter 8

Introduction to counter-terrorism

The preceding chapters in this section serve as an introduction to the history of terrorism and to broaden understanding of terrorism as a strategy. Parts 2–7 address the various elements involved in countering the threat of terrorism through prosecution.

Prosecutors, police and intelligence officials in counter-terrorism structures play specific roles, most notably to:

- Uncover and prevent acts of terrorism
- Investigate incidents of terrorism
- Assist in building a case within a country and assist other countries, where relevant, to successfully prevent, uncover and investigate acts of terrorism
- Prosecute acts of terrorism

In order to successfully prosecute terrorism cases, prosecutors need to possess an understanding of the tools available in addressing terrorism, as well as the precedent for prosecution set by countries that have been faced with this serious crime.

Prosecutors will gain an understanding of the legal instruments available to states to respond to terrorism in Part 2 of this manual, which deals with domestic legal regimes and processes to address the crime of terrorism. The aim hereof is to provide prosecutors with an understanding of international and regional legal obligations.

Part 3 of the manual sets the basis for the need for co-operation among prosecutors across borders in addressing terrorist acts. Prosecutors are guided in understanding international and regional legal instruments to assist with acquiring

evidence, investigating transnational terrorism cases, submitting requests for mutual legal assistance, freezing assets, transferring criminal proceedings, applying for extraditions, etc.

A state's response to terrorism and/or transnational terrorism is largely defined by its legislation; its domestication of international agreements, treaties, conventions and protocols; and the ability of its law enforcement and governmental authorities to co-operate with each other in gathering admissible, reliable and relevant evidence and arresting and prosecuting those persons alleged to have committed acts of terror, in whatever form. It is for this reason that prosecutors are central in guiding the process in responding effectively to terrorist cases. The role of the prosecutor is discussed in Part 4 of the manual.

Protecting witnesses are crucial in obtaining reliable and admissible witness testimony, which is essential to counter-terrorism initiatives. However, in most terrorism and transnational organised crime cases, witnesses are reluctant to give statements and testify due to legitimate fears for their and/or their families' safety and/or where there are direct threats to their lives. Part 5 deals with witness protection to familiarise prosecutors with the concept of witness protection and to discuss best practices and the UN Guidelines on Witness Protection.

Parts 6 and 7 look at dealing with the financing of terrorism and asset forfeiture as valuable initiatives in addressing terrorism. Prosecutors are provided with an understanding of what amounts to terror-financing; the role of financial intelligence centres and/or agencies; the obligations of financial institutions and entities in freezing, seizing and/or confiscating assets related to terrorist financing; and best practices.

Developing an understanding of technical aspects such as cyberterrorism and electronic evidence is key in prosecuting serious crimes, especially crimes involving cyberterrorism. Part 8 of this manual therefore discusses cyberterrorism and the value of electronic evidence.

Part 2

International and regional legal regimes relating to terrorism

Adv. Shaun Abrahams
National Prosecuting Authority of the Republic of South Africa

Index

Aim and objective

International, regional, multilateral and/or bilateral instruments provide an impetus for states to respond to terrorism through criminal, civil and other sanctions via their domestic legal regimes and processes. It is advisable for prosecutors to acquaint themselves with the relevant instruments in order to:

- Identify and understand the applicable international and regional counter-terrorism instruments
- Familiarise themselves with acts of terrorism and/or offences defined in and created by the relevant instruments
- Ensure respect for human rights and the rule of law in the fight against terror
- Acknowledge and understand the obligations upon states parties to conventions and protocols, as created by the aforementioned instruments in the fight against terror

Chapter 1

International instruments: what are they and what effect do they have?

1.1 Importance of international instruments

It is important for judicial authorities to have a real understanding of what these instruments are, what they do and the obligations they are capable of imposing on a state.

1.2 What is a 'convention' and what are the obligations of a state party under a convention?

The UN Drugs Convention, UN Convention against Transnational Organized Crime (UNTOC), UN counter-terrorism conventions and the UN Convention against Corruption (UNCAC) are examples of multilateral treaties. The term 'convention' is generally used for formal multilateral treaties where there are several parties and participation is open to the international community.

The purpose of this section is to provide an overview of the key defining characteristics of a treaty; the different stages of adoption, signature, ratification and accession; and how treaties are implemented under domestic law, giving them domestic legal effect.

1.3 The Vienna Convention on the Law of Treaties 1969 (Vienna Convention)

The rules governing international treaties used to be based on customary international law, or the general principles of law. However, The Vienna Convention, which entered into force on 27 January 1980, codified these rules and sets out with greater clarity the criteria for the establishment and operation of international treaties.

For the purposes of this manual, the following provisions of the Vienna Convention should be noted:

Article 2(1)(a) of the Vienna Convention defines 'treaty' as 'an international agreement concluded between states in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation'.

The terminology that surrounds the treaty-making process can be confusing. It is therefore important to note the distinction between the various procedural terms, as these can determine whether a state has consented to be bound to the terms of the treaty or not.

1.3.1 Adoption

'Adoption' takes place during the treaty-making process, and is the formal act in which participating states consent to the text of a proposed treaty. Article 9 of the Vienna Convention states:

Article 9(1) 'The adoption of the text of a treaty takes place by the consent of all the States participating in its drawing up …'

Article 9(2) 'The adoption of the text of a treaty at an international conference takes place by the vote of two-thirds of the States present and voting, unless by the same majority they shall decide to apply a different rule.'

1.3.2 Signature

A state that has signed a treaty subject to ratification, acceptance or approval does not establish its consent to be bound. Signature is a process of authentication and reflects the willingness of the state to continue in the treaty-making process by qualifying it to proceed to undertake ratification.

A signatory state to a treaty, while not yet bound to its provisions, is nevertheless obligated not to act in any way that would defeat the object and purpose of a treaty prior to its entry into force. Article 18 of the Vienna Convention states:

> A State is obliged to refrain from acts which would defeat the object and purpose of a treaty when: (a) it has signed the treaty or has exchanged instruments constituting the treaty subject to ratification, acceptance or approval, until it shall have made its intention clear not to become party to the treaty …

1.3.3 Ratification

Ratification is the act whereby a state establishes its consent to be bound to a treaty. In the case of multilateral treaties, the act of ratification is normally done by the deposit of the instruments of ratification to an international organisation or to the UN Secretary-General as the depositary. Article 16 of the Vienna Convention holds:

> Unless the treaty otherwise provides, instruments of ratification, acceptance, approval or accession establish the consent of a State to be bound by a treaty upon:
>
> (a) their exchange between the contracting States;
>
> (b) their deposit with the depositary; or
>
> (c) their notification to the contracting States or to the depositary is so agreed

The process of ratification grants states the necessary time frame required to receive domestic approval for the treaty and to enact domestic legislation giving effect to the treaty.

1.3.4 Accession

Accession has the same legal effect as ratification, but applies when a state becomes party to a treaty after the treaty has already been negotiated and signed by other states. Article 15 of The Vienna Convention outlines when consent of a state to be bound by a treaty is expressed by accession:

1. (a) the treaty provides that such consent may be expressed by that State by means of accession;

   (b) it is otherwise established that the negotiating States were agreed that such consent may be expressed by that State by means of accession; or

   (c) all the parties have subsequently agreed that such consent may be expressed by that State by means of accession.

1.3.5 Reservations to international treaties (Articles 19–23 of the Vienna Convention)

Many international instruments provide for a state to make a reservation as to its provisions. A treaty can prohibit reservations entirely, or allow only specific reservations to be made.

A reservation is a declaration made by a state that excludes or alters the legal effect of specified provisions of the treaty to that state. Reflecting the concept of universality, reservations provide a level of flexibility by enabling states to become parties to multilateral treaties while permitting the exemption or alteration of certain provisions with which the state may not wish or is unable to comply.

The integrity of the treaty remains intact by virtue of Article 19(c) of the Vienna Convention, which states:

> A State may, when signing, ratifying, accepting, approving or acceding to a treaty, formulate a reservation unless: … (c) … the reservation is incompatible with the object and purpose of the treaty.

However, it should be noted that there is considerable debate surrounding what constitutes the 'object and purpose of the treaty', which renders this provision rather opaque in practice.

1.4 Giving domestic effect to international treaties

There are two major approaches as to how international treaties enter into force domestically. This process depends on whether a state subscribes to a monist or dualist system governing the relationship between international and national law.

1.4.1 Monist systems

Monist systems reflect a unitary nature between international and domestic law, whereby both sources of law are considered to belong to the same legal family. Under this approach, when a state ratifies a treaty, the treaty is given the domestic force of law without the need to enact subsequent, implementing legislation. Democratic processes leading to the domestic approval of a treaty are attained during the treaty-making process. Under monist systems, domestic courts and other public bodies refer to the language of the treaty provisions itself as a source of law.

Monist legal systems exhibit variations in approach. These include:

- Systems where only certain treaties are considered to be directly applicable in domestic law and where the treaty provisions share the same level of hierarchy as federal laws, in line with the principle that the latest in time prevails
- Systems where the provisions of certain treaties are superior to later legislation, but which remain lower in status to constitutional provisions
- Systems where the constitution provides for the direct applicability of certain treaties and where treaty provisions are considered superior to all laws

Examples of states with monist legal systems (or variations thereof) include Germany, the Netherlands, the US, Namibia, Senegal and the DRC.

However, even in a monist legal system, the effect of the constitution may be that domestic legislation will be needed to address sanctions before any criminal proceedings can be instituted.

1.4.2 Dualist systems

Dualist systems of law stress that international law and domestic law exist separately, and mostly operate independently of each other. Unlike monist systems, when a dualist state expresses its consent to be bound to an international treaty, the treaty does not directly assume the domestic force of law. Rather, domestic legislation must first be enacted for the treaty to have domestic legal effect.

The process by which an international treaty is given the force of law domestically is referred to as the 'act of transformation'; the treaty is expressly transformed into domestic law by the use of relevant constitutional mechanisms (i.e. an Act of Parliament). For example, the United Kingdom (UK), which is a dualist state, ratified the European Convention on Human Rights (ECHR) in 1951, but ECHR provisions did not have the domestic force of law until the process of transformation, which resulted in the Human Rights Act 1998.

Therefore, in dualist systems, a state can express its consent to be bound by a treaty through ratification, placing the state under international legal obligations, but the same treaty provisions will have no domestic legal effect until the act of transformation. Furthermore, before the act of transformation, domestic courts are not strictly bound by the provisions of the treaty, although in practice such sources of law are considered highly persuasive.

Following the British practice, most Commonwealth states (for example, Nigeria, Malawi and Tanzania) have dualist legal systems. Some have made it their practice to pass a single Act of Parliament simply incorporating their international obligations (even if under more than one instrument) into domestic law, while others have chosen to give effect to the treaty by passing comprehensive domestic legislation, based on the requirements of the treaty, that establishes the necessary infrastructure or systems and creates the necessary offences.

Chapter 2

Introduction to international instruments relating to counter-terrorism

Terrorism and related activities strike at the whole of humankind, threaten the good order of the international community and impinge on the international conscience. These are crimes in whose suppression all states have an interest, as they violate the values that constitute the foundations of peace, security and world public order.

In 1937, the League of Nations, in its Convention for the Prevention and Punishment of Terrorism[2] first attempted to define an act of terrorism in Article 1.1 as 'All criminal acts directed against a State and intended or calculated to create a state of terror in the minds of particular persons or a group of persons or the general public.'[3] In Article 2, terrorist acts included the following:

1. Any wilful act causing death or grievous bodily harm or loss of liberty to:
    a) Heads of State, persons exercising the prerogatives of the head of the State, their hereditary or designated successors;
    b) The wives or husbands of the above-mentioned persons;
    c) Persons charged with public functions or holding public positions when the act is directed against them in their public capacity.
2. Wilful destruction of, or damage to, public property or property devoted to a public purpose belonging to or subject to the authority of another High Contracting Party.
3. Any wilful act calculated to endanger the lives of members of the public.
4. Any attempt to commit an offence falling within the foregoing provisions of the present article.

5. The manufacture, obtaining, possession, or supplying of arms, ammunition, explosives or harmful substances with the view to the commission in any country whatsoever of an offence falling within the present article.

Ideological clashes and disagreements on a universally accepted definition of terrorism have since mired the international discussion on terrorism. UN member states subsequently agreed to the passing of a number of international conventions, protocols and UN Security Council resolutions[4] that impose on member states 'the obligation to make punishable and to prosecute in their domestic legal orders certain classes of actions … defined in each convention by indicating the principle outward elements of the offence. The conventions refrained from terming the conduct terrorist, nor did they point to the purpose of the conduct or motive of the perpetrators. Instead, they confined themselves to setting out the objective elements of prohibited conduct.'[5]

Chapter 3

Universal instruments

The UN's efforts to define terrorism and to obligate member states to develop and promulgate domestic measures to fight terrorism is encapsulated in the following instruments:

- 1963 Convention on Offences and Certain Other Acts Committed On Board Aircraft (Aircraft Convention)
- 1970 Convention for the Suppression of Unlawful Seizure of Aircraft (Unlawful Seizure Convention)
- 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Civil Aviation Convention)
- 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons (Diplomatic Agents Convention)
- 1979 International Convention against the Taking of Hostages (Hostages Convention)
- 1980 Convention on the Physical Protection of Nuclear Material (Nuclear Materials Convention)
- 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (extends and supplements the Montreal Convention on Air Safety) (Airport Protocol)
- 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (Maritime Convention)

- 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation
- 1988 Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf (Fixed Platform Protocol)
- 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection (Plastic Explosives Convention)
- 1997 International Convention for the Suppression of Terrorist Bombings (Terrorist Bombing Convention)
- 1999 International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention)
- 2005 International Convention for the Suppression of Acts of Nuclear Terrorism (Nuclear Terrorism Convention)
- 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (New civil aviation Convention)

3.1 1963 Convention on Offences and Certain Other Acts Committed On Board Aircraft (Aircraft Convention)[6]

This convention applies to acts that affect in-flight[7] safety on board any aircraft[8] registered to a state party but which are committed on board a flight that is not in the territory of the state of registration of the aircraft.[9] The convention does not expressly authorise action to be taken in respect of penal offences of a political nature or that are based on racial or religious discrimination.[10]

Jurisdiction over any offence is conferred on the state party in whose territory the aircraft is registered.[11] In terms of Article 4, another state party may only assert jurisdiction in circumstances where:

- The territory of that state is affected by the offence
- The offence was committed by or against a national or permanent resident of that state
- The offence is committed against the security of that state

- Rules or regulations relating to the flight or manoeuvring of the aircraft in that state has been breached as a result of the offence; and in ensuring adherence to any obligation under a multilateral international agreement

The aircraft commander is permitted to take reasonable measures to restrain a person who is reasonably believed to have committed or is about to commit an offence in order to:

- Protect the safety of the aircraft and/or persons and/or property on board the aircraft
- Maintain good order and discipline on board the aircraft
- Enable him to deliver such a person to the competent authorities and/or to disembark such a person[12]

In order to protect due process, the rule of law and fair trial rights and to promote consular rights, states parties are obligated to assist a detained person to immediately communicate with a representative of his/her state.[13]

The terrorist conventions and protocols discussed also obligate states parties, who, in the exercising of their discretion in relation to the *aut dedere aut judicare* principle[14] decide in favour of prosecuting the offender, to allow the offender to:

- Communicate without delay with the nearest appropriate representative of the state of which he/she is a national, or with a representative of a state that is otherwise entitled to protect his/her rights, or, where the offender is a stateless person, with a representative of the state in the territory of which that person habitually resides
- Receive visits from a representative of that state
- Be informed of the aforementioned rights

The aforementioned rights, albeit phrased somewhat differently and provided for in most, if not all, the terrorist conventions and protocols discussed herein, are intrinsically linked to the rights enshrined in Article 36 of the Vienna Convention,[15] which reads:

> With a view to facilitating the exercise of consular functions relating to nationals of the sending State:

(a) consular officers shall be free to communicate with nationals of the sending State and to have access to them. Nationals of the sending State shall have the same freedom with respect to communication with and access to consular officers of the sending State;

(b) if he so requests, the competent authorities of the receiving State shall, without delay, inform the consular post of the sending State if, within its consular district, a national of that State is arrested or committed to prison or to custody pending trial or is detained in any other manner. Any communication addressed to the consular post by the person arrested, in prison, custody or detention shall also be forwarded by the said authorities without delay. The said authorities shall inform the person concerned without delay of his rights under this sub-paragraph;

(c) consular officers shall have the right to visit a national of the sending State who is in prison, custody or detention, to converse and correspond with him and to arrange for his legal representation. They shall also have the right to visit any national of the sending State who is in prison, custody or detention in their district in pursuance of a judgment. Nevertheless, consular officers shall refrain from taking action on behalf of a national who is in prison, custody or detention if he expressly opposes such action.

The rights referred to in paragraph 1 of this Article shall be exercised in conformity with the laws and regulations of the receiving State, subject to the proviso, however, that the said laws and regulations must enable full effect to be given to the purposes for which the rights accorded under this Article are intended.

In *La Grand (FRG. V US) 2001 I.C.J. 466 (Germany v US),* the International Court of Justice (ICJ) confirmed that Article 36 of the Vienna Conventions does not only provide for state rights and obligations but also creates individual rights. In this matter, Walter and Karl La Grand were German nationals who relocated to the US while still young children in 1967. They were later adopted by a US national, but they remained German nationals at all times, never acquiring US nationality. On 7 January 1982, they were both arrested in the US on charges of murder and attempted armed robbery in relation to a bank robbery during which the bank manager was murdered and another bank employee seriously injured in Marana, Arizona. They were both tried and

convicted by the Superior Court, Pima County, Arizona, which convicted them on 17 February 1984 of murder in the first degree, attempted murder in the first degree, attempted armed robbery and two counts of kidnapping. Both were sentenced to death on 14 December 1984 for the murder conviction. Both Germany and US are parties to the Vienna Convention.

The competent US authorities had failed to invoke Article 36 of the Vienna Convention by, inter alia, (1) failing to provide the two accused with the required information as per Article 36, par 1(b) either after arrest, conviction or sentence; and (2) failing to inform the German Consular Post of the arrest of the two accused.

The two accused unsuccessfully challenged their convictions and sentences, first before the Arizona Supreme Court and later before in the US Supreme Court.

The German Consular Post only became aware of the La Grands' convictions and sentences in June 1992 after being notified thereof by the two accused themselves, who had only recently (at the time) learned of their rights under Article 36 of the Vienna Convention. As a result, and only after being visited and assisted by the German authorities, did the two accused start a third attempt to have their convictions and sentenced set aside, one of the grounds being the US authorities' failure to notify the German Consulate of their arrest as is required by Article 36 of the Vienna Convention. This attempt, too, was unsuccessful on the rule of 'procedural default', first in January and February 1995 by the US District Court for the District of Arizona, then in January 1998 when the US Court of Appeal confirmed the decision of the District Court, and last on 2 November 1998 when the US Supreme Court denied any further review of their matter.

The accused were only formally advised of their consular rights by US authorities on 21 December 1998. On 15 January 1999, the US Supreme Court of Arizona ordered the scheduled execution of Karl La Grand for 24 February 1999 and 3 March 1999 for the execution of Walter. Various attempts were made by the two accused and by the German authorities to seek clemency from the death penalty. On 24 February 1999, Karl La Grand was executed. On 2 March 1999, the day before Walter La Grand's execution, Germany filed an application before the ICJ for an order, inter alia, to the effect that:

> The United States should take all measures at its disposal to ensure that Walter La Grand is not executed pending the final decision in these proceedings …

Although the ICJ granted the provisional order on 3 March 1999, Walter La Grand was nevertheless executed later the same day. Germany had, earlier that day, instituted proceedings against the US and the Governor of Arizona in the US Supreme Court, whereby it sought compliance with the order of the ICJ. The US Solicitor-General took the position that an order of the ICJ providing for provisional relief was not binding on the US and hence not a basis for judicial relief. The US Supreme Court dismissed Germany's motion, inter alia, due to jurisdictional barriers under US domestic law. On 27 June 2001, the ICJ found that a state party of a detained person may approach the ICJ for relief and that the US had violated the Article 36 of the Vienna Conventions.

In *Avena and Other Mexican Nationals 2004 I.C.J. 12 (Mex. v US),* the ICJ found that the US had violated its obligations under Article 36 of the Vienna Conventions and thereby the rights of 54 arrested and detained Mexican nationals by its failure to inform the detainees of their rights in terms of Article 36 and its failure to notify the Mexican Consular Post of the arrest and detention of the 54 Mexicans. In this matter, the Government of Mexico initiated proceedings against the US at the ICJ on 9 January 2003, alleging violations of Article 36 of the Vienna Convention in the matter of 54 Mexican nationals who faced the death penalty in the US and seeking a provisional order requiring the US not to take any actions that might prejudice the rights of Mexico or its nationals pending the ICJ's decision on the merits. On 5 February 2003, the ICJ ordered the US to temporarily stay the executions of three of the Mexican citizens on the US death row. On 31 March 2004, the ICJ held, by a vote of 14 to one, that the US had breached Article 36(1) in the cases of 51 of the Mexican nationals, in that it had breached its obligations under Article 36(1)(b) to inform the detained Mexican nationals of their rights, and to notify the Mexican consular post of their detention. In 49 of these cases, the ICJ found that the US had violated its obligations under Article 36(1)(a) by not allowing free communication and access between Mexican consular officers and Mexican detainees, as well as its obligation under Article 36(1)(c) concerning the right of consular officers to visit their detained nationals. In 34 of the cases,

the ICJ held that the breaches of Article 36(1)(b) also violated the US' obligation under Article 36(1)(c) to enable Mexican consular officers to arrange for the legal representation of their nationals.

The ICJ also re-affirmed its ruling in La Grand, to the effect that where there has been a breach of Article 36 rights, the US must allow the review and reconsideration of the conviction and sentence.

In a separate judgement in *Avena and Other Mexican Nationals,* J Sepulveda highlights the nexus between the Miranda warning and Article 36 of the Vienna Convention in which the justice comments as follows:

> There is an intimate link between the Miranda warning and Article 36 in the sense that both aim at correcting a scheme of protection of rights that directly impinge on the fairness of a trial.

and that,

> Fundamental procedural rights become an essential element in the protection of individual rights, transforming a legal instrument into a Constitutional principle. Thus the rights afforded by Article 36 of the Vienna Convention should be considered fundamental to due process.

3.2 1970 Convention for the Suppression of Unlawful Seizure of Aircraft (Unlawful Seizure Convention)[16]

This convention obligates member states to criminalise the hijacking of aircraft. The preamble recognises the serious threat to safety and property, the undermining of people's confidence in the safety of civil aviation, and the urgent need for appropriate measures to be implemented to punish persons who unlawfully seize or exercise control of aircraft in-flight.

Article 1(a) obligates member states to criminalise the conduct of any person who 'unlawfully, by force or threat … or any other form of intimidation, seizes, or exercises control of that aircraft, or attempts to perform any such act, or (b) is an accomplice …' thereto, while Article 2 obligates member states to legislate the most severe penalties for the hijacking of aircraft. The convention is not applicable to the hijacking of military, customs or police aircraft.[17]

Member states are obligated to establish jurisdiction over both the offence and violent acts perpetrated against passengers and crew by the alleged offender in connection with the offence under circumstances where:

- The offence is committed on board an aircraft registered in the territory of that state[18]
- The aircraft on board which the offence is committed lands in that state's territory while the alleged offender is still on board the aircraft[19]
- The offence is committed on board an aircraft leased to a lessee who has his/her principal business or permanent residential address in that state[20]

Most significantly, member states are obligated to create extra-territorial jurisdiction by taking the necessary measures to establish jurisdiction over the offence where:

- The alleged offender is present in the territory of that state
- That state does not extradite him[21] (where the alleged offender is not extradited, states are obligated to submit the matter to their competent authorities for prosecution)[22]

Member states are further obligated to afford one another the greatest measure of assistance in respect of both the investigation and prosecution of such incidents.[23] Member states are also obligated to immediately afford consular rights to a detained and/or arrested person.[24]

3.3 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Civil Aviation Convention)[25]

This convention makes it an offence for any person to unlawfully and intentionally perform any act of violence against a person on board an in-flight aircraft, when this act is likely to endanger the safety of the aircraft or destroy and/or damage it.[26] It is also an offence to place or cause an explosive device or substance to be placed on an aircraft that is likely to damage and/or destroy the aircraft and/or endanger its safety in-flight.[27] The conduct of any person that amounts to an attempt or an accomplice to the aforementioned offences is also criminalised.[28] Member states are obligated to impose severe penalties for the commission of the aforementioned offences.[29]

Member states are obligated to take the necessary measures to establish jurisdiction over the offences under circumstances where:

- The offence is committed in the territory of that state[30]
- The offence is committed against or on board an aircraft registered in the territory of that state[31]
- The aircraft on board which the alleged offence is committed lands in the territory of that state with the alleged offender on board the said aircraft[32]
- The offence is committed against or on board an aircraft leased to a lessee whose principal place of business and/or permanent residence is in the territory of that state[33]
- The alleged offender is present in the territory of that state and it does not extradite him[34]

Member states are obligated to immediately afford consular rights to a detained and/or arrested person to ensure due process and fair trial rights.[35]

3.4 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons (Diplomatic Agents Convention)[36]

This convention recognises that crimes against diplomatic agents and other internationally protected persons not only jeopardise the safety of the aforementioned persons but also create a serious threat to the maintenance of international peace and security and the promotion of friendly relations and co-operation among states.

This convention obligates states parties, under international law, to take appropriate measures to prevent attacks on the person, freedom or dignity of an internationally protected person,[37] and as such to criminalise domestically and legislate severe penalties for the intentional commission of the following categories of offences:[38]

- The murder, kidnapping or other attack on the person or liberty of an internationally protected person
- The violent attack on the official premises, private accommodation or means of transport of an internationally protected person that is likely to endanger his/her person and/or liberty

- A threat or an attempt to commit any of the aforementioned conduct
- Conduct that amounts to participation as an accomplice to any such acts

The convention defines an 'internationally protected person' as:[39]

(a) a Head of State, including any member of the collegial body [who performs] the functions of a head of state under the Constitution of the State concerned, a head of government or a minister for foreign affairs, when if any such person is in a foreign state, as well as members of his family [accompanying] him;

(b) any representative or official of a State or any official or other agent of an international organization of an intergovernmental character who, at the time when and in the place where a crime against him, his official premises, his private accommodation or his means of transport is committed, is entitled pursuant to international law [to] special protection from any attack on his person, freedom or dignity, as well as members of his family forming part of his household.

States parties are further obligated to establish jurisdiction over crimes affecting an internationally protected person in circumstances where:

- The crime is committed in the territory of that state or on board a ship or an aircraft registered in the territory of that state[40]
- The alleged offender is a national of that state[41]
- The crime is committed against an internationally protected person who enjoys the status by virtue of the duties he exercises on behalf of that state[42]
- The alleged offender is present in the territory of that state and it does not extradite him[43]

Article 7 obligates states parties in whose territory the alleged offender is present, and in circumstances where the offender is not extradited, to, without undue delay, submit the case to its competent authorities for the purposes of prosecution in accordance with the laws of that state, while Article 6.2 obligates states parties to afford consular rights to a person detained or arrested for the commission of an offence in contravention of this convention to promote due process and fair trial rights.

3.5 1979 International Convention against the Taking of Hostages (Hostage Convention)[44]

In maintaining international peace and security and the promotion of friendly relations and co-operation among states, this convention recognises that every person has the right to life, liberty and security, and acknowledges that the taking of hostages is an offence of grave concern to the international community and persons who commit such acts must be prosecuted or extradited. This convention calls for the necessity to develop international co-operation among states in devising and adopting effective measures to prevent, prosecute and punish all forms of hostage-taking as manifested in international terrorism.

The offence of hostage-taking is defined in Article 1.1 of the convention as 'any person who seizes or detains and threatens to kill, to injure or to continue to detain another person in order to compel a third party, namely, a state, an international intergovernmental organization, a natural or juridical person, or a group of persons, to do or abstain from doing any act as an explicit or implicit condition for the release of the hostage'. Article 1.2 makes it an offence for persons to attempt to commit hostage-taking and who participate as accomplices thereto.

States parties are obligated to co-operate in the prevention of hostage-taking by taking all necessary measures to prevent the preparation in their respective territories of offences within or outside their respective territories and by exchanging information to prevent the commission of hostage-taking.[45] States parties are also obligated to take the necessary measures to establish jurisdiction over the offence of hostage-taking under circumstances where:

- The offence is committed in its territory or on board a ship or aircraft registered in that state
- The offence is committed by any of its nationals or by a person habitually resident in the territory of that state
- The offence is committed in order to compel that state to do or to abstain from doing any act

- The offence is committed in relation to a hostage who is a national of that state
- The alleged offender is present in the territory of that state and it does not extradite him[46]

In circumstances where an alleged offender is taken into custody for purposes of extradition and/or prosecution, states parties are obligated to immediately afford such a person consular rights.[47]

3.6 1980 Convention on the Physical Protection of Nuclear Material (Nuclear Materials Convention)[48]

The convention criminalises the unlawful possession, use, transfer or theft of nuclear material and threats to use nuclear material to cause death, serious injury or substantial damage to property.[49] States parties are obligated to establish jurisdiction over offences in circumstances where:

- The offence has been committed in its territory or on board a ship or aircraft registered in its state[50]
- The alleged offender is a national of that state[51]
- The alleged perpetrator is present in the territory of that state and that person is not extradited[52]

3.7 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (Airport Protocol)[53]

This protocol supplements the Civil Aviation Convention to include as an offence the conduct of any persons who unlawfully and intentionally use a device, substance or a weapon in:

- Performing a violent act against a person at an international airport that causes or is likely to cause serious injury or death
- Destroying or seriously damaging the facilities at an international airport, including aircraft not in service, or disrupts the services at the airport, where such conduct endangers or is likely to endanger airport safety[54]

3.8 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (Maritime Convention)[55]

In recognising the increase in acts of terrorism, this convention emphasises that unlawful acts against the safety of maritime navigation jeopardises the safety of persons and property and seriously affects the operation of maritime services, which in turn undermines people's confidence in the safety of maritime navigation.

Article 3.1 criminalises the conduct of any person who unlawfully and intentionally:

- Seizes or exercises control over a ship by force or by threat thereof or by any other means
- Performs any act of violence against a person on board a ship when that act is likely to endanger the safe navigation of that ship
- Destroys or causes damage to a ship or to its cargo that is likely to endanger the safe navigation of the ship
- Places or causes to be placed on a ship a device or substance that is likely to destroy or cause damage to the ship or its cargo and that endangers or is likely to endanger the safe navigation of that ship
- Destroys or seriously damages maritime navigational facilities or seriously interferes with the operation thereof, when that conduct is likely to endanger the safe navigation of the ship
- Communicates information that he/she knows to be false, thereby endangering the safe navigation of the ship
- Injures or kills any person during the commission or the attempted commission of any of the aforementioned offences

Article 3.2 also makes it an offence for any person to:

- Attempt to commit any of the aforementioned offences
- Aid and abet any person in the commission of the aforementioned offences or display conduct amounting to that of an accomplice to a person committing any of the aforementioned offences

- Direct a threat aimed at compelling a physical or juridical person to do or to refrain from doing anything that is likely to endanger the safe navigation of the ship

Article 4.2 creates extraterritorial jurisdiction for states parties where the alleged offender is found in the territory of that state party. Article 6 obligates states parties to implement the necessary measures to establish jurisdiction over the aforementioned offences under circumstances where the offence is committed:

- Against or on board a ship carrying the flag of that state at the time of the commission of the offence
- In the territory or territorial waters of that state
- By a national of that state
- By a person who is habitually resident in that state
- When during the commission thereof a national of that state is seized, threatened, injured or killed
- In an attempt to compel that state to do or to abstain from doing anything
- Where the alleged offender is present in the territory of that state and he/she is not extradited (Article 10 obligates states parties to submit a case to its competent authorities for the purposes of prosecution in the event that the alleged offender is not extradited)

States parties are obligated to afford a person, taken into custody for purposes of extradition or prosecution, consular rights in recognition of due process and a fair trial rights.[56] The convention recognises the rules of international law pertaining to the competence of states to exercise investigative or enforcement jurisdiction in respect of ships not flying their flag.[57] States parties are obligated in terms of Article 12 to afford one another the greatest measure of assistance in the criminal investigation and subsequent prosecution of offences under this convention and in accordance with their domestic legislation, while Article 13 obligates states parties to co-operate with each other in the prevention of the commission of offences in this convention by taking the necessary measures to prevent the preparation of the commission of the offences within or outside their territories and to exchange information with affected states parties in accordance with their respective domestic laws.

3.9 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation

This protocol is supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation and in its preamble, inter alia, reaffirms the condemnation of acts, methods and practices of terrorism as criminal and unjustifiable, which jeopardise friendly relations among states, and remain a threat to the territorial integrity and security of states and to international peace and security.

Offences include the conduct of any person who unlawfully and intentionally:[58]

- Acts to intimidate a population or compel a government or an international organisation to do or to abstain from doing any act by:
  - Using against or on a ship or discharging from a ship an explosive, radio-active material or biological, chemical or nuclear weapon/s in a manner that causes or is likely to cause death, serious injury or damage
  - Discharging from a ship oil, liquefied natural gas or other hazardous or noxious substances that cause or are likely to cause death, serious injury or damage
  - Using a ship in a manner that causes death, serious injury or damage
  - Threatening to commit any of the aforementioned offences
- Transports on board a ship:
  - Any explosive or radioactive material, knowing it is intended to be used to cause or as a threat to cause death, serious injury or damage for the purpose of intimidating a population or compelling a government or international organisation to do or to abstain from doing anything
  - Any biological, chemical or nuclear weapon
  - Any source material, special fissionable material or equipment or material especially designed or prepared for the processing, use or production of special fissionable material, knowing that it is intended to be used in a nuclear explosive activity or in any other nuclear activity outside of the safeguards pursuant to the International Atomic Energy Agency Comprehensive Safeguard Agreement
  - Any equipment, material or software or related technology that contributes significantly to the design, manufacture or delivery of biological, chemical or nuclear weapons with the intention of it being used for such purposes

It is also an offence to unlawfully and intentionally transport another person on board a ship knowing that the person has committed an offence in terms of either the convention and its protocol, thereby assisting the person to evade criminal prosecution.[59] In addition, it is an offence when a person:[60]

- Unlawfully and intentionally injures or kills any person in connection with the commission of the offences provided for in the convention or its protocol
- Attempts to commit an offence as set out in the convention or its protocol
- Participates as an accomplice in an offence
- Organises or directs others to commit an offence
- Contributes to the commission of an offence in a group of persons acting with a common purpose with the aim of furthering the criminal activity or criminal purpose of the group while knowing the intention of the group is to commit an offence in terms of the convention or its protocol

States parties are further obligated to take the necessary measures to hold legal entities within their territory or organised under their domestic laws liable where a person responsible for the management or control of such entity commits an offence in terms of the convention.[61] The protocol also amends Article 6.4 of the convention to obligate members to establish its jurisdiction over offences in terms of both the convention and the protocol where the alleged offender is present in the territory of that state and where the alleged offender is not extradited.

3.10 1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf (Fixed Platform Protocol)[62]

This protocol supplements the Convention for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf. It criminalises placing or causing to be placed on a fixed platform a device or substance that is likely to destroy the fixed platform or endanger its safety. It further makes it an offence for any person to threaten to compel a physical or juridical person to do or refrain from doing any act when that threat is likely to endanger the safety of the fixed platform.

In addition, it is an offence for any person to unlawfully and intentionally intimidate a population or to compel a government or an international organisation to do or abstain from the following conduct:[63]

- The use against or on a fixed platform, or the discharging from a fixed platform, any explosive, radio-active material or biological, chemical or nuclear weapon in a manner that causes death, serious injury or damage
- The discharging from a fixed platform oil, liquefied natural gas or other hazardous or noxious substances that cause or are likely to cause death, serious injury or damage
- Threatening to commit any of the aforementioned acts

Article 2 *ter* also makes it an offence where the conduct of a person amounts to:

- Unlawfully and intentionally injuring or killing any person in connection with the commission of the offences provided for in the convention or its protocol
- Attempting to commit an offence as set out in the convention or its protocol
- Participating as an accomplice in an offence
- Organising or directing others to commit an offence
- Contributing to the commission of an offence in a group of persons acting with a common purpose with the aim of furthering the criminal activity or criminal purpose of the group while knowing the intention of the group is to commit an offence in terms of the convention or its protocol

States parties are obligated to establish jurisdiction over offences set out in the convention and the protocol in circumstances where:

- The offence is committed against or on board a fixed platform located on the continental shelf of that state
- The offence is committed by a national of that state
- The alleged offender is present in the territory of that state and he/she is not extradited

3.11 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection (Plastic Explosives Convention)[64]

This convention is concerned with the unlawful use of plastic explosives in terrorist acts and recognises the need to obligate states parties to adopt measures to ensure that plastic explosives are duly marked. As such, the convention obligates states parties to take the necessary measures to prohibit and prevent the manufacture of unmarked explosives within its territories and to prohibit and prevent the movement of unmarked explosives into and out of its territories. States parties are further obligated to take the necessary measures to exercise strict and effective control over the possession and transfer of unmarked explosives.

3.12 1997 International Convention for the Suppression of Terrorist Bombings (Terrorist Bombing Convention)[65]

This convention recognises the increase in terrorist attacks using explosives and other legal devices, the need to enhance international co-operation among states in adopting effective and practical measures and provisions to adequately address and prevent acts of terrorism, and the need to enhance the prosecution and punishment of perpetrators of terrorism in all its forms and manifestations when those acts threaten the maintenance of international peace and security.

The convention obligates states parties to criminalise the following offences under their domestic laws and to impose severe penalties[66] when a person:[67]

- Unlawfully and intentionally delivers, places, discharges or detonates an explosive or any lethal device in, into or against a place of public use, a state or government facility, a public transportation system or an infrastructure facility with the intent to cause death or serious bodily injury and/or with the intent to cause extensive destruction of such a place, facility or system or where such destruction results in or is likely to result in major economic loss
- Attempts to commit the aforementioned offences
- Participates as an accomplice to the aforementioned offences
- Organises or directs others to commit the aforementioned offences
- Contributes to the commission of the aforementioned offences in a group of persons acting with a common purpose

The convention does not apply in respect of: (1) offences committed within a single state; (2) where the alleged offender and the victims are nationals of that state; (3) where the alleged offender is found in the territory of that state; and (4) where no other state has jurisdiction over the offences.[68]

Article 5 obligates states parties to adopt the necessary measures domestically to ensure that criminal acts that are 'intended or calculated to provoke a state of terror in the general public or in a group of persons or particular persons, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature and are punished by penalties, consistent with their grave nature'.

States parties are further obligated to establish jurisdiction over offences in terms of this convention under the following circumstances:[69]

- Where the offence has been committed in the territory of that state
- Where the offence has been committed on board a vessel flying the flag of that state or on board an aircraft registered under the laws of that state during the period of commission of the offence
- Where a national of that state has committed the offence
- Where the offence has been committed against a national of that state
- Where the offence has been committed against a state or government facility of that state abroad, including an embassy or other diplomatic or consular premises of that state
- Where the offence has been committed by a stateless person or a person who is habitually resident in the territory of that state
- Where the offence has been committed in an attempt to compel that state to do or not to do any act
- Where the offence is committed on board an aircraft that is operated by the government of that state
- Where the alleged offender is present in the territory of that state and he/she is not extradited

States parties are further obligated to conduct investigations under their domestic laws where an alleged offender is present in their territory and to ensure the

presence of the alleged offender for the purposes of prosecution or extradition.[70] In circumstances where they do not extradite a person, they are obligated to submit the case to their competent authorities for the purposes of prosecution, irrespective of whether the offence was committed within their territory or not.[71]

States parties must afford one another the greatest measure of assistance in investigating, prosecuting, extraditing and obtaining evidence in offences falling under this convention.[72] In this regard, states parties are obligated to co-operate in the prevention of offences under this convention by:[73]

- Implementing all necessary measures, including the adaption of their domestic laws, to prevent and counter preparations in their territories for the commission of offences within or outside their territories, including prohibiting illegal activities of persons, groups and organisations that encourage, instigate, organise, finance or engage in the commission of offences under this convention
- Exchanging information within the ambit of their domestic laws to prevent the commission of offences under this convention

A political offence or an offence connected thereto or inspired by political motives cannot amount as a defence to extradition, mutual legal assistance or prosecution.[74]

States parties are prohibited from extraditing or rendering assistance by way of mutual legal assistance where it is believed that the alleged offences have been committed on account of that person's race, religion, nationality, ethnic origin or political opinion or where the alleged perpetrator would be prejudiced and/or persecuted for the aforementioned positions.[75]

A person detained pursuant to this convention is guaranteed fair treatment, which includes the enjoyment of all rights and guarantees in conformity with the laws of the state in whose territory the alleged offender is present, the applicable provisions of international law and international human rights law.[76]

3.13 1999 International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention)[77]

This convention obligates states parties to take appropriate measures domestically to combat the direct or indirect financing of terrorism and terrorist organisations. In its preamble the convention recognises that such financing may take place through charitable, social or cultural entities and through unlawful activities such as the illicit

trafficking in arms and drugs, racketeering and the exploitation of persons. It further recognises the need for states parties to adopt appropriate regulatory measures to prevent the movement of funds reasonably believed to be intended for terrorist purposes, without impeding the freedom of legitimate capital movements, and to intensify the exchange of information in relation to the international movement of funds.

Article 2 makes it an offence for any person, directly or indirectly, and unlawfully and wilfully to provide or collect funds with the intention that such funds be used or at least in the knowledge that such funds are to be used either in full or in part to carry out:

- Any act that amounts to an offence under any of the counter-terrorism treaties, listed in the annexure to the convention[78]
- Any act intended to cause death or serious bodily injury to any persons, even persons not taking active part in an armed conflict, where the purpose of such act is to intimidate a population or to compel a government or an international organisation to do or to abstain from doing anything

It is not necessary for the funds to have been utilised in the commission of any offence and in this regard, a person also commits an offence where he/she attempts to commit an offence under this convention and/or participates as an accomplice, organises or directs others to commit an offence or participates in a group of persons acting with a common purpose. States parties are also obligated to adopt the necessary measures to establish the aforementioned offences as criminal offences under their domestic laws and to impose appropriate penalties considering the gravity of the offences.[79]

Article 5 obligates states parties to implement the necessary measures domestically to hold liable legal entities, either criminally, civilly or administratively, within their territory that have committed offences under this convention and, where necessary, to impose monetary sanctions. State parties are further obligated to implement the necessary measures in their respective domestic laws to ensure that criminal offences within the ambit of this convention are not justifiable by considerations of a political, philosophical, ideological, racial, ethnical, religious or other nature.[80]

States parties are obligated to establish jurisdiction over offences within the ambit of this convention under circumstances where the offence:[81]

- Is committed in the territory of that state
- Is committed on board a vessel flying the flag of that state or on board an aircraft registered within the territory of that state at the time the alleged offence is commissioned
- Is committed by a national of that state
- Was directed towards or had resulted in the territory of that state or against a national of that state
- Was directed towards or had resulted against a state or government facility of that state abroad, including diplomatic or consular premises of that state
- Was directed towards or resulted in an offence under this convention that was committed in an attempt to compel that state to do or to abstain from doing any act
- Was committed by a stateless person who is habitually resident in the territory of that state
- Was committed on board an aircraft that is operated by the government of that state
- Was not committed in the territory of that state but where the alleged offender is present in its territory and is not extradited

Article 9 obligates states parties to take the necessary measures domestically to investigate offences under this convention where it has information that the alleged offender is present in its territory. Similarly, states parties are obligated to take the appropriate measures domestically to ensure the presence of an alleged offender for purposes of prosecution or extradition and to afford consular rights to such person without delay after his/her apprehension. Article 10 obligates states parties to refer a case to its competent authorities for the purposes of prosecution without delay where it does not extradite the alleged offender.

Article 8 obligates states parties to take the necessary measures in accordance with their domestic laws to identify, detect, freeze and/or seize any funds used or allocated for the purpose of committing offences under this convention, including any proceeds derived from the commission of such offences, for forfeiture. In terms of Article 12, states parties are obligated to afford the greatest measure of assistance to one another in respect of criminal investigations, extradition

proceedings, obtaining of evidence and the prosecution of offences under this convention.

3.14 2005 International Convention for the Suppression of Acts of Nuclear Terrorism (Nuclear Terrorism Convention)[82]

This convention obligates states parties to criminalise in their domestic laws the conduct of any person who unlawfully and intentionally:[83]

- Possesses radioactive material or makes and/or possesses a device with the intention of causing death or serious bodily injury or to cause substantial damage to property or the environment
- Uses radioactive material or a device or uses or damages a nuclear facility that releases or risks the release of radioactive material with the intent to cause death, serious bodily injury or substantial damage to property or to the environment or with the intent to compel a natural or legal person, an international organisation or a state to do or to refrain from doing something
- Threatens to commit any of the aforesaid offences, or demands a device or a nuclear facility by threat or by use of force
- Attempts to commit any of the offences under this convention or is an accomplice or organises or directs others to commit the same
- Contributes to the commission of any of the offences under this convention in a group of persons acting with a common purpose.

States parties are obligated to domestically ensure that criminal offences within the scope of this convention that are intended or calculated to provoke a state of terror, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature.[84]

Article 9 obligates states parties to establish jurisdiction over offences under this convention under circumstances where the offence:

- Is committed in the territory of the state
- Is committed on board a vessel flying the flag of that state or on board an aircraft registered within the territory of that state at the time of the commission of the alleged offence

- Is committed by a national of that state
- Was directed towards or had resulted in the territory of that state or against a national of that state
- Was directed towards or had resulted against a state or government facility of that state abroad, including diplomatic or consular premises of that state
- Was directed towards or resulted in an offence under this convention that was committed in an attempt to compel that state to do or to abstain from doing any act
- Was committed by a stateless person who is habitually resident in the territory of that state
- Was committed on board an aircraft that is operated by the government of that state
- Was not committed in the territory of that state but where the alleged offender is present in its territory and is not extradited

Article 10 obligates states parties to take the necessary measures domestically to investigate offences under this convention where it has information that the alleged offender is present in its territory. States parties are further obligated to take the appropriate measures domestically to ensure the presence of an alleged offender for purposes of prosecution or extradition and to afford consular rights to such person without delay after his/her apprehension. Article 11 obligates states parties to refer a case to its competent authorities for the purposes of prosecution without delay where it does not extradite the alleged offender.

States parties are obligated to afford the greatest measure of assistance to one another in respect of criminal investigations, extradition proceedings, obtaining of evidence and the prosecution of offences under this convention.[85]

3.15 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (New Civil Aviation Convention)

This convention obligates states parties to domestically criminalise the unlawful and intentional conduct of a person who:[86]

- Performs any act of violence against a person on board an aircraft when that act is likely to endanger the safety of the aircraft
- Destroys an aircraft or causes damage to an aircraft rendering it incapable of flight or committing any act that is likely to endanger its safety in flight
- Places or causes to be placed on an aircraft a device or substance that is likely to destroy or to cause damage to that aircraft rendering it incapable of flight or endangering its safety in flight
- Destroys or damages navigation facilities or interferes with the operation of air navigation facilities in a manner that is likely to endanger the safety of the aircraft while in flight
- Communicates information knowing it to be false and thereby endangering the safety of an aircraft while in flight
- Uses an aircraft in service to cause death, serious bodily injury, serious damage to property or serious damage to the environment
- Releases or discharges from an in-service aircraft any biological, chemical or nuclear weapon or explosive device of radioactive or similar substances in a manner that causes or is likely to cause death, serious bodily injury, serious damage to property or serious damage to the environment
- Uses against all on board an in-service aircraft any biological, chemical or nuclear weapon or explosive or radioactive device or similar substances in any manner that causes or is likely to cause death, serious bodily injury, serious damage to property or serious damage to the environment
- Transports or causes to be transported or facilitates the transport of, on board an aircraft:
  - Any explosive or radioactive material intended to be used to cause or to be used as a threat to cause death, serious injury or damage with the aim of intimidating a population, or compelling a government or an international organisation to do or to abstain from doing something
  - Any biological, chemical or nuclear weapon knowing it to be such a weapon
  - Any source material, special fissionable material, or equipment or material especially designed or prepared for the processing, use or production of such material and knowing that it is intended to be used in a nuclear explosive

activity or in any other nuclear activity not under the safeguards agreement with the International Atomic Energy Agency
    - Any equipment, material, software or related technology that contributes significantly to the design, manufacture or delivery of a biological, chemical or nuclear weapon without lawful organisation
- Using any device, substance or weapon while performing an act of violence against a person at an international airport that causes or is likely to cause serious injury or death, or if such an act endangers or is likely to endanger safety at that airport
- Using any device, destroys or seriously damages the facilities of an international airport or aircraft located thereon or disrupts the services of the airport where such acts endanger or are likely to endanger safety at that airport
- Makes a threat or causes any person to receive such a threat where the threat is credible
- Attempts, organises, directs or participates as an accomplice to an offence under this convention or assists another person to evade investigation, prosecution or punishment while knowing that the person has either committed an offence under this convention or is wanted in respect of an offence or has been sentenced for an offence under this convention

States parties are obligated to establish jurisdiction over offences under this convention under circumstances where:[87]

- The offence has been committed in the territory of that state
- The offence has been committed against all on board an aircraft registered in the territory of that state
- The aircraft on board which the alleged offence has been committed lands in the territory of that state with the alleged offender still on board the aircraft
- The offence has been committed against all on board an aircraft leased to a lessee whose principal place of business or permanent residential address is in that state
- The offence has been committed by a national of that state
- The offence has been committed against a national of that state

- The offence has been committed by a stateless person who is habitually resident in the territory of that state
- The alleged offender is present in the territory of that state and it does not extradite, even though the alleged offence took place in another state

States parties in whose territory the alleged offender is found are obligated to refer the case to their competent authorities for the purpose of prosecution where they do not extradite the alleged offender.[88] States parties are also obligated to guarantee the alleged offender fair treatment and the enjoyment of all rights and guarantees in conformity with their domestic laws, along with applicable provisions of international law, including international human rights law.[89] In this regard, to ensure due process and fair trial rights, states parties are obligated to afford consular rights to the alleged offender immediately after taking him/her into custody. States parties are further obligated to afford the greatest measure of assistance to one another in connection with criminal proceedings that have resulted out of offences under this convention.

Chapter 4

UN resolutions

The following UN resolutions are of importance and are discussed further herein:

- UN Security Council Resolution 1267 (1999)
- UN Security Council Resolution 1373 (2001)
- UN Security Council Resolution 1456 (2003)
- UN Security Council Resolution 1540 (2004)
- UN Security Council Resolution 1566 (2004)
- UN Security Council Resolution 1624 (2005)
- UN Global Counter-Terrorism Strategy [A/RES/60/288]
- UN Security Council Resolution 2133 (2014)

4.1 UN Security Council Resolution 1267 (1999)[90]

Although directed at the activities of the Taliban and Osama bin Laden, this resolution recalls the obligations on states parties to relevant counterterrorism conventions to extradite or prosecute terrorists and thereby preventing states parties from being utilised as safe havens for terrorist and related activities. As such the resolution obligates states to, inter alia:

- Deny permission for aircraft owned, leased or operated by or on behalf of the Taliban to take off from or land within the state's respective territories
- Freeze funds and other financial resources controlled directly or indirectly by the Taliban or that which has been made available for the benefit of the Taliban

In compliance herewith, the resolution established the 1267 Committee of the Security Council to obligate states to comply with its provisions and to analyse and monitor respective states' adherence thereto.

4.2 UN Security Council Resolution 1373 (2001)[91]

This resolution, inter alia:

- Reaffirms that any act of international terrorism constitutes a threat to international peace and security
- Is concerned with the constant increase in acts of terrorism all over the world motivated by intolerance and extremism
- Calls on states to work together to prevent and suppress acts of terrorists by implementing the relevant terrorism international conventions
- Declares that acts, methods and practices of terrorism, and knowingly financing, planning and inciting terrorism are contrary to the purposes and principles of the UN.

States are obligated in terms of the resolution to, inter alia:

- Prevent and suppress the financing of terrorism and related activities
- Criminalise the wilful provision or collection, directly or indirectly, of funds within states' respective territories with the intention or knowledge that such funds are to be used to carry out terrorist acts
- Freeze without delay the funds, financial assets and economic resources of persons and/or entities who commit or attempt to commit or participate in or facilitate the commission of terrorist acts
- Prohibit their nationals or any person and/or entity within their respective territories from, directly or indirectly, making funds, financial assets, economic resources or other related services available for the benefit of persons to commit, attempt to commit, facilitate or participate in the commission of terrorist acts
- Refrain from providing any form of support to persons and/or entities involved in terrorist acts
- Suppress the recruitment of persons as members to terrorist groups
- Eliminate the supply of weapons to terrorists

- Provide early warnings to other states to prevent the commission of terrorist acts by the exchange of information
- Deny safe haven to persons who finance, plan, support or commit terrorist acts
- Ensure that terrorist acts are established as serious criminal offences domestically, incorporating punitive measures that reflect the seriousness of such acts
- Ensure that persons who participate in the financing, planning, preparation or perpetration of terrorist acts or in support thereof are brought to justice
- Afford the greatest measure of assistance to one another in respect of criminal investigations, the obtaining of evidence and criminal proceedings associated with the financing or support of terrorist acts
- Implement effective border controls and measures on the issuing of identity and travel documents, to prevent the movement of terrorists or terrorist groups
- Accelerate the exchange of operational information in line with international and domestic laws and co-operate through bilateral and multilateral treaties to prevent and take action against perpetrators of terrorist acts
- Become parties to the relevant terrorism international conventions and protocols and fully implement the relevant terrorism conventions, protocols and UN Security Council resolutions
- Take the appropriate measures in conformity with international laws before granting access to asylum seekers who may have planned, facilitated or participated in the commission of terrorist acts
- Ensure that political motivation is not recognised as grounds for refusing extradition requests for alleged terrorists

In order to monitor states' obligations under this resolution, the UN Security Council established a Counter-Terrorism Committee (CTC).

4.3 UN Security Council Resolution 1456 (2003)[92]

This resolution, inter alia, reaffirms that:

- Terrorism constitutes one of the most serious threats to international peace and security

- Acts of terrorism are criminal and unjustifiable regardless of their motivation
- A serious and growing danger is terrorists' having access to and use of nuclear, chemical, biological and other deadly materials
- Terrorists are exploiting sophisticated technology, communications and resources for criminal objectives in an increasingly globalised world
- There is an urgent need to strengthen measures to detect and stem the flow of funds and finance for terrorist acts
- Terrorists must be prevented from utilising other criminal activities well established in transnational organised crime, including illicit drug and arms trafficking and money laundering
- Disputes should be resolved peacefully and a climate of mutual tolerance and respect must be created
- In order to defeat terrorism, renewed domestic efforts, as well as the collaboration and active participation of all states and international and regional organisations in conformity with the UN charter and international law, are required.

As such the UN Security Council calls on all states to, inter alia:

- Take urgent action to prevent and suppress all active and passive support for terrorism
- Comply with the relevant UN Security Council resolutions
- Become parties to all the relevant terrorism international conventions and protocols
- Support all international initiatives to combat terrorism and assist each other in the prevention, investigation, prosecution and punishment of acts of terrorism, irrespective of wherever in the world they occur
- Co-operate in the implementation of sanctions against terrorists and their associates
- Take urgent action in denying terrorists and their associates access to financial resources
- Bring to justice persons and entities that finance, plan, support or commit acts of terrorism and provide safe havens, in conformity with the principle of extraditing or prosecuting

- Assist each other in improving domestic capacity to prevent and fight terrorism
- Ensure that any measures taken in combating terrorism comply with all obligations under international law and adopt such measures in accordance with international law, international human rights, refugee law and humanitarian law

4.4 UN Security Council Resolution 1540 (2004)[93]

This resolution is aimed at halting the proliferation of nuclear, chemical and biological weapons and their means of delivery, which constitute a threat to international peace and security. In this regard, the resolution affirms its support for multilateral treaties aimed at eliminating or preventing the proliferation of such weapons and the importance of all states parties to the relevant treaties to implement the same in promoting international peace, security and stability. As such, this resolution obligates states to:

- Refrain from providing any support to non-state actors attempting to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and the respective means of delivery
- Adopt and enforce appropriate effective laws that prohibit any non-state actors from manufacturing, acquiring, possessing, developing, transporting, transferring or using nuclear, chemical or biological weapons and the respective means of delivery
- Take and enforce effective measures domestically to:
  - Prevent the proliferation of nuclear, chemical or biological weapons and their respective means of delivery, including developing same
  - Account for and secure such items in production, use, storage or transport
  - Implement physically protective measures, border controls and law enforcement efforts to detect, deter, prevent and combat the illicit trafficking and brokering in such items, consistent with international law
  - Maintain effective national export and trans-shipment controls over such items

4.5 UN Security Council Resolution 1566 (2004)

This resolution reminds states to ensure that measures taken to combat terrorism comply with all their obligations under international law, international human rights law, and refugee and humanitarian law.

States are called upon to co-operate fully with the:

- CTC, established pursuant to Resolution 1373 (2001)
- Counter-Terrorism Committee Executive Directorate (CTED)
- Al-Qaeda/Taliban Sanctions Committee, established pursuant to Resolution 1267 (1999), along with the Analytical Support and Sanctions Monitoring Team
- Committee established pursuant to Resolution 1540 (2004)

The resolution is binding on all states and is issued in terms of Chapter VII of the UN Charter. It further calls upon all states to, inter alia:

- As a matter of urgency, become parties to the relevant international counter-terrorism instruments, whether or not they are parties to regional conventions[94]
- Co-operate fully and expeditiously to reach consensus in adopting the draft comprehensive convention on international terrorism and the draft international convention for the suppression of acts of nuclear terrorism[95]
- Assist international, regional and subregional organisations to strengthen international co-operation in the fight against terror[96]
- Intensify interaction with the UN, particularly the CTC, in implementation of Resolution 1373 (2001)

This resolution requests the CTC to develop a set of best practices to assist states in implementing Resolution 1373 (2001) in relation to the financing of terrorism, in consultation with relevant international, regional, subregional organisations and UN bodies.[97] The resolution also directs the CTC to, as a matter of priority, visit states (with the consent of the states concerned) to enhance the monitoring of the implementation of Resolution 1373 (2001).[98] In this regard, the CTC is directed to facilitate the provision of technical and other assistance in furtherance of this implementation and to closely co-operate with international, regional and subregional organisations.[99]

In Article 9, the resolution establishes a working group constituted by all the members of the UN Security Council to consider and submit recommendations to the UN Security Council on practical measures to be imposed on individuals, groups or entities that are involved in or associated with terrorist activities. This, inter alia, includes recommendations on more effective procedures to bring such individuals, groups or entities to justice through:

- Prosecution
- Extradition
- The freezing of their financial assets
- Preventing their movement through the territories of member states
- Preventing the supply of all types of arms and related material to them

The resolution further requires the working group to submit recommendations to the UN Security Council on the procedures to be followed for the implementation of these measures.

In Article 10 the working group[100] is requested to contemplate the possibility of the establishment of an international fund to compensate victims of terror and the families of such victims and to submit its recommendations thereon to the UN Security Council. In this regard, funds could be derived from the assets seized from terrorist organisations, their members and/or sponsors.

4.6 UN Security Council Resolution 1624 (2005)

The resolution is deeply concerned with the incitement of terrorist acts motivated by extremism and intolerance. It strongly emphasis the continuation of international efforts to enhance dialogue and broaden understanding among peoples with the aim of preventing the indiscriminate targeting of different religions and cultures and addressing unresolved regional conflicts. To this end, this resolution stresses the importance of the roles of the following industries in enhancing dialogue, broadening understanding, promoting tolerance and coexistence and fostering environments not conducive to the incitement of terrorism:

- Media
- Civil society
- Religious society
- Business community
- Educational institutions

The resolution recalls the right to seek and enjoy asylum as envisaged in Article 14 of the Universal Declaration, along with the non-refoulement obligation upon states under the Refugees Convention[101] and Protocol.[102]

It recognises the importance of an increasing globalised world in which states are required to co-operate in preventing terrorists from exploiting sophisticated technology, communications and resources to incite support for criminal acts.

It further recalls all states' obligations to co-operate fully in the fight against terror in accordance with their obligations under international law to find, deny safe haven and bring to justice any person who supports, facilitates, participates or attempts to participate in the financing, planning, preparation or commission of terrorist acts or who provides safe havens, by invoking the principle of *aut dedere aut judicare*.

As such, in Article 1, all states are called upon to adopt the necessary measures to:

- Prohibit incitement to commit terrorist acts
- Prevent such conduct
- Deny safe haven to any persons against whom credible and relevant information exists

States are further called upon to co-operate in strengthening the security of their international borders by, inter alia, combating the use of fraudulent travel documents and the extent to which they are attainable, and by enhancing terrorist screening and passenger security procedures to prevent suspected terrorists from entering their territories.[103]

Lastly, this resolution calls upon all states to report to the CTC.[104] In this regard, the CTC is directed to:[105]

- Include in its dialogue with states their efforts to implement this resolution
- Work with states to assist in the building of capacity through legal best practices and by promoting information sharing
- Report back to the UN Security Council on the implementation of the Resolution

4.7 UN Global Counter-Terrorism Strategy[106]

The UN General Assembly adopted the UN Global Counter-Terrorism Strategy on 8 September 2006, in which it identifies four key plans of action in fighting and combating the scourge of terrorism across the globe, namely:

- Measures to address conditions conducive to the spread of terrorism
- Measures to prevent and combat terrorism

- Measures to build the capacities of states to prevent and combat terrorism and, in this regard, strengthening the role of the UN
- Measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism

4.8 UN Security Council Resolution 2133 (2014)[107]

This resolution condemns kidnapping and hostage-taking by terrorist groups, particularly for the obtainment of ransom or for political concessions. It calls on member states to prevent terrorists from benefiting directly or indirectly from any ransom payments or political concessions and to take the necessary measures in securing the safe release of hostages.

Chapter 5

Regional instruments in Africa

5.1 The 1999 OAU Convention on the Prevention and Combating of Terrorism[108]

In its preamble, this convention:

- Believes in the principles of international law, the provisions of the Charter of the OAU, the UN Charter and Security Council resolutions on measures aimed at combating international terrorism
- Recognises the need to promote human and moral values on the foundation of tolerance and rejection of all forms of terrorism irrespective of its motivations
- Reaffirms people's legitimate right for self-determination and independence pursuant to the principles of international law
- Desires to strengthen co-operation among member states in combating terrorism, which constitutes a serious violation of human rights, including the right to physical integrity, life, freedom and security, and which impedes social economic development through the destabilisation of states
- Accepts that terrorism cannot be justified under any circumstances and should consequently be condemned, in all its forms and manifestations
- Takes cognisance of the ever-growing links between terrorism and organised crime, particularly the illicit traffic of arms and drugs and money-laundering
- Is, as a result, determined to eliminate terrorism

The convention defines a terrorist act as:[109]

(a) any act which is a violation of the criminal laws of a state party and which may endanger the life, physical integrity of freedom of, or cause serious

injury or death to, any person, any number or group of persons or causes or may cause damage to public or private property, natural resources, environmental or cultural heritage and is calculated or intended to:

(i) intimidate, put in fear, force, coerce or induce any government, body, institution, the general public or any segment thereof, to do or abstain from doing any act, or to adopt or abandon a particular standpoint, or to act according to certain principles; or

(ii) disrupt any public service, the delivery of any essential service to the public or to create a public emergency; or

(iii) create a general insurrection in a state;

(b) any promotion, sponsoring, contribution to, command, aid, incitement, encouragement, attempt, threat, conspiracy, organizing, or procurement of any person, with the intent to commit any act referred to in paragraph (a)(i) to (iii).

States parties hereto have undertaken to, inter alia:[110]

- Review their national laws and establish criminal offences for terrorist acts as defined in the convention
- Prioritise consideration of signing, ratifying or acceding to the international conventions and protocols listed in the annexure to this convention
- Implement the actions as well as the promulgation of legislation on conduct that is criminalised in the international conventions and protocols listed in the annexure to this convention

The struggles waged by peoples in accordance with the principles of international law for liberation or self-determination, including an armed struggle against colonialism, occupation, aggression and domination by foreign forces, cannot be considered as terrorist acts in terms of this convention,[111] and political, philosophical, ideological, racial, ethnic, religious or other similar motives will also not suffice as a justifiable defence against terrorist acts.[112]

States parties are prevented from rendering any direct or indirect assistance to terrorists, including the provision of safe havens, weapons, visas and/or travel documents. States parties are further obligated to adopt the necessary legitimate

measures in their respective endeavours in preventing and combating terrorist acts, which, inter alia, include:

- Preventing their respective territories from being used in the planning, organising or execution of terrorist acts
- Developing and strengthening the detecting and monitoring of illegal cross-border activities
- Promoting the exchange of information and expertise on terrorist acts
- Taking all necessary measures to prevent the establishment of terror support networks
- Ensuring that asylum seekers are not involved in any terrorist and related activities
- Arresting, extraditing or prosecuting perpetrators of terrorist acts in accordance with domestic laws

States parties are obligated to co-operate with each other by:[113]

- Strengthening the exchange of information in relation to terrorist offences and the perpetrators thereof, their means of support, their movement and their modus operandi
- Exchanging information that leads to the arrest of any person charged with a terrorist or related activity and the seizure and confiscation of any weaponry or devices used or intended to be used in a terrorist or related activity

This convention creates jurisdiction over terrorist and related acts for states parties in circumstances where:[114]

- The offence is committed in the territory of that state and the alleged offender is arrested in or outside the territory of that state
- The offence is committed on board a vessel or a ship flying the flag of that state or an aircraft registered under the laws of that state at the time of the commission of the alleged offence
- The offence is committed by a national or a group of nationals of that state
- The alleged offence is committed against a national of that state

- The alleged offence is committed against that state or a government facility of that state abroad, which includes embassies or other diplomatic or consular premises or any other property of that state
- The alleged offence is committed by a stateless person who is habitually resident in the territory of that state
- The alleged offence is committed on board an aircraft that is operated by a carrier of that state
- The alleged offence is committed against the security of that state party
- The alleged offender is present in the territory of that state and he/she is not extradited

States parties are further obligated, under their domestic law, to investigate an alleged offender when such a person is present in their territory and to take the necessary measures to ensure the alleged offender's presence for prosecution.[115] A person against whom such measures are taken will be entitled to consular rights in that he will be entitled to communicate, without any delay, with the nearest representative from his state of nationality or a representative of the state that is entitled to protect his rights or, in the event that the alleged offender is a stateless person, a representative of that state in which he habitually resides. The alleged offender will also be entitled to be visited by a representative of that state, be assisted by a legal representative of his choice and be informed of the aforementioned rights, which shall be exercised in conformity with the domestic laws of the state in whose jurisdiction the alleged offender is.

Part IV of the convention sets out the circumstances and processes to be followed in respect of the extradition of an alleged offender, while Part V sets the same in respect of mutual legal assistance requests and letters of request (*commissions rogatoire*).

5.2 Protocol to the OAU Convention on the Prevention and Combating of Terrorism[116]

This protocol is supplementary to the convention. Its main purpose is to enhance the effective implementation of the convention and give effect to Article 3(d) of the Protocol Relating to the Establishment of the Peace and Security Council of the African Union, having due regard to the need to co-ordinate and harmonise continental efforts in the prevention and combating of terrorism in all its forms and

manifestations, as well as the implementation of all relevant international counter-terrorism instruments.[117]

The protocol obligates states parties to, inter alia, commit themselves to the following:[118]

- Taking all necessary measures to protect the fundamental human rights of people within their respective nations against all acts of terrorism
- Preventing the entry into and the training of terrorist groups in their respective territories
- Identifying, detecting, confiscating and freezing or seizing any funds or assets used or intended to be used in the commission of terrorist acts and establishing a mechanism for such funds to be used in the compensation of victims of terrorist acts and/or the respective families of such victims
- Establishing national contact points in order to facilitate the exchange and sharing of information on terrorists, terrorist groups and activities at regional, continental and international levels, including the co-operation of states for suppressing the financing of terrorism
- Taking appropriate action against the perpetrators of mercenarism
- Strengthening national and regional measures in conformity with the relevant continental and international conventions and treaties that prevent the perpetrators of terrorist acts from acquiring any weapons of mass destruction
- Co-operating with the international community in the implementation of continental and international instruments relating to weapons of mass destruction

Chapter 6

The African Court of Justice and Human and People's Rights

6.1 Protocol[119] and Draft Protocol on Amendments to the Protocol on the Statute of the African Court of Justice and Human Rights[120]

This protocol provides for the establishment of the African Court of Justice and Human and People's Rights and will enter into force 30 days after the deposit of instruments of ratification by 15 member states. Article 16 of the statute provides for the structures to the court, namely:

- A General Affairs section
- A Human and People's Rights section
- An International Criminal Law section

The latter will have three chambers, namely a Pre-trial Chamber, a Trial Chamber and an Appellate Chamber. The General Affairs section will be competent to hear all cases submitted under Article 28 of the statute, with the exception of those offences assigned to the Human and People's Rights section, the International Criminal Law section and as specified. Article 28 includes the offences of:

- Genocide, crimes against humanity and war crimes
- The crime of unconstitutional change of government
- Piracy
- Terrorism
- Mercenarism
- Corruption

- Money-laundering
- Trafficking in persons
- Trafficking in drugs and hazardous wastes
- Illicit exploitation of natural resources
- The crime of aggression

In so far as it is relevant, the offence of 'terrorism' is defined as:[121]

A. Any act which is a violation of the criminal laws of a State Party, the laws of the African Union or a regional economic community recognized by the African Union, or by international law, and which may endanger the life, physical integrity or freedom of, or cause serious injury or death to any person, any number or group of persons or causes or may cause damage to public or private property, natural resources, environmental or cultural heritage and is calculated or intended to:

   1. intimidate, put in fear, force, coerce or induce any government, body, institution, the general public or any segment thereof, to do or abstain from doing any act, or to adopt or abandon a particular standpoint, or to act according to certain principles; or

   2. disrupt any public service, the delivery of any essential service to the public or to create a public emergency; or

   3. create general insurrection in a State.

B. any promotion, sponsoring, contribution to, command, aid, incitement, encouragement, attempt, threat, conspiracy, organizing, or procurement of any person, with the intent to commit any act referred to in sub-paragraph (a)(1) to (3).

C. Notwithstanding the provisions of paragraphs A and B, the struggle waged by peoples in accordance with the principles of international law for their liberation or self-determination, including armed struggle against colonialism, occupation, aggression and the domination by foreign forces, shall not be considered as terrorist acts.

D. The acts by international humanitarian law, committed in the course of an international or none-international armed conflict by government forces or members of organized armed groups, shall not be considered as terrorist acts.

E. Political, philosophical, ideological, racial, ethnic, religious or other motives shall not be a justifiable defense against a terrorist act.

The statute further makes it an offence for any person, who, in relation to any of the offences listed in the statute, inter alia:[122]

- Attempts, incites, instigates, organises, directs, facilitates, finances, counsels or participates as a principal, co-principal, agent or as an accomplice in a collaboration, conspiracy or in an attempt at either
- Aids, abets, is an accessory before or after the fact or participates in any manner in a collaboration, conspiracy or in an attempt at either

The court will not operate retrospectively in respect of offences committed prior to the coming into force of the draft amendment protocol to the protocol and only after a state had become a party to this protocol and statute, after same has come into force.[123] Crimes falling within the jurisdiction of the court will not be subjected to any statute of limitations.[124] Serving heads of African Union (AU) states or governments or persons acting or entitled to act in that capacity or senior state officials will enjoy immunity from prosecution.[125] With the exception of the aforementioned immunity, the protocol also makes provision for individual criminal liability[126] and command responsibility,[127] as well as for corporate liability, with the exception of states.[128] Alleged offenders under the age of 18 years at the time of the alleged offence will not be subjected to the court's jurisdiction.[129]

In addition to the aforementioned, the court may only exercise jurisdiction over offences under circumstances where:[130]

- The state in whose territory the alleged conduct occurred or where the alleged offence was committed on board a vessel or aircraft registered in the territory of the member state
- The alleged offender is a national of that member state
- A national of that member state is a victim of the alleged offence
- Acts were committed extraterritorially by a non-national that threaten the vital interests of that member state

In respect of offences listed in Article 28A of the statute, the court may exercise jurisdiction in circumstances where:[131]

- One or more of the alleged offences are referred to the prosecutor by a state party
- One or more of the alleged offences is referred to the prosecutor by the AU's Assembly of Heads of State and Government or its Peace and Security Council
- An investigation has been initiated by the prosecutor as a result of having received information of the alleged commission of an offence falling within the ambit of Article 28A of the statute

The court's jurisdiction will be complementary to that of national courts and to courts within the regional economic communities where provision has been made for same.[132] Nevertheless, the court will lack jurisdiction in circumstances where:[133]

- The state that has jurisdiction over the matter is investigating or prosecuting the case
- The state having jurisdiction over the case, after investigating it, decides not to prosecute the alleged offender
- The case is of such a nature that it lacks sufficient gravity for further action to be taken by the court

However, in circumstances where the state having jurisdiction over the case is unwilling or unable to carry out the investigation or prosecution, the court will consider the following principles of due process recognised by international law prior to intervening:[134]

- Whether the alleged offender is being shielded from criminal responsibility for offences falling within the jurisdiction of the court
- Whether an unjustified delay in the proceedings has taken place in circumstances inconsistent with the intent to bring the alleged offender to justice
- Whether the proceedings against the alleged offender were or are not conducted impartially or independently in a manner that is inconsistent with the intention to bring the alleged offender to justice
- Whether as a result of a total or substantial collapse or the unavailability of a state's national judicial system, that state is unable to secure the presence of the

alleged offender or obtain the necessary admissible evidence and testimony or is otherwise unable to carry on with the proceedings

The statute, inter alia, also makes provision for the following:

- The enforcement of fines and forfeiture measures[135]
- The pardon or commuting of sentences within the confines of the interests of justice and general principles of law[136]
- The obligation of states parties to co-operate with the court in the investigation and prosecution of alleged offenders of offences falling with in the ambit of the statute, and any other assistance not prohibited by the domestic law of the requested state

Article 22 of the statute provides for the Office of the Prosecutor, which will:

- Consist of the prosecutor and two deputy prosecutors
- Be responsible for the investigation and prosecution of crimes specified in the statute
- Act independently as a separate organ of the court
- Not receive any instructions from any state party, or any other source for that matter
- Have the power to question suspects, victims and witnesses
- Have the power to collect evidence and conduct on-site investigations

Part 3

International co-operation

Ms Arvinder Sambei & Martin Polaine, Global Center on Cooperative Security (UK), and Adv. Johan J du Toit, National Prosecuting Authority of the Republic of South Africa

Index

Aim and objective

Applicable counter-terrorism UN conventions, protocols, UN Security Council resolutions and the AU Convention on the Prevention and Combating of Terrorism, inter alia, call for states to provide the widest level of co-operation in the investigation and prosecution of terrorism, terror-financing and related offences. This call is echoed by the various recent APA declarations.

The aim and objective of Part 3 is for prosecutors to:

- Recognise those international and regional instruments applicable to mutual legal assistance and extraditions
- Understand the processes relating to requests for mutual legal assistance and extraditions
- Understand the international principle of comity
- Understand and appreciate the type and extent of assistance that may or may not be sought
- Understand the legal framework, mechanisms and purpose of freezing assets
- Understand the international obligation and concept of *aut dedere aut judicare*
- Understand the principle of the transfer of criminal proceedings
- Understand the issue of renditions
- Understand the concept of non-refoulement
- Understand the use of Interpol notices

NB: The following chapters set out the broad principles applicable to each of the measures set out therein and provide general guidance for practitioners across the region; they are not an exhaustive study of the relevant international co-operation laws in the region.

Practitioners are urged to familiarise themselves with their own domestic laws on international co-operation and the relevant treaties/ conventions to which they are a state party. The contents of this part of the manual are for guidance only.

Chapter 1

Mutual legal assistance: general principles

1.1 Introduction

Most criminal activity today is either transnational in character and/or contains key transnational elements. As such, investigators and prosecutors must gather evidence across borders. Against this background, the framework and procedures within which both formal assistance (referred to as 'mutual legal assistance', or MLA) and informal co-operation (referred to as 'mutual assistance') are obtained are often bewildering and frequently depend on the attitude and opinions of those on the ground to whom the request is made. With that in mind, what are the real and practical legal issues and difficulties, and what are the solutions?

The major challenges are, increasingly:

- The international mobility of offenders
- Their use of advanced technology and international banking for the commission of offences
- A framework of prosecutorial and law enforcement co-operation that is often slow, unwieldy and, in many regions, still lacking the networks of practitioners and officials necessary to facilitate the process

Readers should always bear in mind that it is more necessary than ever for law enforcement and judicial authorities to co-operate with and assist each other in an effective way if investigations, prosecutions and judicial proceedings are to run their true course.

Practitioners should be aware that many states have enacted laws to enable them

to provide assistance to foreign jurisdictions and, increasingly, have obligated themselves to do so in treaties (both multi- and bilateral) or agreements on MLA in criminal matters. Such treaties or agreements usually list the kind of assistance to be provided, the requirements that must be met for affording assistance, the obligations of the co-operating states, the rights of alleged offenders and the procedures to be followed for submitting and executing the relevant requests.

Chapter 2

Mutual legal assistance (judicial) and administrative (informal) assistance

2.1 Definitions

Mutual legal assistance or MLA, sometimes known as 'judicial assistance', is the formal way in which states request and provide assistance in obtaining evidence located in one state to help in criminal investigations or proceedings in another state. The state making the request is usually referred to as the 'requesting state', while the state to whom the request is made is the 'requested state'.

Administrative assistance is sometimes referred to as 'informal assistance', as it does not involve the issuing of a formal letter of request, which forms the basis of an MLA request.

Practitioners must be aware of the following:

- Mutual legal assistance is designed for the gathering of evidence, not intelligence or other information
- A mutual legal assistance request cannot be made for the arrest of a person. Such a request is strictly the domain of extradition

Chapter 3

Administrative (informal) assistance

Administrative assistance can and should be used:

- In requesting intelligence
- As the first step in any evidential request of complexity, even where it is always the intention to issue a formal letter of request. Prosecutors and investigators sometimes take recourse to MLA without exploring whether informal mutual assistance would, in fact, meet their needs. Prosecutors must thus ask themselves whether they really need a formal letter of request to obtain a particular piece of evidence
- When making evidence-gathering requests to a state where no court order is required in order to obtain the evidence

By beginning on a police-to-police or prosecutor-to-prosecutor basis, the requesting state will:

- Have the opportunity to discuss the form and requirements of the letter with the requested state before the letter is finalised
- Ensure that it addresses all matters that the requested state needs and that avenues of enquiry are narrowed down as much as possible in advance of the formal request
- Assist the authorities in both states to build networks and contacts, as the importance of excellent working relationships being built up and maintained trans-nationally cannot be stressed too greatly
- Reduce the risk of delay

Practitioners must bear in mind that, although administrative assistance is sometimes referred to as 'informal assistance', it does not mean that the form of the evidence obtained is informal or non-evidential; on the contrary, an evidence request complied with administratively/informally should present the evidence in the same form as though it were gathered in answer to a formal letter of request.

The extent to which states are willing to assist even with a formal request varies greatly. In many cases, it will depend on a particular state's own domestic laws, the nature of the relationship between it and the requesting state and, it has to be said, the attitude and helpfulness of those officials to whom the request is made.

Examples of some types of administrative assistance

Although no definitive list can be made of the type of enquiries that may be dealt with informally, some general observations are useful:

- If the enquiry is a routine one and does not require the requested state to seek coercive powers, it may be possible for the request to be made and complied with without a formal letter of request
- Public records, such as land registry documents and papers relating to the registration of companies, may often be obtained administratively. Such documents might even be available as open-source material, so always check
- Potential witnesses may be contacted to see if they are willing to assist the authorities of the requesting state voluntarily
- A witness statement may be taken from a voluntary witness through an administrative request, particularly in circumstances where that witness's evidence is likely to be non-contentious
- Obtaining lists of previous convictions and basic subscriber details from communications and service providers that do not require a court order may also be dealt with in the same, informal way

There are certain key considerations that a prosecutor must keep in mind when deciding whether evidence is to be sought by informal/administrative means from abroad:

- It must be evidence that can be lawfully gathered under the requesting state's law, and there should be no reason to believe that it will be excluded in evidence when sought to be introduced at trial within the requesting state
- It should be evidence that may be lawfully gathered under the laws of the requested state
- The requested state should have no objection
- The potential difficultly in failing to heed these elements might be that (in states with an exclusionary principle in relation to evidence) such evidence will be excluded
- Inappropriate actions by way of informal request may well irritate the authorities of the foreign state, who might therefore be less inclined to assist with any future requests

The golden rule is: *ensure that any administrative informal request is made and executed lawfully.*

To make the administrative process as efficient as possible:

- Maintain a good relationship, i.e. execute lawfully
- Avoid inappropriate informal requests, as this will inevitably frustrate and irritate the authorities of the requested state
- Use informal assistance, rather than legal assistance, if possible; it is invariably quicker
- Use informal assistance to pave the way for formal assistance; in particular, use it to do all the background research so that a focused and targeted formal request of MLA can be made

3.1 Building networks

Obtaining material via informal assistance is likely to be more easily achieved if positive and collaborative relationships have been built with key individuals in other states. Investigators and prosecutors can develop such relationships by arranging joint training courses, mutual exchanges of personnel, and seminars and regional

information-exchange sessions with other states. A more formal approach is the agreeing of a Memorandum of Understanding (MoU) between investigative agencies from two or more states; an MoU may be purely bilateral or regional. Its primary purpose will be to supplement and refine, particularly for practitioners within law enforcement and prosecution, co-operation and the mechanics thereof between the states concerned.

Further progress can be made by appointing law enforcement liaison officers in other states. These liaison officers would have to have access, in accordance with the laws of the host state, to all agencies within the state with relevant responsibilities.

Chapter 4

Formal requests (mutual legal assistance)

Once a decision to issue a formal letter of request has been made, prosecutors or judges should carefully consider the following:

4.1 When should I make the request?

As soon as sufficient grounds emerge to warrant the making of a request abroad and the need for such a request is clear, the letter should be issued. Problems that occur in all jurisdictions in respect of both incoming and outgoing requests are that of timing and delay. A request may take weeks, sometimes months and occasionally even years to execute.

4.2 Does domestic law allow the request to be made?

Prosecutors/judges must ensure that their own domestic laws allow the request that is being made. For instance, a piece of domestic legislation might, in fact, disallow some requests or types of request that many conventions, treaties or other international instruments would appear to allow. In some states, domestic legislation will have primacy. Making a request other than in accordance with domestic law in such circumstances will be to invite challenges or arguments for the exclusion of evidence at a later stage.

4.3 Is the request urgent?

It is important that urgent requests be kept to a minimum and that everyone involved in the process should appreciate that an urgent request is urgent and unavoidably so. If a request is urgent the letter should say so clearly (both in the heading and body of the letter) and in terms that explain the reasons why.

4.4 What is the format of the request?

The requesting authority should compile a letter that is a stand-alone document. It should provide the requested state with all the information needed to decide

whether assistance should be given and to undertake the requested enquiries. Depending upon the nature of those enquiries and the type of case, the requested state may be quite content for officers from the requesting state to travel across and play a part in the investigation.

4.5 What is the legal basis for the request?

Before a formal request can be made and MLA provided, there must be a legal basis. In criminal matters, there is no universal instrument or treaty that governs the gathering of evidence abroad. However, the building blocks for formal requests are the conventions, schemes and treaties that states have signed and ratified.

The legal bases include:

- Multilateral instruments, including general MLA conventions (e.g. the SADC Protocol on Mutual Legal Assistance, the ECOWAS Convention on Mutual Assistance in Criminal Matters, the IGAD Convention on Mutual Legal Assistance in Criminal Matters) or penal instruments (e.g. the UN Drugs Convention, the UN CT conventions and the UN Convention against Corruption)
- Bilateral treaties
- Schemes or voluntary arrangements, such as the Harare Scheme for Commonwealth states
- National law, with or without a requirement for reciprocity
- Reciprocity/comity-focused and -targeted formal requests of MLA can be made

Examples of enquiries where a formal MLA request is likely to be required:

- Obtaining testimony from a non-voluntary witness
- Seeking to interview a possible suspect
- Obtaining account information and documentary evidence from banks and financial institutions
- Requests for search and seizure
- Internet records and the contents of emails
- The transfer of consenting persons into custody in order for testimony to be given

Chapter 5

The form of the letter of request

Prosecutors and prosecuting authorities are recommended to make early contact with the requested state to determine if there are any limitations on the assistance that can be given; for example, some states have reserved the right to refuse judicial assistance when the offence is already the subject of a judicial investigation in the requested state. The key principle must be this: *Regard should always be given to the fact that a requested state will have to comply with its own domestic law, both as regards whether assistance can be given at all and how that assistance is given, if at all.*

5.1 A letter of request checklist

A proposed checklist for the requesting state on what must be included in the letter of request is as follows:

- An assertion of authority by the author of the letter
- Citation of relevant treaties and conventions
- Assurances (i.e. as to reciprocity, dual criminality, etc.)
- Identification of defendant/suspect
- Present position of the criminal investigation/proceedings
- Charges/crimes under investigation/prosecution
- Summary of facts and how those facts relate to the request being made (the description of the facts must be as detailed as possible and should indicate why the evidence being sought is necessary)
- Enquiries to be made

- The assistance must relate to criminal proceedings (whether at an investigative stage or after court proceedings have begun) in the strict and accepted sense; that is to say, an investigation or proceedings against the perpetrators of a criminal offence under ordinary law
- Assistance required
- Signature of the author of the letter

In addition to the above, some states may require:

- A guarantee of a fair trial and respect for the fundamental rights laid down in the International Covenant on Civil and Political Rights (ICCPR) and regional human rights instruments within the legal system of the requesting state
- An assertion that the request does not relate to fiscal, political or military misdemeanours

Chapter 6

Format of the evidence from the requested state

Although a request is executed by the competent judicial authority[137] of the requested state in accordance with its own laws and rules and procedures, often it will be possible for the requesting authority to make an express request that the requested state apply the requesting state's rules of procedure.

If such a request is available to the requesting authority, advantage should be taken of it. The reason is obvious. A fundamental difficulty, often overlooked, is that different states have different ways of presenting evidence. The whole purpose of a request is to obtain useable, admissible evidence. That evidence must therefore be in a form appropriate for the requesting state, or as near as possible to that form as circumstances allow. It should be made clear, therefore, by the requesting state in what form, for instance, the testimony of a witness should be taken. The requested state cannot be expected to be familiar with the rules of evidence gathering and evidence adducing in the requesting state.

Further to the above, instruments may contain a provision to the effect that the method of execution specified in the request shall be followed to the extent that it is compatible with the laws and practices of the requested state. If in doubt, the requesting authority should provide examples of what is required to the requested authority.

Chapter 7

Problems experienced when mutual legal assistance is sought

Problems may be experienced when mutual legal assistance is sought in cases of serious and organised crime, counter-terrorism, corruption, etc.

7.1 Influential target

If an investigation involves an influential politician or business figure in the requested state, or if a powerful suspect in the requesting state has allies in the state where the request is to be made, the assistance sought may never be provided. The requested authority may, for instance, cite 'national interest' or immunities/jurisdictional privilege enjoyed by certain sections of the community (e.g. government ministers or judges).

This challenge is not an easy one to overcome. However, some practical steps can be taken.

- First, as much information and detail should be obtained on who in the requested state may be trusted and what are the most accurate sources of information. It might be that embassies in the requested state will be in a position to answer this, but the requesting state's financial intelligence unit (FIU) might also be able to assist.
- Second, the requesting authority must get to know the requested state itself in the widest sense, particularly its political and legal systems, while putting aside any prejudice or preconceptions. The same applies to the officials themselves with whom will be liaised during the process.
- Third, the requesting state can seek assurances from the requested state. Although assurances are sometimes broken, there is always pressure on a state to ensure that guarantees are respected.

- Fourth, the requested state can be reminded that there is always a next time. The possibility that the requested state today may well be tomorrow's requester is always a powerful motivator; indeed, it is one of the unspoken driving forces in international co-operation.

7.2 Appeals

In some states, the person in respect of whom the MLA request is made is able to appeal against the sharing of evidence with the requesting authority. When such an appeal is available it may cause a lengthy delay. In those European states that have traditionally enjoyed favourable tax and banking conditions, for instance Liechtenstein and Switzerland, an appeal avenue is available in relation to the disclosure of information on financial position etc. In these states, in addition, institutions such as banks may have similar rights of appeal.

7.3 Requests for freezing and confiscation

Requests for the freezing, confiscation and repatriation of proceeds of crime have traditionally caused particular difficulties. UNTOC and the International Convention for the Suppression of the Financing of Terrorism (Financing Convention) have made some significant inroads, while UNCAC has addressed these issues in detail and provided fresh obligations. However, it is still the case that no internationally binding legal instrument sets out a comprehensive mandatory regime for the repatriation of assets.

7.4 Search and seizure

Search and/or seizure generally can be problematic. Essentially, the authority making the request should be careful to provide as much information as possible about the location of the premises, etc. However, it must be remembered that different jurisdictions set different thresholds. Search and seizure is a powerful weapon for investigators. It must be assumed that the requested state will only be able to execute a request and search/seizure if it has been demonstrated that reasonable grounds exist to suspect that an offence has been committed and that there is evidence on the premises or person concerned that goes to that offence. These 'reasonable grounds' should be set out specifically in the letter.

Generally, it will not be enough simply to ask for search and seizure without explaining why it is believed the process might produce evidence. Interference with

property and privacy is justifiable only if there are pressing social reasons, such as the need to prosecute criminals for serious offences. Even if all these factors are addressed, it may well be that the searching of the person and taking of fingerprints, DNA and other samples will have less chance of success in some jurisdictions. It is therefore vital to liaise with the requested state on this point specifically before a request is issued.

Important additional information to include in a request for search and seizure of evidence:

- The full address or a precise description of any place to be searched
- Details of how the place to be searched is connected with the case or the suspected person
- Any information available that indicates that the material requested may be held on computer
- Full details of the specific material or type of material to be seized (it is not usually enough to simply state 'evidence relevant to the investigation')
- A full description of the criminal conduct concerned (requests for search and seizure are generally subject to a need for dual criminality)
- An explanation why the material requested is considered both relevant and important evidence to the investigation or proceedings
- Why the evidence is thought to be on the particular premises or in the possession of the particular person concerned
- Why the material would not be produced to a court in the requested state if the natural or legal person holding the material were ordered to do so by means of a witnesses order/summons (this is to help ensure that the request is less likely to fail or be subject to subsequent legal challenge)
- Appropriate undertakings for the safekeeping and return of any seized evidence
- If it is anticipated that the searching officers may come across confidential material (e.g. medical records or similar that might have special status in the requested state, or legally privileged material) during the course of a search
- Any other information that would be of operational use to the executing authority in connection with the execution of the request

7.5 Investigations and proceedings of sensitivity

As crime becomes increasingly sophisticated and transnational, and as more and more cases involve a link with organised crime, there may be extremely sensitive aspects to an investigation. That sensitive information may also have to be included in a formal request for assistance in order to satisfy the requested authority. At the same time, the disclosure of prospective witnesses and other information that could be exploited by criminals, organised criminals or those who are otherwise corrupt, must be weighed in the balance.

In reality, the system for obtaining MLA globally is inherently insecure. The risk of unwanted disclosure will be greater or lesser depending on the identity of the requested state. When considering the matter, those making the request must have regard to duty of care issues that arise for them. Sometimes, difficulties can be avoided by the issuing of a generalised letter that leaves out the most sensitive information but provides enough detail to allow the request to be executed. If the sensitive detail proves to be needed, the letter may be supplemented by a briefing given personally by, for instance, the requesting prosecutor to the receiving prosecutor. Exceptionally, consideration can be given to the issuing of a conditional request for MLA; in other words, a request that is only to be executed by the requested authority if it can be executed without sensitive information having to be disclosed.

Chapter 8

Practical steps by those intending to make a request to a foreign state

A number of sources (the latest of which is the UN Office on Drugs and Crime's [UNODC] Technical Guide to UNCAC) have addressed the steps that should be taken by a person intending to make an MLA request. A distillation of these is as follows:

- As a practical matter, the prosecutor or judicial authority requesting assistance will need to recognise that the case it is pursuing is much more important to it than it is to the requested state party. It is vital, therefore, that the requesting state makes strenuous efforts to make it as easy as possible for the requested state to respond positively.
- The requesting authority should identify the substantive and procedural requirements in the requested state for the provision of assistance (since this is often very resource intensive, it may be necessary to select the highest priority cases and engage external legal assistance to ensure that the research is thorough and accurate – all the more important therefore that the assistance of the requested state be sought on this).
- The requested state should be contacted directly to ensure that the request is sent to the proper authority.
- Discuss the request informally with the requested state in advance, which may require the submission of a preliminary draft of the request, so that the requested state can draw attention to errors or advise on the best way to make the request.
- After transmission, follow up on the request to ensure it arrives safely, contains no errors and is being dealt with appropriately.

8.1 Matters the prosecutor or judicial authority should keep in mind before issuing the letter

The prosecutor or other judicial authority issuing the letter of request must satisfy him/herself of the following before the letter is issued:

- Whether an offence has been committed or there are reasonable grounds for suspecting this to be so, and which offences are under investigation.
- The subject/s of the investigation.
- The assistance sought and its relevance to the investigation.
- The identity of any competent overseas authority that is, will, or may be able to give assistance (when dealing with a state to which direct transmission is likely, the issuer of the letter should ideally identify the court with jurisdiction over the area where the evidence is sought and the person who is expected to give assistance).
- Is the proposed enquiry permitted by national law in both the requesting and requested state?
- Is the proposed enquiry permitted under the relevant convention, treaty or other international instrument that is being cited within the letter?
- Has enough factual information about the case been given to provide a proper basis for the assistance to be sought?
- Does the assistance sought amount to little more than a 'fishing expedition'? (In particular, if any coercive measures, such as a search warrant, are likely to be needed in the requested state, it is highly likely that a judicial authority will have to be satisfied that the enquiry is more than just speculative, that there are grounds for believing that the evidence exists or can be made available. The issuer of the letter should, therefore, state in the letter of request the basis for believing that this is so and show a legitimate and clear nexus between the facts and the assistance sought.)
- What value will the assistance sought have for the investigation or proceedings? MLA is a time-consuming process, not just for the requesting judicial authority, but also for the executing judicial authority in particular, for

which it can also be both human and financial resource-intensive. The issuer should consider whether the assistance sought is likely to be proportionate to the case, and should explain in the letter of request what bearing the assistance sought will have upon the case.

- Can the assistance be obtained by other means? Judicial authorities should not use MLA for enquiries that could be made by other, less formal, means.
- Can the assistance that is sought be realistically given? Some enquiries that could not be undertaken easily in one state might be relatively straightforward in another. For example, in the case of European business centres, France and Belgium keep centralised banking records, whereas Germany, Switzerland and the UK do not.
- Can the assistance be given in the time available?
- Is the assistance sought likely to produce admissible evidence?
- What are the consequences of issuing a letter of request? Would making the request create unacceptable/unjustifiable security risks? Would seeking assistance risk revealing a sensitive investigation? Some jurisdictions are unable to carry out investigations without notifying those concerned or those being targeted, while others are able to do so. Each jurisdiction will have different criteria governing whether or not secrecy can be maintained.

8.2 Common and avoidable problems: matters to note

One of the concerns most frequently expressed by representatives of the competent judicial authorities of states is of delays in execution, or refusal of requests for inconsistent reasons. There are a number of recurring causes for delay or refusal, which include:

- Letters of request transmitted that lack precision, letters in which there is no nexus between the summary of the facts and the assistance being requested, or poor translation into the language of the requested state.
- Sometimes the evidence requested is unavailable or delayed because, for instance, it is in the possession of a third party, such as a bank, or is 'historical' and therefore archived or destroyed.

- Frequently letters of request fail to set out the contact details of those undertaking the investigation in the requesting state.
- The requesting state should always consider the likely effect in the requested state of executing a request where an ongoing investigation is taking place in the requested state.

Chapter 9

Grounds for refusal

The granting of mutual legal assistance by a state is an exercise of sovereignty. There is, therefore, a general discretion to refuse assistance; although when MLA is sought on the basis of a treaty, where bilateral or multilateral, that discretion is subject to the obligations contained therein.

The principal difficulties are less outright refusal than delay and the often-cumbersome process involved in making and executing a formal request. The international imperative is to encourage states to address concerns they might have in executing a request by adopting measures short of outright refusal. Such measures could include attaching conditions to the execution of a request or postponing execution (where, for instance, the enquiries requested would be likely to prejudice an ongoing domestic criminal investigation in the requested state). Moreover, in circumstances where a state is minded to refuse a request, it should notify the requesting state and give reasons. Where practicable, it should then consult with the requesting state before reaching a final decision (in the hope that the obstacle to assistance can be resolved through discussion). This consultative approach is specifically provided for in the MLA provisions of recent instruments.

Different international instruments contain some common and some different grounds for refusal. Similarly, states vary as to the grounds for refusal set out in domestic law and may take different approaches in relation to the same grounds.

It is, for obvious reasons, a basic principle of MLA that a state can refuse a request if its execution would be contrary to domestic law. Accordingly, those instruments that address MLA often contain a specific provision to that effect. In addition, though, it is always important to ascertain what grounds for refusal are contained within the national MLA law(s) of the state to which a request is to be made.

Whether or not assistance is given in response to an individual request for assistance is a matter for the competent authority of the state from which assistance is sought (usually, but not always, a court or investigating magistrate). If assistance is refused there is usually little if any scope for negotiation.

In practice, refusal is rare and is most likely to occur simply because the request cannot be executed at all, perhaps due to insufficient information to establish the whereabouts of the evidence or a witness. Occasionally assistance may be refused for legal reasons, perhaps because in the receiving state the conduct complained of would not be an offence, the assistance sought would not be lawful, or the subject of the request has already been acquitted or convicted of the same offence.

Given that most MLA requests will be made pursuant to a treaty, it is worthwhile to keep in mind the sort of discretionary refusal powers that MLA treaties and treaties containing MLA provisions provide to contracting states.

It should be noted that some instruments and arrangements addressing MLA contain explicit provisions addressing those discretionary grounds for refusal long recognised as being legitimate reasons to refuse a request for assistance. These include:

9.1 State/public interest

International instruments addressing MLA, whether multilateral or bilateral, will typically contain an explicit provision allowing for assistance to be refused (in connection to a request made in relation to the instrument in question) where providing assistance would prejudice or be detrimental to the requested state's interests. The form of words used varies, but the UN Drugs Convention, at Article 7(15)(c), is a good example.

This reason is not particularly common in practice, except perhaps when national security is engaged. Practitioners will usually realise in advance which cases may trigger it. When such a case arises, the requesting and requested states should consult each other to try to resolve the matter and to strike an appropriate balance between international co-operation and the protection of the national interests of one state. As always with MLA, dialogue is usually the key.

9.2 Lack of reciprocity

The principle of reciprocity provides one of the legal bases for requesting assistance, but a lack of reciprocity is also potential grounds for refusal. Some states will afford assistance even where the requesting state would not be able to comply with the request were it to be made to it, but other states will not. International instruments recognise this variation in practice and generally provide that the absence of reciprocity is a discretionary ground for refusal in respect of a request made in reliance to the instrument in question.

9.3 Absence of dual criminality

The principle of dual criminality is one that has been transposed into the framework of MLA from extradition law. For MLA purposes, the absence of dual criminality is not an absolute bar to execution in the way it is for extradition. The applicability of the principle in MLA varies greatly from state to state. Many international instruments (and voluntary arrangements, such as the Harare Scheme) expressly provide for it as discretionary grounds for refusal. *It is particularly important, therefore, that the stance of the requested state is canvassed in discussions or consultation before a letter of request is sent.* Some states do not insist on the dual criminality requirement being satisfied, while others make it an essential pre-condition to giving assistance. Confusingly, a third category of state (including the UK) requires dual criminality for coercive measures, such as search and seizure, to be undertaken. To add to the uncertainty, some of those states that insist on dual criminality as a pre-condition nevertheless consider its absence to be discretionary grounds for refusal, while others regard dual criminality as mandatory.

As there is such a range of approaches by states, those who are preparing a letter of request must find out from the requested state exactly what its position is. If it does require the dual criminality requirement to be satisfied, it should be borne in mind that the test is whether the conduct that gave rise to the investigation or proceedings is criminal in both states, not whether the conduct is given the same offence 'label' or criminalised as the same offence in both states. This consideration is of particular importance in relation to those offences that are generally less common – if the requested state does not have the same offence, then the requesting state will need to be thorough in ascertaining whether the alleged conduct fits into the description of an offence in the requested state, even if the title of that offence is markedly different between the two states. An example

of this would be an abuse of function offence in a civil law state that amounts to the common law offence of misconduct in public office.

It should be kept in mind that the 'modern' international approach is for states to be encouraged to be as permissive as possible, in other words, to avoid refusal whenever they can.

9.4 Tax (fiscal) offences and bank secrecy

MLA in cases involving organised or financial crime, terrorism financing, corruption or drug trafficking will usually involve making bank and financial institution documents available. Some states might seek to refuse to give assistance because the material sought falls under bank secrecy laws or regulations. Treaties and laws in many states may also allow refusal of MLA because the offence underlying a request is a tax offence or involves fiscal matters. In practice, though, this is a reason for refusal that is rarely relied upon.

If a judicial authority is faced with a denial of assistance because of fiscal offences or bank secrecy, he/she should carefully examine the provisions of the relevant treaty, if an instrument is forming the basis of the request. Some treaties (e.g., Article 18(8) of UNTOC, Article 12 of the Financing Convention and Articles 46(8) and 46(22) of UNCAC) now prohibit the refusal of assistance on those grounds. Practitioners should also look at the relevant laws of the requested state to ascertain whether the state's claim of bank secrecy is, in fact, justified. Very often, through misunderstanding or mis-application, it will not be.

As a practical, pre-emptive measure, and to attempt to prevent a rejection on the grounds of bank secrecy, the requesting authority should try to obtain as much information as possible through informal means concerning a bank account before sending a request. This will be a difficult task in some investigations, but could prove worthwhile. FIU-to-FIU contact could be one initial route to bring this about.

9.5 Capital punishment/human rights

Many states will refuse MLA assistance if the death penalty may be imposed by the requesting state in the case in question. The determining factor is not whether a state retains the death penalty, but rather whether the offence in question is punishable by death. The principle is harder to apply to a request for MLA than to one for extradition, because the request for MLA will usually occur at an early

stage in a case, when it may be difficult to say with any certainty whether the death penalty may be imposed.

A requesting authority that is faced with the issue will want to consider whether the death penalty is, in fact, applicable to the case. It may then wish to consider whether an assurance can be given that, in the event of conviction, the death penalty will not be imposed in that case. It follows that where, for the requested state, the death penalty is discretionary grounds for denying assistance, the requesting and requested states should consult each other as a matter of priority to try to resolve the issue.

On broader human rights issues, all the authorities involved in making and executing an MLA request are public authorities and, therefore, generally bound by the provisions of the relevant international and regional human rights instruments. They must act compatibly with those when making a request and in giving assistance. Even if the MLA treaty in question does not contain specific bases for refusal on human rights grounds, a request should be refused if its execution would bring about an unjustified breach of a qualified right or a breach of an absolute right.

Each competent authority must keep in mind the practice of regional human rights courts and tribunals, as it is the responsibility of national courts to examine whether certain evidence should be rejected due to measures that violate human rights, and what measures were used in collecting evidence and making that evidence available to the court.

In addition, obligations under other instruments, such as the Convention Relating to the Status of Refugees and the Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment, should not be overlooked.

9.6 Extraterritoriality

For some states, there may be special restrictions in executing MLA requests in cases where the underlying offence occurs outside the territory of the requesting state. This is a particular issue in corruption and organised crime cases, since many states' national laws provide for extraterritorial jurisdiction to enable them to prosecute crimes that have taken place on the territory of another state. Under some treaties and national legislation, there is an express provision that MLA may be granted only if the laws of the requested state provide for the punishment of the same offence committed outside its territory. There is no escaping the potential difficulty that extraterritoriality can cause to some states in this regard;

however, if the principles and any applicable treaties or laws are applied reasonably, international co-operation through MLA should not be unduly restricted.

9.7 *Non bis in idem* (double jeopardy)

Most states will be inclined to refuse an MLA request if the principle of *non bis in idem* (double jeopardy) will be offended in a given case. However, it should be noted that there are a number of variations on the principle from one instrument or treaty to another. Thus, some treaties focus on whether a person has been convicted/punished for the crime in the requesting and/or requested state/s, while others may also consider whether the person has been convicted/punished in a third state. Different treaties also use different formulations: some ask whether the person has been punished, while others look at whether the person has been tried, acquitted or convicted. Hence, if double jeopardy might be an issue in an intended request, practitioners should closely examine the language of the relevant treaty and relevant national laws.

On a practical level, the problem of double jeopardy could be addressed by examining whether there are facts that support a different offence in circumstances where the alleged conduct is distinct from the conduct that was the subject of the earlier acquittal/conviction/punishment.

With the above in mind, the reader is referred to the observations relating to dual criminality set out above: conduct, not 'label', is the important factor common to both dual criminality and *non bis in idem*. For the latter, a practical effect is that if, for instance, a person has been convicted of laundering a bribe, the principle of double jeopardy arguably should not bar further proceedings against that person for accepting the same bribe, since bribe-taking and money-laundering are separate and distinct courses of conduct.

9.8 Political offences, offences of a political character, and persecution

Refusal of MLA on the grounds that the offence is a political one or is of a political character will be unlikely to arise in most financial, drug trafficking or organised crime cases, but can pose a great challenge in corruption investigations. The definition of a political offence is not always clear. Thus, some states might argue that these grounds apply to the prosecution of a former public official who belongs to a political party that is no longer in power.

To address this concern, some instruments such as the UN CT conventions state that the convention offences cannot be political offences. If the relevant instrument has no such provision, then emphasis should be placed on the facts and evidence. In other words, a claim that an offence is of a political character must be founded on sufficient evidence. As with other grounds for refusing assistance, the requesting and requested states should consult with each other on the point.

A state may also deny assistance on the grounds that the request for assistance has been made to prosecute or punish a person on account of his/her sex, race, religion, nationality, ethnic origin or political opinions. As with the claim of political offence, an MLA request should not be denied because of a mere allegation of persecution. The claim ought to be supported by sufficient facts or evidence.

9.9 Relevance of the requested enquiries

It should not be forgotten that a request may be refused (or a supplementary letter required) if the enquiries that are sought do not appear to the requested state to be relevant. It is, therefore, important that the relevance to the overall investigation is clearly set out within the summary of facts.

In deciding whether an enquiry is relevant, a court in the requested state should adopt a wide interpretation and should bear in mind that admissibility will be a matter for the trial court in the requesting state (see the principles confirmed in *Re Mutual Legal Assistance in Criminal Matters* (Court of Appeal, Ontario, Canada),[138] 13 September 1999, in relation to an MLA request submitted by the Russian Federation to Canada).

Chapter 10

Other issues of common difficulty

10.1 Locating suspects abroad

When an extradition request has been made, locating the suspect is of the utmost importance. However, a prosecutor cannot issue a letter of request to locate a suspect for the purposes of arrest, as this is not a request to obtain evidence. If a state makes an MLA request for a person to be interviewed in the requested state as a suspect, the MLA request will inevitably also involve the suspect's being located by law enforcement for the purposes of the interview. This is incidental to the assistance actually being requested (the interview) and is therefore permissible. As indicated below (re: incidental enquiries), the best practice in such a circumstance is for the requesting state to refrain from explicitly requesting that the suspect be located for the purposes of interview, since he/she will be located in any event and, if a request for locating is specifically set out, there is a chance that the requested state might express concern and lose sight of the incidental nature of what is being asked for.

10.2 Distinguishing between evidence and incidental enquiries

It is good practice to itemise in the letter of request the assistance sought. However, this can result in some letters requesting assistance in locating the suspect when in fact the request is that a suspect be located and evidence be gathered from him, such as 'covert DNA' (in other words, DNA obtained from a fingerprint or lip smear on a drinking glass in circumstances without the suspect being made aware of the evidence-gathering exercise that is taking place) or video footage/surveillance. Locating the suspect is necessary but incidental to the assistance sought. To avoid confusion, in such circumstances it may not be necessary to specify that

the suspect be located as this may go without saying. If the executing authorities cannot locate the suspect, they cannot obtain evidence from him.

10.3 A request on behalf of the defence

The defence in a criminal case cannot issue a letter of request itself. At the same time, the defence may have legitimate enquiries that need to be made in another state in order to ensure a fair trial or to put the defendant's case fully. In some jurisdictions the judge will be in a position to issue a letter of request setting out the enquiries that need to be made. In common law states, a defendant can usually apply to a judge to issue a letter after criminal proceedings have been instituted against him/her; in addition, in those states the prosecutor can often issue the letter of request as part of the prosecution's duty to ensure fairness to the accused.

Generally, where a judge is unable to issue a letter or where the investigation is protracted (e.g. large-scale international fraud), it is often more straightforward for the prosecutor to do so (subject to this course of action being consistent with the prosecutor's role and duties in a given state), as the prosecution has extensive machinery for obtaining assistance, something which the defence may not have. Prosecutors should remain aware of this and, when appropriate, liaise with a suspect's legal representatives to establish whether they want any enquiries abroad made on their behalf.

There are clear advantages to the administration if the judge or prosecutor assists the defence in this way, as it can place the prosecutor in a better position to resist defence applications to adjourn or delay proceedings pending enquiries. It also ensures that a case is not dismissed against a defendant solely on the grounds that evidence that might have supported his case is no longer available. Prosecutors must consider these possibilities.

10.4 Requests for intelligence gathering, etc.

It has already been highlighted, but requests for what can only be described as intelligence gathering, or for family liaison visits and anything else that cannot properly be described as evidence gathering, should not be made in a letter of request, unless such enquiries can fairly be said to be incidental to assistance in obtaining evidence that can properly be sought. Obtain this assistance on an administrative, prosecutor-to-prosecutor/police-to-police basis.

10.5 Participation of authorities from the requesting state

The participation of the authorities of the requesting state in the execution of a request is sometimes a sensitive issue that can either increase the efficiency of a investigation or ruin it. The requesting state knows best what evidence and issues are at stake in its enquiry, but its officials cannot operate in foreign territory. Hence, whenever possible, requested states should allow foreign investigators to:

- Be present when hearing witnesses, and allow them to ask questions or indicate what questions to ask (these may be prepared in advance)
- Be present during searches, to help decide what to seize
- Participate in sorting out the documents seized, to indicate which ones are of use

To give an example: Switzerland, a financial centre, has a reputation for not always allowing foreign investigators to be present. However, Swiss legislation does allow it on the condition that foreign investigators commit themselves to not using the information that they obtain while in Switzerland until they receive it through the formal MLA channels.

Taking all the above into account, if it would be of assistance to have the investigating officers present when the enquiries are made, the requested state should be asked expressly in the letter to grant permission for the officers to be present. Depending upon the nature of those enquiries and the type of case, the requested state may be content for officers from the requesting state to play a part. On a request that is largely documentation-driven, however, such as telecommunications service provider records, it may be that such travel would not be of any benefit.

Issues do frequently arise when officials of the requesting state conduct undercover operations in the requested state. One of the obstacles to such operations is that the requesting state loses control over the gathering of information and its use by the requested state, which contradicts the basic principles of international co-operation. Experience tends to show that such undercover operations should only be carried out between states bound by an established and mutual confidence.

10.6 Challenges arising from the right against self-incrimination

Many MLA requests seek to obtain evidence or statements from individuals in the requested state. Upon receiving the request, the requested authorities must often

ask the requesting state whether the witness is a suspect or a target, because national law (and sometimes the constitution) in many states protects witnesses against self-incrimination. Therefore, different rules usually apply to witnesses and suspects.

Sometimes the requested authorities will ask the requesting authorities to offer a witness immunity from prosecution. This is a potential problem in civil law states, where granting immunity to a witness is particularly rare.

10.7 Witness protection

Another related issue is the existence of a witness protection programme. Witnesses under these programmes have agreed to co-operate with the prosecution in a domestic case in the requested state. Since these witnesses are often kept in secret locations, they are not easy to reach for interviews. Early liaison and discussion between the authorities is vital. In exceptional cases, a protected witness may be required to travel to the requesting state to give evidence. Close liaison between authorities must take place in such circumstances, and alternatives, such as video-linked evidence, should be considered if national laws permit. As the availability of technological resources expands, states may wish to consider an international instrument, arrangement or MoU to provide for video-link evidence-giving in criminal cases.

There are many criminal prosecution cases that fail or even fail to start due to witnesses being frightened of retribution or intimidated. The use of fear and/or intimidation against an individual(s) is a tactic that is deployed by criminals to prevent or undermine prosecutions against them. To combat this it is important to have a comprehensive and effective witness protection programme in place.

Such a programme should provide an individual with effective protection and lend appropriate support to individuals who have given or have agreed to give information/evidence. Consideration will also have to be given to the protection of relatives and associates due to the risk to the security of the person.

It is critical that the appropriate authorities providing witness protection understand that such protection can often go beyond just the time of criminal proceedings and in exceptional cases can involve an individual being given a new identity and relocated, perhaps even in another state.

Chapter 11

Legality of special investigative techniques

Increasingly, and in many regions, states are making requests for special investigative means (for example, controlled delivery, surveillance, deployment of undercover agents, etc.) to be deployed by the requested state. Practitioners need to familiarise themselves with MLA procedures and safeguards, including any human rights jurisprudence in the region.

Given the complexity of the issues involved in the deployment of special investigative techniques, those will not be set out in the present manual. The issue is raised for prosecutors and law enforcement agencies to be aware of such requests.

Chapter 12

Practical steps to effective funds/assets restraint and confiscation co-operation

Requests for the restraint and confiscation of funds and other assets are particularly important in combating the financing of terrorism (CFT) cases/economic crime/corruption/drug trafficking etc., and generally require dual criminality and a full justification as to why it is necessary. Without this information, a court will be unable to give an order to freeze assets effectively or register an order to confiscate assets.

The requested authority dealing with the request will make the appropriate applications before the court for the assets to be restrained and should inform the requesting authority as soon as this has been done.

The requesting state must then serve a copy of the restraint order upon the suspect and any other person known to be affected by it once it receives it from the requested state. The requested state's courts will usually require an acknowledgement that this has been completed, otherwise the court may discharge the order.

In most but not all states, the order to freeze assets can be obtained by a court on behalf of a foreign jurisdiction at the investigative stage of criminal proceedings.

12.1 Important additional information to include in an MLA request for the freezing/restraint of property in the requested state:

- The name, address, nationality, date and place of birth, and present location of the suspect(s) or defendant(s) whose criminal conduct has given rise to the anticipated confiscation or forfeiture proceedings
- Details of the criminal investigation

- Details of the law applicable to the investigation and current evidence against the suspects
- Particulars of the property that is intended to be restrained in the requested state, the persons holding it and details of the link between the suspect and the property (this is important if the property to be restrained is held in the name of a third party such as a company or another person)
- Whether prior assistance in the case (including asset tracing assistance) has been provided and, if so, particulars of the requested state's enforcement or other authority involved and details of the assistance already received
- Where applicable, details of any court orders already made in the requesting state against the suspect in respect of his/her property (if a court order has been made, a duly authenticated copy should be included with the request; that is, a true copy of that order certified by a person in his/her capacity as a judge, magistrate or officer of the relevant court of the requesting state, or by an official of the central authority in the requesting state)
- If possible, brief details of all known property held by the suspect outside the requested state
- A certificate or statement issued by or on behalf of the requesting state's central authority, stating:
  - That an investigation has been instituted in that state and has not concluded, or that proceedings have been instituted and are ongoing in the requesting state
  - That the order that the court of the requesting state is expected to make will have the purpose of recovering property or ordering the forfeiture of instrumentalities of crime
  - That any future order that is made can be enforced outside the jurisdiction of the requesting state

- That there is an undertaking or agreement to serve a copy of the order once it has been made upon the suspect and other persons known to be affected by the order

12.2 Important additional information to include in a request for confiscation/forfeiture of property in the requested state:

- The information as outlined above for freezing/restraint applications
- If direct enforcement is sought, an original confiscation or forfeiture order, or a duly authenticated copy of the order
- A certificate or statement issued by or on behalf of the requesting state's central authority, stating:
  - That the order was made consequent on the conviction of the person named in the order
  - That the order is in force, and that neither the order nor any conviction to which it may relate is subject to appeal
  - That all or a certain amount of the sum payable under the order remains unpaid in the territory of the requesting state or that other property recoverable under the order remains unrecovered there
  - That the confiscation order has the purpose of recovering property, or the value of property received in connection with the commission of crime, or, in the case of a forfeiture order, has the purpose of ordering the forfeiture of instrumentalities of crime
  - That the order made can be enforced outside the jurisdiction of the requesting state

Note: The court has to be satisfied that granting a freezing/restraint order or a confiscation/forfeiture order, or giving effect in the requested state to a confiscation order made in the requesting state, will not be incompatible with any rights under such regional human rights instrument as may be applicable. The requesting state, in particular, must consider its request against the provisions of applicable human rights instruments.

12.3 Obstacles to be overcome when seeking forfeiture/ confiscation co-operation in combating the financing of terrorism (CFT) cases

Among the procedural, evidentiary and political obstacles to recovery efforts are:

- Anonymity of transactions impeding the tracing of funds and the prevention of further transfer
- Lack of technical expertise and resources
- Lack of harmonisation and co-operation
- Problems in the prosecution and conviction of offenders as a preliminary step to recovery
- Absence of institutional/legal avenues through which to pursue claims successfully (certain types of conduct not criminalised, immunities, third-party rights)
- Questions of evidence admissibility, type and strength of evidence required, differences regarding in rem forfeiture, time-consuming, cumbersome and ineffective mutual legal assistance treaties when the identification and freezing of assets must be done fast and efficiently
- Limited expertise to prepare and take timely action, lack of resources, training or other capacity constraints
- Lack of political will to take action or co-operate effectively

Chapter 13

Transmission of an MLA request: competent authorities and central authorities

To avoid confusion, it should be noted that a competent authority is a judicial, prosecutorial or law enforcement authority or agency within a state that is authorised under the law of that state to make and/or execute a request for MLA. As indicated below, in some states a competent authority may also be the central authority.

A helpful definition and explanation of what a central authority is, and what its core functions are, may be found in Article 18, para 13 of UNTOC, which specifically references the creation of a central authority for each of the parties to the treaty and makes it compulsory for each party to designate a central authority for the purposes of MLA (this does not seek to preclude direct transmission in appropriate instances, however).

Most states designate a central authority with the power to receive and execute MLA requests or transmit them to the competent domestic authorities for execution, thus providing an alternative to diplomatic channels. The judicial authorities of the requesting state can communicate directly with the central authority.

Some central authorities are also competent to issue a letter of request (e.g., many small jurisdictions, including significant financial centres, have an Attorney General who performs both functions). In some states the central authority is little more than a 'postbox'; in others, it is much more proactive and may, for instance, assure the quality of outgoing requests.

Increasingly, even more direct channels are being used, in that an official in the requesting state can send the request directly to the appropriate official in the other state. Direct transmission, as this is called, is particularly important where a request is of great urgency. A judicial authority should always check whether the national law of the other state with whom she is dealing allows direct transmission in its national

law. However, in most states, even directly transmitted letters will also be copied by the requesting state's competent authority to its central authority for record-keeping and, sometimes, follow-up purposes.

When sending directly, quote the relevant treaty and ensure that the request indicates clearly that the evidence can also be returned directly.

Chapter 14

Receiving foreign material into evidence in the requesting state

Since the procedural and evidence-gathering laws of states differ considerably, the requesting state may require special procedures (such as statements under oath, notarised affidavits, or audio/video-recorded interviews of suspects) that are not recognised under the laws of the requested state.

This may pose a difficulty for a requesting state, since the general principle has always been that the requested state will give primacy to its own procedural law. This principle has caused practical problems, in particular when the requesting and the requested states represent different legal traditions. For instance, the evidence transmitted from the requested state may be in the form prescribed by its laws, but such evidence may be unacceptable under the procedural law of the requesting state.

The modern approach is to allow more flexibility as regards procedures generally. Thus, for example, according to Article 7(12) of the Vienna Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988, a request should be executed in accordance with the domestic law of the requested state party. However, the article also provides that, to the extent not contrary to the domestic law of the requested state party and where possible, the request should be executed in accordance with the procedures specified in the request. Thus, although not going so far as to require that the requested state comply with the procedural form needed by the requesting state, it certainly encourages the requested state to do so. Such a provision may properly be cited in a letter of request in which reliance is being placed on a treaty and the treaty itself contains the provision.

Notwithstanding the above, however, there will be occasions when a piece of evidence gathered pursuant to a letter of request needs to be adduced but is

not in the usual, or prescribed, form for the purposes of the requesting state. It is, therefore, important that a state has, if possible, a provision in its procedural law allowing into evidence material from a foreign state that is not in the usual form. Depending on the demands of national law, some states give their courts discretion on whether to allow such evidence, while others provide that such evidence shall be treated in the same way as though it were a piece of domestically generated evidence produced in the prescribed form.

Chapter 15

Permission to use evidence for other purposes

Evidence provided by the requested state should only be used for the investigation or proceedings stated in the request (rule of specialty). If a requesting state wishes to use evidence for different purposes or to share the evidence with a third state, a new request must be submitted to the central authority that dealt with the original request. This request should explain what the requesting state wishes to use the information for, and why.

Chapter 16

Challenging a refusal by the requested state to execute the letter of request

International co-operation, whether by way of a formal MLA or an informal request, depends in very large part on goodwill, a willingness to assist. What can be done in the event of a refusal to execute a request?

If a letter of request is issued on the basis of comity, without the force of a treaty obligation, the requested state will be at liberty to refuse to execute if it is unwilling to co-operate.

However, if the request is made in reliance upon a treaty, whether bilateral or multilateral, an unjustified refusal will put the requested state in breach of its treaty obligation. Such a course may well risk embarrassment and prompt executive or diplomatic pressure to accede to the request.

Nevertheless, if a state remains steadfast in its refusal there is, in practical terms, little that can be done. Depending on the instrument concerned, the matter may be put before the conference or assembly of the states parties and result in censure, or it might be referred to the organisation or body with 'ownership' of the instrument in question. Either way, rebuke and little more will be the outcome.

A further avenue that a requesting state might go down is to bring an action before the ICJ in The Hague. The ICJ (the principal judicial organ of the UN) handed down a judgement on 4 June 2008 following an action brought by Djibouti against France in respect of a refusal to execute an MLA request. The judgement itself does not assist on any substantive principle relevant for present purposes, as the court found that France, by not giving Djibouti the reasons for its refusal to execute the letter of request, transmitted on 3 November 2004, failed to comply with its international obligation under Article 17 of the 1986 treaty between the two states. The finding of that violation constituted appropriate satisfaction, and the court rejected all other claims by Djibouti. Nevertheless, the case serves to highlight that the ICJ is capable of providing a forum for redress when one state wishes to challenge a refusal by another to execute a letter of request.

Chapter 17

Temporary transfer of a prisoner for purposes of investigation

The law of many states allows for the temporary transfer abroad of prisoners who consent to assist with foreign criminal investigations and proceedings. It is a request provided for specifically in some international instruments and arrangements (e.g. the Harare Scheme).

Prisoners cannot be transferred without their consent. Requests for the temporary transfer of prisoners must be sent to the appropriate central authority. The request must usually be made formally, via a letter of request.

Before agreeing to the transfer, the relevant central authority must be satisfied that the presence of the prisoner is not already required in the requested state for the purposes of investigations or proceedings and that the transfer would not prolong the prisoner's period of detention.

Where the transfer is agreed with the requesting authority, the central authority of the requested state arranges for:

- The prisoner in custody to be taken to a departure point and be delivered into the custody of a person representing the requesting authority
- The prisoner to be escorted back to the requested state by the requesting authority
- The subsequent transfer of the prisoner in custody from the arrival point in the requested state to his place of detention

The costs of escorting and accommodating prisoners from their point of departure in the requested state to their point of return are, in these circumstances, met by the requesting authority (not the requested state, unlike costs of MLA generally).

Additional information to include in a request for temporary transfer of prisoners to the requesting state to assist in the requesting state's investigation:

- Dates on which the presence abroad of the prisoner is required, including the dates on which the court or other proceedings for which the prisoner is required will commence and are likely to be concluded
- Information for the purpose of obtaining the prisoner's consent to the transfer and satisfying the requested authorities that arrangements will be made to keep the prisoner in secure custody, such as:
  - Whether the prisoner will have immunity from prosecution for previous offences
  - Details of proposed arrangements for collecting the prisoner from and returning the prisoner to the requested state
  - Details of the type of secure accommodation in which the prisoner will be held in the requesting state
  - Details of the type of escort available abroad to and from the secure accommodation

Chapter 18

Recognition of criminal judgements of foreign courts

This is a procedure through which a foreign court decision is adapted to the legal system of the state of enforcement, with the prospect of a state recognising a foreign court's decision to apply its legislation, in which case the court's judgement shall not be less favourable for a person convicted abroad.

When acting upon a foreign court's judgement, it should be kept in mind that the purpose of enforcing the foreign court's judgement is not to transform a foreign judgement into a domestic judgement, because that judgement will always remain a foreign judgement. Bearing this in mind, the court should respect the judgement's factual and legal basis. Typically, the prosecutor's office will play an important role in controlling the legality of the court's actions in such cases.

Chapter 19

Sensitive and confidential information: different approaches to release and 'disclosure'

It has already been explained that thought and planning is needed to deal with MLA requests that contain sensitive information. However, a related topic can loom large in cases that involve MLA requests; that is, the topic of the disclosure of sensitive or confidential material to parties in a criminal case.

As might be imagined, there are some differences of approach between practices in common law states and in civil law jurisdictions. The central issue with which we are presently concerned is this: where the requesting state has been provided by the requested state (as a result of an MLA or administrative assistance request) with sensitive or confidential information that is not being adduced as evidence to prove a fact in the case, but has nevertheless come into the possession of the prosecution in the requesting state, how should it be dealt with and how should possible conflicting interests of (1) ensuring a fair trial and (2) maintaining the requested state's confidentiality, be managed?

For clarity, we should first look at general principles. One of the fundamental tenets of the rule of law is the right to a fair trial. This is reflected in the various international and regional and human rights instruments that set out the basic requirements that satisfy the guarantee of the right to fair trial. For present purposes these include:

- The International Covenant on Civil and Political Rights 1966 (Article 14)
- The African Charter on Human and Peoples' Rights 1986 (Article 7)

The right to a fair trial in essence enshrines the need for the defence to be fully informed of the case against the accused and permit him to mount a 'full and robust' defence. As part of the proceedings, therefore, the defendant must be served with the evidence that the prosecution seeks to adduce during the course of the trial and be provided with all relevant material that has come into existence as part of the investigation but upon which the prosecution does not intend to rely.

19.1 Civil law states

The traditional civil law approach is that any material that is gathered as part of the investigative file will be disclosed to the parties to the case (prosecution, defence and *partie civile* [where applicable]), without any distinction being drawn between evidence that the prosecution says supports its case and other material that might support the defence's contentions or take the case as a whole no further. Such disclosure in civil law jurisdictions will usually be subject to the editing or excision of sensitive material before serving it on the defence. That determination is usually made by the investigating magistrate/judge.

In addition, there might also be material, usually intelligence or information, gathered before the investigation file was formally opened. In some civil law states, such material will remain confidential; in others, it is may be disclosed to the parties if it becomes relevant to an issue being decided in the case (such as the grounds for deploying a special investigative technique).

19.2 Common law states

In common law jurisdictions, evidence that the prosecution intends to rely upon as admissible evidence to prove its case is regarded as being part of its case (so-called 'used material') and must be made available to the defence, either by inspection or service, depending on the nature and gravity of the offence alleged.

However, in addition, there will be material gathered by the investigators (both nationally and, increasingly, from abroad) that is not part of the case that will be put forward by the prosecution to the court at trial. Such material is usually referred to as 'unused material' (this may include items that contain sensitive information attracting a claim of public interest immunity).

At common law such material must be disclosed to the defence if it is 'relevant'. The test of relevance is whether the material can be regarded, on a sensible appraisal by the prosecution, (1) to be relevant or possibly relevant to an issue in the case; (2) to raise or possibly raise a new issue whose existence is not apparent from the evidence the prosecution proposes to use; or (3) to hold out a real, as opposed to fanciful, prospect of providing a lead on evidence that goes to (1) or (2).

Some jurisdictions, such as Uganda, Kenya, Australia and the UK, now have a codified approach to such material and its disclosure. However, that codified law largely reflects the traditional common law position.

Chapter 20

Extradition

20.1 Introduction

It is worth stating at the outset: extradition processes and procedures are governed by the domestic law of the requested state. The reader must, therefore, be fully acquainted with:

- The domestic law on extradition
- The treaties/conventions/schemes on extradition that apply to their state: for example, any bilateral or regional agreements. Examples of regional arrangements in Africa include the Southern African Development Community (SADC) Protocol on Extradition,[139] the Intergovernmental Authority on Development (IGAD) Convention on Extradition, and the Economic Community of West African States (ECOWAS) Convention A/P 1.8.94 on Extradition[140]
- Other international instruments that apply, for example, the various UN instruments: the UN counter-terrorism (CT) conventions, UNCAC and UNTOC

20.2 What is extradition?

Extradition is the process by which a state seeks the return of a person accused and/or convicted, usually based on a treaty or voluntary arrangement between the requesting and requested state.

Traditionally, states entered into bilateral extradition treaties; however, as crime has become increasingly transnational in nature (e.g. drug trafficking, serious and organised crime, human trafficking, terrorism, etc.) and travel has become easier, the international community (acting either through the UN General Assembly or regionally) has adopted a number of multilateral treaties or conventions not only to

address the criminal conduct but also to provide states parties with a legal basis for co-operation.

The real advantage of an international or regional instrument can be set out as follows:

- States parties can use the instrument as a legal basis for extradition
- Where there is an existing arrangement between the parties, but the convention crimes are not included as extradition offences, the convention seeks to fill that gap
- Each state party will be fully aware of the obligations contained within the convention, including any reservations/declarations that a state party may enter

Who can be the subject of an extradition request?

A request for extradition can be made for:

- A person accused
- A person convicted and sentenced
- A person convicted but not yet sentenced

When can a request for extradition be made?

An extradition request can be made where:

- A person has committed an offence in state A and has fled to state B (practitioners will be more familiar with this practice)
- A person has never been to or visited state A, but the conduct has come within the wider criminal jurisdiction of that state: with the rise of transnational crime, states, in particular common law states, have begun to assert a wider jurisdiction, with the result that those who may be caught within the reach of such laws have widened. A direct consequence of this wider criminal jurisdiction, for the purposes of extradition, is that there is no longer a need for a person to have fled the jurisdiction; the mere fact that their criminal activity comes within the criminal jurisdiction of a state founds the basis for an extradition request (e.g. foreign bribery, cartel offences, etc.).

20.3 Rendition and surrender

Practitioners will be aware of reference being made to both 'rendition' and 'surrender' as a means of returning those accused or convicted of criminal conduct.

The term 'rendition' is used where there is no formal treaty in existence but an 'arrangement' is agreed and its terms incorporated in domestic legislation (for example, Commonwealth states have the London Scheme for Extradition).[141]

The term 'surrender' applies where states, particularly neighbouring states, simplify the extradition process through a 'backing of warrants' or when it concerns an international tribunal such as the UN tribunals or the International Criminal Court (ICC).

20.4 Legal bases for extradition

The first requisite in any extradition request is that there must be a legal basis for making a request. Broadly speaking this can be:

- Bilateral arrangements
- Regional extradition treaties/arrangements/schemes (e.g. SADC Protocol)
- International instruments (e.g. UN penal conventions)
- Ad hoc arrangements
- Comity (it is also regarded as a potential legal basis, but reliance upon it will present real difficulties and it should therefore be avoided)

Practitioners must be aware that in some instances more than one treaty could apply. Although there is no strict hierarchy of treaties, practitioners should place reliance, first, on any bilateral treaty; if none exists, then on the regional convention. Where neither is in existence, the UN conventions should be considered as the legal basis for the request.

20.5 How extradition starts

There are essentially two ways in which the extradition process may start, namely:

- Provisional arrest
- 'Full' request

20.5.1 Provisional arrest

Provisional arrest is sought when a person is considered to be a flight risk, is transiting a state, or any other urgency, and when it is anticipated that if the person is not arrested, they are likely to leave the jurisdiction.

The provisional arrest process: Practitioners[142] in the requesting state must decide whether there is a genuine or real risk that a person is likely to flee if they are not arrested; if so, a request for the provisional arrest of the individual will usually follow.

The provisional request for arrest is usually submitted via Interpol with an accompanying letter that provides an undertaking that an extradition request will be made.

> The following documents are usually required for a provisional arrest:
>
> - Warrant of arrest (for an accused person) or certificate/record of conviction (for a convicted person)
> - List of charges
> - Description of conduct
> - The relevant law setting out the offence and applicable penalty (this can be incorporated into the letter that provides the undertaking)
> - Details of the person sought: name, date of birth, nationality, passport or ID number, any distinguishing features etc. and, if available, a photograph of person sought.

The documents are then transmitted to the requested state, usually through Interpol; however, practitioners should check with the requested state to see if it has any additional or alternative requirements under its domestic law.

Once a person has been arrested under the provisional warrant, the requested state will notify the requesting state that the person has been arrested and of the time period in which the formal request should be submitted. The time period for such submission is governed by the relevant treaty[143] or domestic law.[144]

In the event that the request is not transmitted within the time period stipulated by the treaty or domestic law, the provisional arrest period comes to an end and the person is discharged. Some states may, if their domestic law permits, extend the time period for the submission of the documents.

The reason for discharging in the absence of the receipt of the request is quite straightforward – the person has been arrested at the behest of the requesting state, and this is based on an assurance from the requesting state that it will submit the necessary documents in support of the extradition. Therefore, in the absence of a request, the requested state does not have the power to continue to hold a person in detention, particularly as they are not subject to any criminal proceedings in the requested state apart from the extradition proceedings. This does not, however, prevent a subsequent arrest when the request is received, and if the person is still present in the requested state.

Those responsible for preparing the extradition request in the requesting state should:

- Check the date for submission of the request (if for any reason they have not been informed)
- Check if there are any certification/authentication requirements under the law of the requested state
- Check if the request needs to be translated; if so, this must accompany the request
- Check if there are any certification requirements for the translation, as some states will require a certificate from the translator confirming that he/she has translated the documents
- Make sure the request is transmitted through the appropriate channels (usually diplomatic) within the stipulated time period

20.5.2 'Full' request

A 'full' request is submitted where there is no risk that the person is likely to leave and there is no urgency. The requesting state will prepare the full extradition request (in line with the treaty requirements) and submit it to the requested state. The request is usually processed through diplomatic channels. The authorities in the requested state will then consider the request before arrest takes place.

20.6 Channels of communication and supporting documents

The channels for submitting an extradition request are usually diplomatic, unless agreed otherwise between states or regionally. The conventions and treaties will set

out the documents that need to be submitted in support of an extradition request. However, in line with international best practice, it is advisable to include the following documents:

Accusation cases must include:

- Warrant of arrest (check if the requested state requires any authentication if you are sending a copy of a warrant). A warrant of arrest is the warrant used in the requesting state. There is no such thing as an 'international warrant of arrest'. The warrant must set out all the offences for which extradition is sought. Practitioners will also need to make sure bail provisions are addressed; however, it is for the judge in the requested state to decide if the person is to be released on bail during the extradition proceedings in accordance with the laws of the requested state.
- The statement of facts in support of the request or evidence. Most international conventions and modern treaties urge states to 'expedite extradition procedures and to simplify evidentiary requirements', and this approach has been adopted by the SADC Protocol, the ECOWAS Convention on Extradition and the IGAD Convention on Extradition. However, the London Scheme for Extradition that applies within the Commonwealth states requires the requesting state to provide a prima facie case, unless otherwise agreed between the parties.
- Relevant law setting out the offence and the sentence threshold; where the offence has extraterritorial elements the statement of law must specify that the conduct can be tried in the requesting state and set out the relevant provisions. If reliance is being placed on case law, then that too should be explained.
- Particulars of identity of the person sought (usually a photograph and/or fingerprints).

Conviction cases should include:

- Certificate of conviction setting out the offences for which the person was convicted and the sentence imposed.
- A statement setting out the criminal conduct for which the person has been convicted. The statement must also confirm the time remaining to be

served (after parole etc., if applicable). Where a person has been convicted but not sentenced, the statement must confirm if the conviction is final and the maximum penalty available. If the person has been convicted in their absence, the requesting state must set out if there is the possibility of a re-trial or appeal.

- Relevant law.
- Particulars of the identity of the person sought (usually a photograph and/or fingerprints).

20.7 Summary of the extradition process

Step 1

The requesting state submits a request through one of the above routes: provisional arrest or full order request.

Step 2

- The requested state notifies the requesting state of the arrest and advises on the time period in which the request must be submitted.
- The requesting state submits the documents in support of its request (check with the requested state on any formalities for seal/certification that are required under its laws).
- If it is a 'full' request, the court will usually fix a date for the extradition hearing.

Step 3

- Once the formal request is received from the requesting state, the proceedings are governed by the law of the requested state.
- In some jurisdictions, particularly in common law states, the request is first considered by the executive prior to the judicial hearing. However, in most civil law jurisdictions the request is submitted directly to the judiciary for proceedings to commence. The extradition law of each state will determine this.

- For those states that engage both the executive and judicial process, it is important to determine what the initial executive stage involves. Is the executive simply confirming the receipt of the request or does it need to consider it further? Most states that involve the executive at this stage will require the minister to consider the request to determine if it should proceed to the next stage. After this, the judicial process starts.

Step 4

The matter is then usually heard at the first instance court to determine:

- Does the request relate to an extradition crime?
- Does the request relate to the person before the court (i.e. identity)?
- Does the request contain the correct documents required under the domestic law of the requested state?
- Do the documents meet the formal requirements, if any, under the domestic law of the requested state?
- Are there any bars to extradition (usually raised by the defence)?

Upon conclusion of the initial hearing, the person sought may be entitled to lodge an application for appeal or a writ of habeas corpus.

A practical note: extradition hearings will broadly fall into three phases:

Phase 1: The court, at the request of the prosecutor or relevant authority, will consider the formalities of the request before moving on to any defence submissions/challenges. The most important consideration is whether the alleged conduct amounts to an extradition crime; if it does not amount to an extradition crime, the request fails and the person will have to be discharged. The requirements for an extradition crime are discussed below. If the court is satisfied that the conduct amounts to an extradition crime and the request relates to the person before the court, the hearing will move into the second phase, the defence challenges.

Phase 2: The challenges that the defence can raise will be determined by both the domestic law and any grounds for refusal contained in the treaty or **convention.**

Phase 3: The appeal process.

Step 5

Once all the judicial proceedings are concluded, the matter may, if domestic law so requires, be referred once again to the executive to decide on the final surrender of the person to the requesting state.

20.8 What is an extraditable offence?

At the heart of an extradition proceeding is the notion of an extradition crime and the rule of double criminality. It has long been regarded as one of the key safeguards in extradition, in that, if conduct does not amount to an extradition crime, then no extradition can lie.

Given the critical importance of the rule of double criminality in such proceedings, it may help to look closely at what is involved when determining an 'extradition crime'.

What amounts to an extradition crime/offence varies between instruments, and practitioners must check this when submitting a request. Broadly speaking, requirements fall into two categories: the 'list' test and the 'conduct' test.

20.8.1 The 'list' test

In older treaties, particularly bilateral treaties, states would agree on a list of offences that would be considered as extradition crimes. This is commonly referred to as the 'list' test.

When a request was received the requested state considered the offence to determine if the criminality fell within the list of offences; if it did, the request would continue, otherwise it would fail. This worked well in the 18th and 19th centuries when the list of identified serious crimes was fairly short. However, as transnational crime increased and the international community (mostly through the UN bodies) sought to criminalise other conduct, the list had to be continually amended and updated. Such a process could be rather lengthy, in particular for dualist states.

To accommodate the change in trend, in terms of both criminal conduct and its impact, modern extradition treaties take a different approach, commonly referred to as the 'conduct' test.

20.8.2 The conduct test

This test avoids the complexities usually associated with trying to fit the conduct in a general list. The main criteria for an offence to amount to an extradition crime under this test are as follows:

- The conduct amounts to an offence in both the requesting and requested state
- The date of the offence: as the offence has to be a crime under the laws of both the requesting and requested state, difficulties may arise where the conduct is criminalised at a date later than when it occurred in the requesting state
- It is punishable under the laws of both states with a period of imprisonment of usually 12 months or more[145]

However, practitioners should also be aware that while the test is relatively straightforward and easily determined where the conduct falls entirely within the territory of the requesting state, complexities do arise in relation to transnational crime where the conduct occurs in more than one state; for example, drug trafficking and serious and organised crime will not be confined to one state. In such cases, practitioners will need to consider if there are there any extra-territorial elements to the conduct. The relevant authority in the requested state would then need to decide if the entire conduct (both in the requesting state and elsewhere) would amount to a crime under its domestic law.[146]

Thus, to amount to an 'extraditable offence', the conduct has to satisfy the following criteria:

- Double criminality
- Sentence
- Occurring within the 'jurisdiction' of the requesting state, which includes both territorial and extraterritorial offences

It does not mean, however, that if part of the conduct does not satisfy the double criminality rule, it should lead to a refusal of extradition on the entire conduct; the requested state can find that part of the conduct satisfies the test and return a person in respect of that. Such a finding would be binding on the requesting state under the speciality rule.

Equally, where an extradition request relates to a number of offences, some of which are extradition offences and some of which are not, the requested state can

reject those offences that are not extradition offences and return on the offences that satisfy the test.

20.9 Grounds for refusal

The decision on extradition always remains one for the requested state, as the person is found within its territory and it is for that state to determine if the person should be removed. However, given that the objective of extradition is to deny safe haven to those accused of crimes, states must try, as far as their domestic law and policy dictate, to permit extradition. The requested state can, and should, engage with the requesting state in making the decision so as to allow any further information to be made available to it.

This international push towards keeping the grounds of refusal to a minimum is echoed in most treaties; however, unlike MLA, which is concerned with the gathering of evidence, extradition proceedings has as its central focus the individual. It is therefore important to bear in mind that the grounds of refusal may be wider than those contained within MLA. Most treaties will contain mandatory and discretionary grounds for refusal.

In addition to the grounds for refusal contained in the treaty or convention, most domestic laws may well have their own grounds, which may replicate, add to or reduce those contained in the treaties. When submitting a request for extradition, practitioners should be aware of the possible challenges and grounds for refusal in the requested state.

20.10 Extradition of nationals/extradite or prosecute

Most civil law states assert criminal jurisdiction over their nationals for all offences, wherever those nationals may have committed the offence(s), i.e. the active personality principle. The corollary is that they will not extradite their own nationals. This is in direct contrast to common law practice where the assertion of active personality criminal jurisdiction must be specifically provided for by statute. In order to accommodate this difference between the legal systems, treaties usually preserve the right not to extradite nationals where such surrender is prohibited under a state party's constitution or domestic law.

As the definition of 'nationals' may vary among states parties, states should declare who falls within the category of 'national' under either the constitution or domestic law. Practitioners are advised to check with their counterparts in the requested state

should a case involving the national of the requested state arise and if it is known that they do not extradite their own nationals. In the event that a request is refused on the grounds of nationality, the requested state must submit the matter for consideration of prosecution to its authorities ('extradite or prosecute')

Therefore, where the requested state refuses to extradite its own nationals solely on the grounds of nationality, it must submit the case to its authorities to consider criminal proceedings in the requested state. The obligation is to consider prosecution in line with its domestic law.

20.11 Political offence exception

The political offence exception has received renewed attention in international instruments, particularly in the UN counter-terrorism conventions and protocols and regional treaties. In practice there have been cases, few and far between, where the requested state has refused to extradite the fugitive on the grounds of the political offence exception.

Despite its common usage both in extradition and refugee law, there is no definition or an agreed meaning of this phrase. Treaties, whether bilateral, regional or international, have all remained silent. It has been largely left to national courts to interpret the term, assisted to some extent by the general comments and interpretation guidance issued by human rights committees and commissions.

Historically the political offence exception has constituted grounds for refusal for extradition in many states. That exception was based on an understanding among states that they would not assist in punishing political activity directed against the government of another state, such as treason, sedition or attempts to force a ruling group to change or adopt certain policies, otherwise referred to as 'pure' offences. This approach is fairly straightforward and clear, but the difficulty arises in respect of 'relative' offences, that is, conduct that alleges criminality but is also linked with political activity. It is this latter range of offences with which national courts and international bodies have sought to grapple.

The starting point must, therefore, be a determination by the court as to whether the offence falls within the exception and, if so, whether it is a 'pure' or a 'relative' offence. Once that is determined, it becomes a matter for the court to decide if the particular facts lend themselves to the application of the exception.

20.12 Other considerations

20.12.1 Waiver

This provides for a person to waive the extradition proceedings, as long as the domestic law of the requested state allows this. It means that the person arrested can choose, if she wishes, to return to the requesting state without the requirement of a full extradition hearing. Under most domestic laws, a waiver is usually conducted before a judge or magistrate and requires the explicit consent of the person sought.

20.12.2 Rule of speciality

The rule of speciality acts as a safeguard to ensure that a fugitive is not tried or sentenced for an offence other than that upon which his return is based. It forbids the re-extradition or the handing over of a person by the requesting state once the person has been surrendered to it, unless the requested state is notified and consents to such a re-extradition. The purpose of the rule is to protect the individual from being subject to prosecution for offences that were not disclosed in the request, a disguised extradition or rendition to another state.

20.12.3 Handing over of property

When officers arrest a person on an extradition warrant, evidence relating to the offence may be found with him, or at his premises. As mutual legal assistance and extradition are different measures and a request for one cannot be used to secure the other, it is important that any evidence seized is retained and handed over to the requesting state if it so requests (under an MLA request).

20.12.4 Costs

The practice is that the costs in relation to the extradition process are usually borne by the requested state. The requesting state is responsible for preparing the request and any translations that may be required. The requesting state also bears the costs of any additional information that may arise and require action in the requesting state and all the transport costs (by any means) for conveying the individual at the end of the process in the requested state.

However, circumstances may arise whereby an extradition request raises complexities that involve additional or extraordinary expenses in the requested state. In such cases, states usually liaise on how the costs are to be met, and it may well mean that the requesting state agrees to bear the additional costs.

Chapter 21

Transfer of sentenced persons

21.1 Introduction

A measure of international co-operation that hitherto has been somewhat dormant and is now increasingly coming into focus is that which relates to the transfer of sentenced persons. The underlying rationale is to allow nationals of a foreign state who have been convicted and sentenced to a period of imprisonment the opportunity to serve the sentence in their home state.

With the increasing trend of transnational criminality, it is not unusual to find nationals of one state within the jurisdiction of another state, in furtherance of a crime. For example, a drug trafficker who is a national of state A agrees to act as a courier of a consignment and is arrested in state B, where he may be a total stranger. Following his trial, he is convicted and sentenced to a term of imprisonment. As a stranger in state B, he is unlikely to be visited by members of his family and will in all probability find himself in an unfamiliar culture and environment. It is this aspect of the process that states and the international community have sought to address through bilateral and multilateral arrangements. Such arrangements therefore also serve a humanitarian purpose.

21.2 The UN conventions

A number of the UN conventions have provisions inviting states to consider entering into bilateral or multilateral arrangements for the transfer of sentenced persons, and do not prescribe any detailed process.

Examples include:

- Article 6, paragraph 12 of the Vienna Convention
- Article 17 of UNTOC
- Article 45 of UNCAC

To assist states, UNODC has a Model Treaty on the Transfer of Sentenced Persons and also published the *Handbook on the international transfer of sentenced persons*.[147]

In addition to the UN conventions, there are a number of regional conventions addressing the transfer of prisoners, as well as bilateral arrangements between states.

21.3 Regional conventions

- The Council of Europe Convention on the Transfer of Sentenced Persons (1983) and its Additional Protocol sets out the procedures and factors that states need to take into account when embarking on such transfers (it provided a model for later conventions)
- The Scheme for the Transfer of Convicted Offenders within the Commonwealth
- Inter-American Convention on Serving Criminal Sentences Abroad (1996)
- European Union (EU) Framework Decision 2008/909/JHA
- Part VII of the Riyadh Arab Agreement for Judicial Co-operation (1983)

The main principles that can be distilled from the regional and bilateral arrangements are as follows:

21.3.1 Who can ask for transfer?

- The sentencing state (the state where the person is sentenced)
- The administering state (the state where the person will serve the sentence)
- The sentenced person

21.3.2 Conditions for transfer

A transfer can only be considered if all of the following conditions are met:

- The person is a national of the administering state or has close ties with it that the administering state recognises
- The judgement is final
- At the time of receipt of the request for transfer, the sentenced person still has at least six months of the sentence to serve or if the sentence is indeterminate

- The transfer is consented to by the sentenced person or by the sentenced person's legal representative (where in view of her age or her physical or mental condition, where one of the two states considers this necessary)
- The acts or omissions on account of which the sentence has been imposed constitute a criminal offence according to the law of the administering state or would constitute a criminal offence if committed on its territory
- The sentencing and administering states agree to the transfer

In addition, the sentenced person must:

- Be informed of his/her rights under the relevant convention/scheme
- Give his/her consent voluntarily (unless the sentence is accompanied by a deportation or expulsion order)
- Understand the legal consequences of transfer

21.3.3 Effect of the transfer

A number of consequences flow from a transfer:

- It suspends the enforcement of the sentence in the sentencing state
- If the administering state considers that the sentence has been served, the sentencing state cannot, even if it disagrees, enforce its sentence
- The administering state must decide how the sentence is to be given effect under its domestic law. This can be achieved in two possible ways:
  - Continue the enforcement of the sentence immediately or through a court or administrative order
  - Convert the sentence, through a judicial or administrative procedure, into a decision of that state, thereby substituting for the sanction imposed in the sentencing state a sanction prescribed by the law of the administering state for the same offence, subject to certain conditions

The conditions, in general terms, are that the administering state:

- Is bound by the findings as to the facts insofar as they appear explicitly or implicitly from the judgement imposed in the sentencing state
- May not convert a sanction involving the deprivation of liberty to a pecuniary sanction

- Shall deduct the full period of deprivation of liberty served by the sentenced person
- Shall not aggravate the penal position of the sentenced person, and shall not be bound by any minimum that the law of the administering state may provide for the offence or offences committed

21.3.4 Can the administering state alter the sentence?

The administering state is bound by the nature and length of the sentence; however, if that sentence is incompatible with its domestic law, the administering state can adapt the sentence that is available for the offence under its law provided it is of a similar nature; however, it cannot enhance the sentence.

It is important to bear in mind that this is not a review of the sentence, but steps to find equivalent measures; any decision as to an application for review remains with the sentencing state.

Conventions vary as to whether either or both states can grant any 'pardon, amnesty or commutation of the sentence in accordance with its Constitution or other laws'.[149] The Council of Europe Convention permits either state to grant a pardon, amnesty or commutation, whereas the Commonwealth Scheme confines it to the sentencing state, unless both states agree.

Chapter 22

Concurrent jurisdiction: principles and practical issues

The challenge of dealing with competing jurisdictions where more than one state is seeking or can claim jurisdiction to try a criminal case is not an easy one, as evidence may be scattered across a number of states; those suspected may be in one or more state (in the region or elsewhere); and each state will have its own criminal jurisdiction principles. How then should states resolve such issues?

There is no single internationally agreed set of criteria that can be called on to resolve these issues. Therefore, in the absence of such agreed criteria, it has been left to national courts[150] or regions to develop criteria that should be taken into account when addressing questions of jurisdiction. For example, after continued difficulties in terms of jurisdiction, Eurojust drew up guidelines[151] to assist law enforcement agencies (including prosecutors). More recently, the International Association of Prosecutors (IAP)[152] issued similar guidelines.

Given that the factors to be considered in any transnational investigation are likely to be similar, irrespective of geographic location, African countries may find it helpful to consider the practice that has developed in other regions or states with a view to either reaching a regional agreement or including those factors in their own domestic law or guidance. It may also help to provide prosecutors with guidelines, a practice adopted in a number of states (for example, the Crown Prosecution Service Guidelines for prosecutors in England & Wales).

States should try to make decisions at an early stage and may wish to ask when and how the issue of jurisdiction should be considered, as well as which authorities will be responsible for consultations and agreement. The issue of timing may also be relevant, as the question is raised whether the decision should be made at the beginning of investigation or after the nature of the case has been ascertained.

The types of questions that states should ask include:

- Where was the offence committed and where was the offender arrested?
- Where are the most witnesses or most important evidence or victims of the crime concerned located?
- Which jurisdiction has the best/most effective laws?
- Which jurisdiction has the best confiscation laws?
- In which jurisdiction will there be less delay?
- Which jurisdiction provides the best security and custody assurances?
- Which jurisdiction can best deal with sensitive disclosure issues?
- Which jurisdiction can bear the costs of the proceedings?
- In which jurisdiction did the crime have the most substantial effect?
- Where are most of any potentially recoverable assets located?
- Which state has the most developed asset-recovery mechanisms?
- Has the state concluded agreements or arrangements on transfer of criminal proceedings?
- Has the state developed policy and practical criteria for decisions on transferring or accepting criminal proceedings?
- Does that policy paper lay out the judicial, operational and sentencing implications of decision-making on these issues?
- Does the policy paper address the implications of decision-making in relation to the proceeds of crime?
- Has the state identified and mandated an authority to take lead responsibility for consultations and decision-making on related issues?

For ease of reference, the Eurojust Guidelines on Competing Jurisdiction are set out below. Prosecutors may also find it useful to familiarise themselves with the IAP Guidelines, any decisions made by a court in the African region on competing jurisdiction, and any policy guidelines that may be issued nationally or agreed region-wide.

Eurojust Guidelines

The guidelines address the issues arising from competing claims of jurisdiction in the following ways:

A presumption

There should, as a starting point, be a preliminary presumption that, if possible, prosecution should take place in the jurisdiction where the majority of the criminality occurred, or where the majority of the loss was sustained.

In order to reach a decision, prosecutors should balance carefully and fairly all the factors both for and against commencing a prosecution in each jurisdiction, where it is possible to do so.

There are a number of factors that should be considered and that can affect the final decision. All these factors should be considered at a meeting of prosecutors from the relevant states. Making a decision will depend on the circumstances of each case and the intention should be to bring consistency to every decision-making process.

Factors that should be considered:

- The location of the accused, i.e. the possibility of a prosecution in that jurisdiction and whether extradition proceedings or transfer of proceedings are possible
- Extradition and surrender of persons, i.e. the capacity of the competent authorities in one jurisdiction to extradite or surrender a defendant from another jurisdiction to face prosecution

Dividing the prosecution into cases in two or more jurisdictions

- The investigation and prosecution of complex cases of cross-border crime will often lead to the possibility of a number of prosecutions in different jurisdictions.
- In cases where the criminality occurred in several jurisdictions, provided it is practicable to do so, prosecutors should consider dealing with all the prosecutions in one jurisdiction. In such cases prosecutors should take into account the effect that prosecuting some defendants in one jurisdiction will

have on any prosecution in a second or third jurisdiction.

- Every effort should be made to guard against one prosecution undermining another.
- When several criminals are alleged to be involved in linked criminal conduct, if it is possible and efficient to do so, prosecutors should consider prosecuting all those involved together in one jurisdiction (this may not always be practical).

The attendance of witnesses

- Securing a just and fair conviction is a priority for every prosecutor. Prosecutors will have to consider the willingness of witnesses both to give evidence and, if necessary, to travel to another jurisdiction to give that evidence.
- In the absence of an international witness warrant, the possibility of the court receiving evidence in written form or by other means (such as remotely, by telephone or video-link) will have to be considered.
- The willingness of a witness to travel and give evidence in another jurisdiction should be considered carefully, as this factor is likely to influence the decision as to the jurisdiction where a prosecution is to be instituted.

The protection of witnesses

- Prosecutors should always seek to ensure that witnesses or those who are assisting the prosecution process are not endangered.
- When making a decision on the jurisdiction for prosecution, factors for consideration may include, for example, the possibility of one jurisdiction being able to offer a witness protection programme where another jurisdiction has no such possibility.

Delay

A maxim recognised in all jurisdictions is that 'justice delayed is justice denied'. While time should not be the primary factor in deciding which jurisdiction should prosecute, if other factors are balanced prosecutors should consider the length of time that proceedings will take to be concluded in a particular jurisdiction.

If several states have jurisdiction to prosecute, consideration should always be given to how long it will take for the proceedings to be concluded.

Interests of victims

Prosecutors must take into account the interests of victims and whether they would be prejudiced if any prosecution were to take place in one jurisdiction rather than another. Such consideration would include the possibility of victims claiming compensation.

Evidential problems

- Prosecutors can only pursue cases using reliable, credible and admissible evidence. Evidence is collected in different ways and often in very different forms in different jurisdictions. Courts in different jurisdictions have different rules for the acceptance of evidence, often gathered in very diverse formats.
- The availability of evidence in the proper form and its admissibility and acceptance by the court must be considered, as this will affect the decision on where a prosecution might be brought.

Legal requirements

- Prosecutors must not decide to prosecute in one jurisdiction rather than another simply to avoid complying with the legal obligations that apply in one jurisdiction but not in another.
- All the possible effects of a decision to prosecute in one jurisdiction rather than in another and the potential outcome of each case should be considered. These matters include the liability of potential defendants and the availability of appropriate offences and penalties.

Sentencing powers

- The relative sentencing powers of courts in the different potential prosecution jurisdictions must not be a primary factor in deciding in which jurisdiction a case should be prosecuted.
- Prosecutors should not seek to prosecute cases in a jurisdiction where the penalties are highest.

- Prosecutors should ensure that the potential penalties available reflect the seriousness of the criminal conduct that is subject to prosecution.

Proceeds of crime

- Prosecutors should not decide to prosecute in one jurisdiction rather than another only because it will result in more effective recovery of the proceeds of crime.
- Prosecutors should always give consideration to the powers available to restrain, recover, seize and confiscate the proceeds of crime and make the most effective use of international co-operation agreements in such matters.

Resources and costs of prosecuting

- The cost of prosecuting a case, or its impact on the resources of a prosecution office, should only be a factor in deciding whether a case should be prosecuted in one jurisdiction rather than in another when all other factors are equally balanced.
- Competent authorities should not refuse to accept a case for prosecution in their jurisdiction because the case does not interest them or is not a priority to the senior prosecutors or their ministry of justice.

Matrix

The factors that should be considered in making decisions on which jurisdiction should prosecute are set out in this manual. The priority and weighting that should be given to each factor will be different in each case.

Chapter 23

Practical explanation on international co-operation

23.1 Introduction

The world is becoming smaller, especially within Africa. International co-operation is needed to deal with terrorism, organised crime and other human rights abuses. The vehicle or engine room to assist states in dealing with these problems is state-to-state co-operation, in particular through requests for MLA and extraditions. Many countries in Africa have agreements or treaties with each other. Such co-operation is supplemented by regional and UN co-operation.

A good example of regional co-operation within Africa is the SADC Protocol on Extradition and Mutual Legal Assistance.[153] UN treaties are also available to assist with inter-state co-operation – e.g. UNTOC.[154] Even where there is no treaty or agreement between individual states the internationally recognised principle of comity is available as a legal basis to assist states to co-operate with each other.

The purpose of this section is not to provide an exhaustive review of all the available and applicable treaties or agreements – some of these are dealt with extensively in other parts herein. Each state needs to identify, at the time of forwarding or receiving a request for MLA or extradition, the applicable treaties/agreements relevant at the time of the request to ensure that the correct legal requirements are met. This part of the manual will briefly deal with some practical aspects regarding the procedure to be followed in requests for MLA and extradition, taking into account the diversity of legal systems and other procedural requirements within each state. It should be treated as a guideline only, without trying to prescribe to states how they should deal internally with requests for MLA and extradition.

23.2 Request for mutual legal assistance

23.2.1 Outgoing formal requests to states

States have internal procedures as to the structure and format of requests to other states. It is recommended that at least the following aspects should be dealt with in preparing requests for MLA:

- The legal basis: does your country have a treaty or agreement with the other country – if so state it clearly and if not, argue that the principle of comity/ reciprocity is applicable.
- Provide a short introduction as to what the request is all about. Indicate whether or not any person has been arrested and the urgency of the matter.
- Introduce the person signing the application: set out the position held by the person, his/her qualifications and experience and that he/she is qualified to prepare and sign the application.
- Provide background facts: say what this is all about and set out a summary of the relevant facts.
- Identify the main purpose of the request: set out why you are forwarding the request and briefly set out what you want the other state to do for you.
- Clearly specify the assistance needed: set out specifically want you want. Remember the person at the other side is not involved at all in the investigation and you must make it as clear as possible what you want, providing as much information as possible to identify, e.g. the bank account, document, witness, etc.
- The law: set out the elements of the crime you are investigating and the range of sentences to be imposed. This also needs to be done to show the other state that it may have similar offences. It will make it easier for the other state to recognise that it has similar offences to the ones under investigation in your state.
- The format of the evidence to be presented: states have different ways in preparing witness statements. If your state has a specific way, request the other state to prepare the statement in the format it will be admissible in your state – you may even attach a draft of such a statement to be completed.

- Reciprocity: indicate that your state will also assist with similar requests in future from the state you are dealing with.
- Reservation of rights: build in the application the right to amend and supplement the application later.
- Undertaking: provide an undertaking that the evidence will only be used for the case/investigation with which you are requiring assistance. Make it clear that you will not share the evidence provided to you with other parties etc. without prior authorisation from that state. In doing so you signal to the other state that it can trust you with evidence provided to your state, either public or confidential.
- Assurances: provide assurances that the investigation is not of a political nature or on account of a person's race, religion, nationality or political opinion.
- Contact numbers: provide contact numbers for the lawyer and investigating officer working on the case.
- Translation: it is essential to establish the working language of the country involved as it may need you to translate the original. It is essential to provide the original plus the translated version.

23.2.2 Incoming formal requests from states

If a request is received by a state for assistance, the following can be considered:

- Respect the legal system and procedure requirements of the requesting state, especially if it is different to what you are familiar with in your state.
- Ensure that the request for assistance has been approved by your central authority or other relevant body within your state before you proceed.
- It may be necessary to subpoena a person to provide information to the requesting state.
- Provide the requested information through the procedure/channel approved by your state.

- If a request for search and seizure is received, make sure that it is prepared in accordance with the relevant law of your state. It may also be necessary to identify the names of the persons from the requesting state in the application for the search warrant that will accompany members of your police force during the operation. It is always very helpful for those persons to join your police members, as it is sometimes essential to consult with them when decisions are to be taken before seizing material/evidence. It is, however, also imperative that it is made clear that the local police members will be in charge of the search and seizure operations.
- Keep a record of information/evidence provided to the requesting state. In some states it is required that the evidence requested be placed before a magistrate or other official. It will then be forwarded through diplomatic channels to the requesting state. It can do no harm, in appropriate cases, to provide the state with informal copies of the documentation/evidence, but it is essential to ensure that the formal documentation/evidence be forwarded through official/diplomatic channels.

23.2.3 Informal requests for MLA – police to police, state to state and through Interpol

It is essential that we also allow for informal co-operation between states, but be aware of the following:

- Do not allow any state to abuse the legal processes within your state by e.g. obtaining evidence without going through approved and appropriate channels.
- There can be no problem with providing lead and other information about a person's whereabouts, etc. However, once your state is requested to forward witness statements, bank documents, etc., these must be prepared and forwarded in terms of the applicable rules relating to requests for MLA in your respective state. Be careful not to provide evidence to another country without a proper paper/legal trail.
- States will sometimes provide you with statements or documents on an informal basis due to urgency, but it is a good practice to later forward a

formal request for MLA to that state indicating what has happened on an informal basis (have a look again at the manual where the Henry Okah case is discussed – it provides an excellent example of how states can work together through requests for MLA, both informally and formally).

23.3 Extradition

23.3.1 Request for provisional arrest by your state

A fugitive may reside in another state or be in the process of leaving that state. A request for provisional arrest can be prepared and is normally forwarded through Interpol channels. Each state has its own requirements as to format, but the following can be taken into account in preparing such applications:

- Introduce the person signing the application: set out to the other state the position held by the person, his/her qualifications and experience and that he/she is qualified to prepare and sign the application.
- Provide the legal basis for the request: identify the relevant treaty etc. between the two states or make use of the principle of comity.
- Provide background facts as to the whereabouts of the fugitive: make it easy for the other state to locate the person by providing sufficient information.
- Provide a short description of the available evidence against the fugitive.
- Briefly identify the offence(s) the fugitive will be prosecuted for and whether or not prescription is applicable.
- Inform the other state that this request will be followed up with a substantial request for extradition in accordance with the time periods set out by the applicable treaty/agreement.
- Provide the state with an original arrest warrant.

23.3.2 Request for provisional arrest to your state

As indicated, each state has its own procedures, but also keep in mind the remarks made earlier. In addition, the following can be taken into account:

- If you are approached to assist with the arrest of a fugitive through Interpol or on a red notice, ensure that the requesting state will provide you with sufficient documentation to make a provisional arrest. The documentation must also include a guarantee that a formal application for extradition will follow within the prescribed time periods set by the relevant treaty you are operating upon.
- It may also be prudent, in appropriate cases, to ensure that the guarantees set out above are provided to your state before you embark on arresting the fugitive.

23.3.3 Formal request for extradition by your state

Each state has its own procedures and format in the preparation of requests for extradition, and it is necessary to respect that. However, the following aspects can be taken into account as guidelines on what should be in the extradition application:

- Provide a short introduction as to what the request is all about and indicate the legal basis of the request. Also indicate whether any person has been arrested provisionally.
- The legal basis: does your state have a treaty/agreement with the other state – if so state it clearly and if not, argue the principle of comity/reciprocity.
- Introduce the person signing the application: set out to the other state the position held by the person, his/her qualifications and experience and that he/she is qualified to prepare and sign the application.
- Provide a summary of the available evidence and attach relevant witness statements.
- Provide identification information about the fugitive, if not arrested already provisionally.
- The law: set out the elements of the crime(s) the fugitive will be prosecuted for and the range of sentences to be imposed if convicted. Many countries will not allow you to add any subsequent counts if they are not clearly set out in the initial application. Some treaties also set out minimum sentences to be imposed on the fugitive before extradition can be considered.

- Double criminality: it is important to consider this, especially as the conduct must amount to a crime in both the requesting and requested state. The crimes need not be called the same but should have similar elements.
- The strength of the case: some states prefer that there is a further statement from the person signing the document that there is sufficient evidence or a prima facie case linking the fugitive with the crimes alleged. In certain cases it may also be advisable to include a draft charge sheet.
- Limitation: indicate that the intended prosecution is not barred by prescription.
- Warrant of arrest: attach the warrant to the application, if not already done, as part of the provisional arrest application.
- Contact numbers: provide contact numbers for the lawyer and investigating officer working on the case.
- Translation: it is essential to establish the working language of the state involved, and to provide the original plus the translated version.
- Other guarantees: some states may also request additional guarantees before they will extradite, e.g. at which prison facility will the fugitive be kept pending trial and if convicted, be serving his/her sentence.

23.3.4 Formal request for extradition received by your state

The requesting state's application may differ from the format you use in your state, although it must adhere to the key aspects of any relevant treaties, etc. The following can also be taken into account:

- Has the request for extradition and arrest been cleared by the central authority or other institution within your state?
- If so, does it appear from the application that there is sufficient evidence or a prima facie case against the fugitive?
- Double criminality – is the crime on which extradition is requested also a crime in your state? The crimes need not be called the same but should have similar elements.
- Has the fugitive applied for political asylum in your state (this may delay the commencement of the extradition proceedings)?

Part 4

Criminal justice responses to terrorism and the role of the prosecutor

Adv. Shaun K Abrahams
National Prosecuting Authority of the Republic of South Africa

Index

Aim and objective

A state's response to terrorism and/or transnational terrorism is largely defined by its domestic legislation, its domestication of international agreements, treaties, conventions and protocols, and the strength and experience of its domestic law enforcement authorities and various governmental agencies in co-operating with each other in the gathering of admissible, reliable and relevant evidence and in the arrest and prosecution of persons alleged to have committed acts of terror, in whatever form. The significance of witness protection schemes and mechanisms can also not be overstated. The role of the prosecutor is central in demonstrating a state's response to combating terrorism and/or transnational crime, particularly in:

- Collaborating with various stakeholders
- Giving guidance in collecting relevant and admissible evidence
- Protecting the integrity of reliable and admissible evidence
- Safeguarding witnesses
- Decision-making
- Upholding the independence of prosecuting authorities and the integrity of the administration of justice
- Ultimately representing the state in the prosecution of offenders, without fear, favour or prejudice
- Upholding fundamental human rights and constitutional values in so far as these relate to the fair trial rights of an accused

The aim of Part 4 is to demonstrate, largely through practical case studies, how law enforcement authorities and other governmental stakeholders co-operated in the investigation and prosecution of terror-related cases, and to emphasise the role of the prosecutor therein.

The object is for prosecutors:

- To understand what the role and responsibilities of a prosecutor are in the investigation and subsequent prosecution of terrorism matters
- To understand the close co-operation required between various government departments
- To understand the roles and responsibilities of investigative authorities, intelligence authorities and other government stakeholders
- To understand the role of prosecutors as per the UN guidelines on the role of prosecutors
- To understand the role of a prosecutor in safeguarding the rule of law and upholding fundamental human rights in due process

Chapter 1

Introduction

Africa has suffered tremendously over many years as a direct result of the scourge of terrorism. The proliferation of terrorist attacks during the late 1990s and early 2000s, including the terror attacks on the US embassies in Nairobi, Kenya and Dar es Salaam in 1998 and the terror attacks of 11 September 2001 in the US, has left no region immune. In East Africa, the Somalia-based terrorist group Al-Shabaab was the primary terrorist threat. Among the most notable attacks by Al-Shabaab was that on the Westgate Mall, Nairobi on 21 September 2013, which left 65 people dead. In West Africa, the attacks by Boko Haram have resulted in over 1 000 casualties. The kidnapping of hostages for ransom has also increased significantly. These very real threats, to mention but a few, still exist. The continued terror attacks by Al-Shabaab in Kenya; the persistent onslaught on the people of Nigeria by Boko Haram, particularly in northern Nigeria but also spreading across the rest of that country; and the attacks by al-Qaeda in the Islamic Maghreb (AQIM) during the first half of 2014 are only a few examples of the continued threat terrorism poses to peace and security on the African continent.

The objectives of establishing the OAU in 1963 were largely to:

- Promote unity and solidarity among states on the African continent
- Safeguard the sovereignty and territorial integrity of states parties
- Promote international co-operation within the framework of UN conventions, protocols and treaties
- Co-ordinate and intensify co-operation and development among states parties
- Rid the African continent of the remnants of colonialism and apartheid

These objectives have since evolved and were, together with further objectives, incorporated into those of the AU. Never has there been a greater responsibility and

obligation on AU states parties to form a united and solidified front than the present in the fight to combat terrorism, organised crime, international crime, corruption and money-laundering. Emerging trends, coupled with the upsurge in the commission of these offences, domestically and transnationally, call upon states parties to be proactive.

The UN Global Counterterrorism Strategy[155] created a new framework for international counterterrorism actions by states, inter alia calling on states parties to collectively approach the challenges of international terrorism by endorsing the security-related counter-terrorism measures of the UN Security Council; prioritising a commitment to address underlying conditions conducive to the emergence and spread of terrorism; highlighting the importance of development as an important element of global counterterrorism efforts; and ensuring that counter-terrorism measures respect human rights and the rule of law.

The AU's counter-terrorism framework, which consists primarily of the AU Convention and the Plan of Action, is indicative of member states' political will to strengthen the continent's initiatives to combat terrorism and implement counter-terrorism measures within peace and security frameworks.

Intrinsic to a state's response to serious national and transnational crime is a strong criminal justice system with a proactive and independent prosecution service. Bringing terrorists to justice, however, poses major challenges as a result of the complexity of investigating, prosecuting and adjudicating on these cases. Terrorism evolves continuously, forcing law enforcement authorities to develop new and more effective responses.

The prosecution of terrorism is a key component of a state's approach to its effective prevention and suppression. At the same time, gathering intelligence, investigating this intelligence and collecting admissible and reliable evidence are paramount to the successful prosecution of acts of terrorism and related offences.

Countering terrorism ultimately depends on the ability of law enforcement authorities to co-operate domestically and transnationally, to detect crime and its emerging trends at an early stage, and to work in close proximity and within a framework of respect for human rights and the rule of law in bringing terrorists to justice.

Effective counter-terrorism investigations and successful prosecutions can only be conducted within in a rule of law framework and by ensuring compliance with

international and regional counterterrorism instruments, upholding human rights standards and adhering to UN Security Council resolutions.

This section endeavours to place states' responses to terrorism within a human rights and rule of law framework through case studies demonstrating the listed aims and objectives. Prosecutors can benefit not only from the lessons from success but also from failure.

Chapter 2

The role of prosecutors

Prosecutors play a crucial role in the administration of justice.[156] They are the cardinal gatekeepers of the criminal justice system, and their responsibilities include the following:

- Instituting prosecutions (who, when, on what charges)[157]
- Managing investigations (providing technical and legal guidance to investigating agencies)[158]
- Performing their duties fairly, consistently, expeditiously and with respect for the protection of human dignity and the upholding of human rights, thereby ensuring due process in the administration of justice[159]
- Executing their responsibilities impartially, avoiding political, social, religious, racial, cultural, sexual or any other kind of discrimination[160]
- Protecting the public interest by being objective and paying due regard to all information, favourable or unfavourable to their case and/or to the advantage or disadvantage of an accused[161]
- Keeping matters confidential, considering victims' concerns and advising them of their rights in accordance with the Declaration of Basic Principles of Justice for Victims and Abuse of Power[162]
- Paying due regard to the investigation and prosecution of, inter alia, grave violations of human rights and crimes recognised by international law, as criminalised domestically[163]
- Refusing to make use of evidence obtained through unlawful means and which constitutes the violation of a suspect's fundamental human rights, and bringing the perpetrators of such abuse to justice[164]

Prosecutors are further required to co-operate with other stakeholders in the criminal justice system, such as the police, courts, legal profession, government departments and institutions.[165]

Prosecutors are first and foremost officers of the court, who are expected to exercise their duties without fear, favour or prejudice as administrators of justice in maintaining and/or restoring public confidence in the administration of justice.

The exercise of prosecutorial discretion has an impact on the criminal justice system in terms of its efficiency and is capable of destroying people's lives, careers and reputations.[166] Hence, such discretion must be exercised responsibly with due cognisance of the rule of law, constitutional values and the integrity and responsibility of the office held. Prosecutors are ultimately duty bound to assist the court in seeking the truth.[167]

In *S v Yengeni*,[168] a South African high court, in reference to the oath, affirmation and impartiality and esteem of the office of the prosecutor, held as follows:

> '[51] Every member of the authority is obliged to undertake an oath or affirmation prior to the commencement of their service to uphold this provision. The Constitution guarantees the professional independence of the National Director of Public Prosecutions and every professional member of his staff, with the obvious aim of ensuring their freedom from any interference in their functions by the powerful, the well-connected, the rich and the peddlers of political influence.
>
> [52] The untrammelled exercise of their powers in a spirit of professional independence is vital to the functioning of the legal system. The independence of the Judiciary is directly related to, and depends upon, the independence of the legal professions and of the National Director of Public Prosecutions. Undermining this freedom from outside influence would lead to the entire legal process, including the functioning of the Judiciary, being held hostage to those interests that might be threatened by a fearless, committed and independent search for the truth.
>
> [53] Section 22(4)(f) of the Act obliges the National Director of Public Prosecutions to bring the provisions of the United Nations guidelines on the Role of Prosecutors to the attention of every prosecutor and director of the authority and to promote respect for and compliance with its principles.'

In *Zhang v Canada (Attorney-General)*,[169] and in reference to *Kostuch v Alberta*,[170] the court held that the exercise of prosecutorial discretion is reviewable when flagrant impropriety can be demonstrated. In this regard the court relied on the following extract:

> '… flagrant impropriety can only be established by proof of misconduct bordering on corruption or violation of the law, bias against or for a particular individual or offence.'

In *National Director of Public Prosecutions v Freedom Under Law*,[171] it was held that the review of a prosecutorial decision is permissible on the principle of legality.

> '[28] The legality principle has by now become well-established in our law as an alternative pathway to judicial review ... Its underlying constitutional foundation appears, for example, from the following dictum by Ngcobo J in Affordable Medicines *Trust & Others v Minister of Health & Others* 2006 (3) SA 247 (CC) para 49:
>
> "The exercise of public power must therefore comply with the Constitution, which is the supreme law, and the doctrine of legality, which is part of that law. The doctrine of legality, which is an incident of the rule of law, is one of the constitutional controls through which the exercise of public power is regulated by the Constitution."'
>
> '[29] Legality is an evolving concept in … jurisprudence, whose full creative potential will be developed in a context-driven and incremental manner … But for present purposes it can be accepted with confidence that it includes review on grounds of irrationality and on the basis that the decision-maker did not act in accordance with the empowering statute (see *Democratic Alliance & others v Acting National Director of Public Prosecutions & others 2012* (3) SA 486 (SCA) paras 28-30).'

In *Hurd v People*,[172] the Court of Michigan held:

> 'The prosecuting officer represents the public interest, which can never be promoted by the conviction of the innocent. His object like that of the court should be simply justice; and he has no right to sacrifice this to any pride of

> professional success. And however strong may be his belief of the prisoner's guilt, he must remember that, though unfair means may happen to result in doing justice to the prisoner in the particular case, yet, justice so attained, is unjust and dangerous to the whole community.'

Prosecutors must refrain from falling in the trap as explained by John F Terzano et al[173] when dealing with sensitive investigations and prosecutions of, for example, terrorism and transnational organised crime, namely:

> 'When prosecutors form a theory of guilt for a defendant, confirmation bias and belief perseverance can threaten their ability to adjust their thinking, even when confronted with evidence strongly challenging the accuracy of their theory. Psychological biases can lead prosecutors to favour evidence that confirms their theory, while ignoring or discrediting contradictory information. This phenomenon often leads to a "tunnel vision" mentality, where prosecutors and law enforcement focus all of their attention and efforts on building a case against a single suspect, often overlooking weaknesses in their case or leads pointing to other suspects. Tunnel vision is particularly dangerous when the prosecution's theory is wrong, and the defendant is in fact innocent.'

In addition, prosecutors' independence must be understood in such a way that:[174]

> '[P]olitical, personal, and private considerations must be set aside so far as the exercise of discretionary power is inherent in the office of the prosecutor. No matter how much pressure is put on him due to the heinous nature of an offence, the surrounding publicity, or the parties involved, the prosecutor must retain an inward sense of impartiality and display outward objectivity.'

It is against this backdrop that prosecutors' roles have changed over the years. Prosecutors can only exercise their duties in the confines of what domestic law and applicable international law permit, along with the state's constitutional values. Prosecutors are duty bound to ensure that justice is seen to be done. In this regard, their role in the guidance and management of investigations obliges them to leave no stone unturned in the search for truth and justice. With the advent of globalisation and the increase in, for example, terrorism, transnational organised crime and cybercrime, prosecutors as the ultimate decision makers and

the presenters of relevant, reliable and admissible evidence, play a leading role in directing, gathering and/or obtaining evidence. This includes:

- Authorising intrusively obtained evidence, such as detailed and itemised telephone billings, bank records, email communications, Internet usage, live communication interception monitoring, search warrants, subpoenas, etc.
- Submitting letters of request for MLA to foreign states
- Extraditing alleged offenders
- Authorising arrest warrants
- Authorising undercover operations
- Engaging with key governmental stakeholders, domestically and internationally
- Guiding the gathering of intelligence into admissible evidential material
- Interviewing key witnesses to secure their assistance and co-operation
- Safeguarding witnesses

In *Boucher v The Queen*[175] the following was said in reference to the purpose of a criminal prosecution and the role of a prosecutor:

> 'It cannot be over-emphasized that the purpose of a criminal prosecution is not to obtain a conviction; it is to lay before a jury what the Crown considers to be credible evidence relevant to what is alleged to be a crime. Counsel have a duty to see that all available legal proof of the facts is presented: It should be done firmly and pressed to its legitimate strength but it must also be done fairly. The role of a prosecutor excludes any notion of winning or losing; his function is a matter of public duty than which in civil life there can be none charged with greater personal responsibility. It is to be efficiently performed with an ingrained sense of dignity, the seriousness and the justness of judicial proceedings.'

In *S v Shaik and Others*,[176] in reference to prosecutor-guided investigations, it was stated that:

> 'The purpose of an investigator is to hand over as much evidence to the prosecutor as can be lawfully obtained. It is in the best interest of all, even that of the accused, for the prosecutor to have as much evidence available as possible in her or his position as the truth-seeker.'

To this end, all responsibilities of prosecutors must be exercised with due regard to the rule of law and fair trial rights of an accused.

A truly African case study that epitomises co-operation among African states and various law enforcement authorities and government departments, as well as the role of the prosecutor, is that of *S v Henry Okah*.[177] Due to the significance of this trial, which has been described as a victory for Africa in the fight against terror,[178] it is discussed comprehensively below in so far as it is relevant to the domestication of international instruments.

Chapter 3

S v H Okah – a truly African case study

What does a prosecutor do when an international terrorist is in his/her territorial state? This is the question prosecutors in the Priority Crimes Litigation Unit (PCLU) in the Office of the National Director of Public Prosecutions (NDPP), South Africa asked on the morning of 1 October 2010 in Pretoria.

3.1 Brief historical overview

Henry Emomotimi Okah, a 46-year-old Nigerian national, was convicted on 13 terrorism-related charges by the South Gauteng High Court, Johannesburg on 21 January 2013, with him being in contravention of the Protection of Constitutional Democracy against Terrorist and Related Activities Act 2004 (Act 33 of 2004, or the POCDATARA). Okah, the leader of MEND, a rebel militant organisation in the oil-rich Niger Delta region, was later sentenced to serve an effective period of 24 years' imprisonment in a South African correctional services facility. This trial demonstrated Africa's ability to speedily administer justice in transnational crimes through co-operation.

MEND had been in continuous conflict with the Nigerian government since 2005, and publicly took responsibility for targeted attacks on oil and petroleum pipelines and the kidnapping of petroleum company employees, in the form of emails and press releases to the media that coincided with the attacks. The accused, who had made South Africa his home, was first arrested in Angola in 2007 and later repatriated to Nigeria in February 2008, where he was indicted on 62 counts, including charges of high treason, terrorism, illegal possession of firearms and arms trafficking. He faced the death penalty were he to be convicted before a Nigerian federal court.

The Nigerian government initiated an amnesty programme in 2009, which included rebel and militant disarmament by MEND and all other rebel factions associated with

it, in a bid to end attacks on the oil industry. In July 2009, the accused accepted the offer of amnesty extended to him by the Nigerian government and offered to work with the latter towards the restoration of peace in the Niger Delta region. He was released by the Nigerian authorities on 13 July 2009 and returned to South Africa on 22 August 2009.

Most militants in the Niger Delta region laid down their arms after having accepted amnesty. From that moment, MEND in essence ceased to exist. There was no longer a need for those who had accepted amnesty to rebel against the Nigerian government. Subsequently, and as a result of government initiatives and undertakings, oil production rose from 700 000 barrels a day (at the height of the crisis in the Niger Delta) to 2,6 million barrels a day. More than 20 000 former militants received training in various parts of the world, including South Africa, in the oil, gas, construction, maritime, piloting and other industries.

Bombings at Government House Annex, Warri, 15 March 2010

Okah was dissatisfied with what he believed to be the Nigerian government's unequal and discriminatory sharing of oil revenues, which, in his view, had adversely affected the Niger Delta region, and with the government's failure to restore the land of the Niger Delta to its people (who believed it had been unlawfully taken from them). On 15 March 2010, members of MEND, acting at the behest of the accused, detonated two vehicle-born improvised explosive devices (VBIEDs) in the vicinity of the Government House Annex, Warri, Nigeria. This was where a post-amnesty dialogue was scheduled to take place, facilitated by the publisher of the Vanguard Newspaper, a Nigerian publication. Some of the dignitaries scheduled to participate in the dialogue included the Minister of the Niger Delta, and the governors of Delta, Edo and Imo states. One person died and 11 sustained injuries as a result of the explosion. The accused had orchestrated these attacks by, among others, financing the purchase of the two vehicles used in the attacks, arranging for a Nigerian welder to install hidden compartments in these vehicles, arranging for the supply of the dynamite, detonators and timers used in the construction of the VBIEDs and giving guidance and direction in the manufacture, strategic placement and detonation thereof, with the assistance of Nigerian nationals.

Bombings at Eagle Square, Abuja, Nigeria, 1 October 2010

On 1 October 2010, two VBIEDs were detonated on the main road near Eagle Square, Abuja, on the day of Nigeria's 50th Independence Day celebrations. The President of Nigeria and the other dignitaries were about 300 m away from where the devices were detonated. Eight people died and 53 suffered severe injuries. Hours prior to the attack, MEND released warnings of its intended detonation of explosives via an email to the media. On 2 October 2010, MEND, via another email to the media, accepted responsibility for the Abuja bombings and blamed the irresponsibility of the Nigerian Governments Security Forces for the loss of lives. The accused was the mastermind behind the bombings in that he had, among others, financed the purchasing of the two vehicles used in the explosions, directed the supply of the dynamite, detonators and timers used in the construction of the bombs, and directed the location, strategic placement and detonation of the VBIEDs. The persons who manufactured the VBIEDs had acted at the behest and direction and in concert with the accused. Between January and September 2010 the accused was also responsible for setting up militant camps and supplying weapons (i.e. arms, ammunition and explosives) and military clothing and accessories to militants who returned to the creeks of the Niger Delta region after having embraced amnesty. Four Nigerian nationals, including Okah's brother Charles, were arrested and indicted in the Federal High Court of Nigeria, Abuja for their respective roles in the Warri and Abuja bombings.

Threats directed at the South African Government, 27–30 January 2012

On 27 January 2012, the European representative of MEND forwarded a communiqué to various persons and entities, including the South Africa–Nigeria Chamber of Commerce, in which MEND threatened the South African Government. If the government failed to facilitate the release of the accused from lawful detention, MEND threatened to disrupt the business activities of South African entities in Nigeria and to take South African nationals employed by these entities hostage. On 30 January 2012, the accused made the same threats to the investigating officer while incarcerated.

3.2 Information-sharing and investigations

In the days leading up to Nigeria's 50th Independence Day celebrations, the Nigerian Department of State Security received credible information of the accused's plans to detonate VBIEDs at Eagle Square, Abuja to mar the event. This information was shared with the South African law enforcement authorities late in the evening of 29 September 2010.

During the early morning of 30 September 2010, a multi-disciplinary team comprising law enforcement and intelligence authorities conducted a search and seizure operation at the accused's home in the south of Johannesburg without a warrant. However, they had insufficient evidence linking the accused to the plans of 1 October 2010 and did not find anything at his home that implicated him in these offences. Due to the lack of evidence linking the accused to any offence he was released. The National Prosecuting Authority (NPA) was unaware of these developments at the time.On the morning of 1 October 2010, PCLU prosecutors were briefed by the various investigative and intelligence authorities for the first time about the accused and the plans to detonate VBIEDs at Eagle Square, Abuja that same day. At the conclusion of the briefing there was still no evidence implicating the accused.

At the time, both the South African and Nigerian law enforcement and intelligence authorities were unaware of the accused's involvement in the earlier Warri bombings.

The lead prosecutor recalls hearing, while driving to his chambers from the briefing, a breaking news report over the radio of the detonation of the first VBIED and, about 10–15 minutes later, of the detonation of the second VBIED. At that stage there was still no evidence linking the accused to the Abuja bombings.

Later that evening, an affidavit under oath was received from the Nigerian authorities implicating the accused as the mastermind of the Abuja bombings. The investigating officer obtained both a warrant of arrest and a search warrant on the strength thereof early on 2 October 2010. Intelligence authorities were monitoring the accused's movements in the event he attempted to flee the country in order to evade justice.

Both warrants were duly executed later that morning. The accused was, inter alia, informed of his rights to legal representation, the purpose of his arrest and the charges against him, which at the time were a main count of engaging in a

terrorist activity and an alternative charge, namely the delivery, discharging and/or detonation of an explosive device that caused death and serious bodily injuries and extensive damage to property.[179] This was criminalised domestically under both the UN International Convention for the Suppression of Terrorist Bombings and the OAU Convention for the Prevention and Combating of Terrorism.

The accused's legal representative was present during the search and seizure operation. The accused was at the conclusion thereof detained at a high-risk detention centre and first appeared in court on 4 October 2010, after which the matter was adjourned for a formal bail application to 14 October 2010. A number of persons, including his brother Charles, were arrested in a corresponding investigation in Nigeria[180] by that country's authorities.

At the commencement of the accused's bail application he argued that his matter had been erroneously enrolled, as the NDPP's authorisation of his prosecution had not been obtained.[181] The NDPP's certificate is only required prior to the commencement of a trial, when the investigation has been concluded and the accused is required to enter a plea. The bail court had not been faced with this dilemma previously as this was the first prosecution in contravention of POCDATARA and subsequently disagreed with the prosecutor, threatening to remove the matter from the court roll if the authorisation was not obtained within an hour. The NDPP's authorisation was timeously obtained and a somewhat protracted bail application proceeded. The court later refused to admit the accused to bail. The accused's appeal against this ruling was unsuccessful.

The Supreme Court of Appeal, in *Bogaards v The State*,[182] later supported the correctness of the prosecutor's submission in the *Okah matter*, ruling that the NDPP's certificate was only required once the investigation had been concluded, as 'a charge of this nature is taken by the highest official after properly considering all the relevant facts and implications of such a prosecution'.

The first hurdle the South African authorities had to overcome was the question of whether Nigeria would apply for the accused's extradition, as the offences had taken place in that country, or whether it would assist South Africa by providing the necessary evidence for the accused to be prosecuted in South Africa.

As early as the bail application the accused communicated his intention to oppose any application for this extradition to Nigeria on three grounds, namely:

- Nigeria still enforced the death penalty[183]
- He would not receive a fair trial[184]
- He was persona non grata in Nigeria

In February 2011, the Nigerian Attorney-General[185] gave a written undertaking not to apply for the accused's extradition to Nigeria, and guaranteed Nigeria's co-operation with South Africa in the investigation, the provision of evidence and the availability of witnesses.

It was evident from the onset that the accused could not be prosecuted in South Africa without reliable and admissible evidence having been obtained in Nigeria. As a result, informal sharing of information and intelligence took place on a prosecutor-to-prosecutor, police-to-police and intelligence-to-intelligence basis. It was during these interactions that reliable and admissible evidence implicating the accused in the Warri bombings also surfaced. This resulted in a formal letter of request being submitted to Nigeria and the US:

Evidence requested from Nigeria included:

- Witness statement from justice collaborator witnesses and/or co-perpetrators who were granted amnesty in return for their voluntary co-operation
- Forensic evidence and photo albums from the scene of both the Warri and Abuja bombings
- Detailed itemised telephone billing records from service providers
- Forensic analysis of mobile telephone handsets, SIM cards and laptop computers and notepads of collaborator witnesses and Nigerian co-accused
- Victim and eye witness statements
- Hospital records, post-mortem reports, medical reports, chain statements etc.
- Reports on damage to property
- Bank records
- Hotel records
- Movement Control records

- Company records
- Witness statements from former MEND militants
- Statements from senior government officials, including cabinet ministers
- Vehicle purchase registration records

Evidence requested from the US included:

- Expert post-blast explosive reports (experts from the US had conducted forensic and ballistic investigations at the scene of the Abuja bombings and had collected swabs and samples that were submitted to the US for expert analysis)
- Email account information and records from Yahoo

The aforementioned evidence was crucial to a successful prosecution in either South Africa or Nigeria. The final indictment was drawn up with the accused facing 13 terror-related offences. These included the following charges (demonstrating South Africa's domestication of UN conventions, UN Security Council resolutions and the OAU Convention):

- Two counts of engaging in terrorist activities[186] (falls within the ambit of the OAU Convention on the Prevention of Terrorist Bombings)
- Two counts of delivering, placing and/or detonating an explosive device causing death and serious bodily injury[187] (falls within the ambit of the International Convention for the Suppression of Terrorist Bombings)
- Two counts of delivering, placing and/or detonating an explosive device with the purpose of causing extensive damage to and/or destruction of a place and/or facility[188] (falls within the ambit of the International Convention for the Suppression of Terrorist Bombings)
- Two counts of attempting to cause harm to internationally protected persons[189] (falls within the ambit of the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons including Diplomatic Agents)
- Two counts of terror financing: providing and/or making available property to commit or facilitate the commission of a specified offence[190] (falls within the ambit of the International Convention on the Suppression of the Financing of Terrorism)

- Two counts of committing an act that enhances the ability of an entity to engage in a terrorist activity[191] (falls within the ambit of the OAU Convention on the Prevention of Terrorist Bombings)
- One count of threatening to engage in a terrorist activity[192] (falls within the ambit of the OAU Convention on the Prevention of Terrorist Bombings and the International Convention Against the Taking of Hostages)

3.3 A legitimate armed struggle

The accused objected to the jurisdiction of the court on the basis that the charges related to his engagement in a legitimate armed struggle and placed reliance on the African (Banjul) Charter on Human and People's Rights and the judgements in *SERAP v the Federal Republic of Nigeria*[193] and *Aniso & Others v The President and Commander-in-Chief of the Armed Forces of the Federal Republic of Nigeria & Others*,[194] in an attempt to demonstrate the legitimacy of his conduct.

Banjul Charter

The accused's reliance on the Banjul Charter was misplaced. Article 7(2) of the Banjul Charter provides that the accused may not be condemned for an act that did not constitute a legally punishable offence at the time of its commission. The accused's acts amounted to various offences in two different countries. Article 29(3) places an obligation on the accused not to compromise the security of the state whose national or resident he is. Article 29(4) obligates the accused to preserve and strengthen social national solidarity, especially when same is threatened. Article 29(5) obligates the accused to preserve and strengthen the national independence and territorial integrity of his country and to contribute to its defence, and Article 29(7) obligates the accused to engage with members of society in the spirit of tolerance and dialogue and to contribute to the promotion of the moral well-being of society. The cases of SERAP and Aniso refer to the situation in the Niger Delta prior to amnesty being granted to the accused and prior to the initiatives undertaken by the Nigerian government, and are markedly distinguishable from the accused's case. The court correctly determined that there was '[n]o basis in fact or in law … before this Court by the accused to bring himself within the four corners …' of his actions forming part of a legitimate armed struggle.

3.4 South African court's assumption of extra-territorial jurisdiction

The accused also objected to the court having jurisdiction to hear his matter. In this regard, the applicable UN conventions referred to above call for state parties to establish jurisdiction over offences where, inter alia:

- The alleged offender is present in the territory of that state and it does not extradite him
- The offender is not extradited (here the state party is obligated to submit the case to its competent authorities for prosecution)

The above principles are commonly referred to as *aut dedere aut judicare* (i.e. extradite or prosecute). In *Mohamed and Another v President of the Republic of South Africa and Others*[195] the Constitutional Court held that:

> 'Extradition is a consensual act by two States directed at the handing over by one State to another State of a person convicted or accused there of a crime so that the receiving State may deal with it in accordance with the provisions of its law. It involves a request by the first State for such delivery and delivery by the requested State for the purposes of trial or sentence in the territory of the requesting State'.

The expression *aut dedere aut judicare* is a modern adaptation of a phrase used by Grotius: *'aut dedere aut punier'* (either extradite or punish):[196]

> … *aut dedere aut judicare* is commonly used to refer to the alternative obligation to extradite or prosecute which is contained in a number of multilateral treaties aimed at securing international cooperation in the suppression of certain kinds of criminal conduct …[197]
>
> 'The verb judicare primarily means 'to judge' or 'to try'. It suggests a full trial …; It only requires that the requested state take steps towards prosecution: However, the noun form judicatio also can refer to 'an inquiry into an accusation'.[198]
>
> The question of jurisdiction is required to be contextualised 'within the broader parameters and principles of public international law (PIL)'.[199]

International treaties impose international duties on persons.[200] Antonio Cassese further argues that international criminal law is a branch of PIL whose rules 'emanate from sources of international law (treaties, customary law etc.). Hence, they are subject, among other things, to the principles of interpretation proper to that law.'[201] In this regard, 'a core principle of PIL which has assumed customary status is that of state sovereignty …', which 'dictates that states are empowered to act at their discretion within their own territory'.[202]

> A state's jurisdiction, being 'the authority that a state has to exercise its governmental functions by legislation, executive and enforcement, and judicial decrees over persons and property', is derived from its sovereignty.[203]
>
> … failing the existence of a permissive rule to the contrary [a state] may not exercise its power in any form in the territory of another state … jurisdiction … cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.[204]

In *National Commissioner, SAPS v SAHR Litigation Centre*,[205] the court, referring to *R O'Keefe*,[206] noted the general distinction drawn between (1) prescriptive, (2) enforcement and (3) adjudicative jurisdiction. Prescriptive jurisdiction empowers states to proscribe certain conduct through either the common law or its national legislation.[207] In this regard, international law traditionally recognises several bases for jurisdiction. This primarily includes territoriality, nationality, residence and the commission of acts that are considered to prejudice a state's safety and security. Enforcement jurisdiction enables states to enforce prescriptions through investigations and prosecutions,[209] while adjudicative jurisdiction is states' capacity to determine the outcome of a matter followed through the exercise of enforcement jurisdiction.[210]

In *R. v. Hape*, the Canadian Supreme Court recognised the roles of extraterritorial prescriptive and extraterritorial adjudicative jurisdiction.[211] In *National Commissioner, SAPS v SAHR Litigation Centre*,[212] the court in referring to the following extract from the *Lotus Case*,[213] recognised that there are no absolute restrictions on jurisdiction:

> 'It does not, however, follow that international law prohibits a State from exercising jurisdiction in its own territory, in respect of any case which relates to acts which have taken place abroad, and in which it cannot rely on some permissive rule of international law … it leaves them in this respect a wide measure of discretion which is only limited in certain cases by prohibitive rules;

as regards other cases, every State remains free to adopt the principles which it regards as best and most suitable.

"Crimes that struck at the whole of humankind and impinged on the international conscience led to greater efforts to ensure that their perpetrators did not go unpunished".'[214]

Hence, a need arose to adequately implement measures to combat such crimes nationally and internationally, thereby preventing perpetrators from seeking out states as safe havens to avoid prosecution and punishment.

Although the court in *National Commissioner, SAPS v SAHR Litigation Centre*[215] refers to international crimes (piracy, war crimes and Rome Statute offences, etc.) in the context of universal jurisdiction, noting that the

[I]ncreased consciousness of human rights and fighting impunity gave rise to an emerging and sometimes contested additional basis for prescriptive jurisdiction, namely the idea of universal jurisdiction, which suggests that states are empowered to proscribe conduct that is recognised as [threatening] the good order not only of particular states but of the international community as a whole. They are crimes in whose suppression all states have an interest as they violate values that constitute the foundation of the world public order … [T]his basis for jurisdiction is not tied to the state's territory or some other traditional connecting factor, but is rather grounded in the universal nature of the offence committed, it is aptly applicable to terrorism and related crimes.

The court went on to say:

[S]tates opted for the passing of international conventions on specific categories of conduct. They thus agreed upon a string of conventions through which they imposed on contracting parties the obligation to make punishable and to prosecute in their domestic legal orders certain classes of actions … The conventions refrained from terming the conduct terrorist.[216]

South Africa has expressly created extra-territorial jurisdiction in section 15 of POCDATARA.[217] The long title of the Act, inter alia, reads:

To provide for measures to prevent and combat terrorist and related activities; … an offence of terrorism and other offences associated or connected with terrorist activities; … for Convention offences; to give effect to international instruments dealing with terrorist and related activities; … a mechanism to

comply with United Nations Security Council Resolutions, which are binding on member States, in respect of terrorist and related activities; … measures to prevent and combat the financing of terrorist and related activities; … investigative measures in respect of terrorist and related activities; and to provide for matters connected therewith.

Although phrased differently, the content of the long title has, by and large, been incorporated into the Preamble of the Act which, inter alia, in so far as it is relevant, recognises and emphasises that:

- Terrorist and related activities are intended to achieve political and/or other aims violently and/or unconstitutionally
- Terrorism and related activities are an international problem
- Terrorism can only be effectively addressed by means of international cooperation
- The South African government has committed itself in international forums such as the UN, AU and Non-Aligned Movement to the prevention and combating of terrorist and related activities
- It is a requirement of UN Security Council Resolution 1373/2001, which is binding on all UN member states, and the Convention for the Prevention and Combating of Terrorism for member states to become party to instruments dealing with terrorist and related activities
- The UN Security Council passes resolutions under Chapter VII of the UN Charter, inter alia, requiring member states to combat terrorist and related activities, and by taking effective measures to prevent and combat the financing of terrorist and related activities
- In relation to domestic (or municipal) legislation and co-operation, and in emphasising *Aut dedere aut judicare*: the duty to extradite or prosecute in international law, its sovereign discretion, the preamble notes:

> '[the] importance to enact appropriate domestic legislation necessary to implement the provisions of relevant international instruments dealing with terrorist and related activities, *to ensure that the jurisdiction of the courts of the Republic of South Africa enables them to bring to trial the perpetrators of*

> *terrorist and related activities*; and to co-operate with and provide support and assistance to other States and relevant international and regional organisations to that end' [own emphasis] and further recognises South Africa's obligations in the fight against terrorism nationally and internationally in that it is *'committed to bringing to justice persons who commit such terrorist and related activities; and to carrying out its obligations in terms of the international instruments dealing with terrorist and related activities'* [own emphasis]

UN Security Council Resolution 1373/2001 reaffirms that any act of international terrorism constitutes a threat to international peace and security and calls upon states to work together to prevent and suppress terrorist acts, through increased co-operation and full implementation of the relevant international conventions relating to terrorism.[219]

> In this regard, states are obligated in terms of Article 2(c) to '[d]eny safe havens to those who finance, plan, facilitate or commit terrorist acts, or provide safe havens'; to (Article 2(d)) prevent their territories from being used to commit terrorist and related acts; and to (Article 2(e)) ensure such persons are brought to justice by domesticating appropriate laws and regulations to combat such crimes.

In reference to other binding international instruments, the preamble confirms that South Africa is a party to a number of UN conventions and protocols, as listed.

This is clearly indicative of South Africa having promulgated the POCDATARA Act, to give effect to its international obligations in terms of the international instruments dealing with terrorist and related activities.

In this regard, Section 1(1)(ii)(a) of the POCDATARA Act, inter alia, defines a 'Convention offence' as 'an offence, created in fulfilment of the Republic's international obligations in terms of instruments dealing with terrorist and related activities, referred to in Part 2 of Chapter 2'.

The aforementioned international instruments largely obligate states parties to establish jurisdiction over the offences concerned under circumstances where, inter alia: (1) the offence is committed against that state or in its territory; (2) the offence is committed by a national of that state; (3) the offence is committed by a stateless person who habitually resides in that state; (4) during the commission of the offence,

a national of that state is seized, threatened, injured or killed; (5) the offence is committed in an attempt to compel that state to do or to abstain from doing any act; or (6) the offence is committed against the security of the state party.

These jurisdictional bases fall within the ambit of prescriptive jurisdiction and the requirements of territoriality, nationality, residence and the commission of acts that are considered to prejudice a state's safety and security, as referred to in *National Commissioner, SAPS v SAHR Litigation Centre*.[220]

Significantly, the international instruments[221] obligate a state party to 'take such measures as may be necessary to establish its jurisdiction over the offences … in cases where the alleged offender is present in its territory and it does not extradite him to any of the state parties which have established their jurisdiction'.

This clause is apposite to what the court in *National Commissioner, SAPS v SAHR Litigation Centre*[222] describes, falls squarely within Articles 2(c), (d), (e), (f) and 3(c) of UN Security Council Resolution 1373(2001) and is in line with South Africa's international obligations.

In *Glenister v President of the Republic of South Africa and Others*,[223] the Constitutional Court set out South Africa's constitutional obligations and duties to give effect to relevant international instruments and how the constitution integrates international law into the country's domestic legislation.

In *Minister of Home Affairs and Others v Tsebe and Others*,[224] the Constitutional Court, in reference to the Prevention and Combating of Corrupt Activities Act[225] and the Implementation of the Rome Statute of the International Criminal Court Act,[226] recognised that South Africa had passed legislation to give its court's jurisdiction to try crimes which have been committed outside South Africa'; the concern that the South Africa should not be seen as a safe haven; and that 'if the government cannot deport or extradite persons … this may be seen as undermining its obligations under treaties concluded … in terms of which they must co-operate to fight crime … This Court regards these concerns as legitimate because it is true that government must not only fight crime but it must also be seen to be sparing no effort in fighting crime.'

In *South African Litigation Centre & Another v National Director of Public Prosecutions*,[227] the North Gauteng High Court recognised South Africa's international obligations to investigate and prosecute crimes in South Africa that are in contravention of the Implementation of the Rome Statute of the International

Criminal Court Act. In an appeal to the Supreme Court of Appeal on 27 November 2013 in *National Commissioner, SAPS v SAHR Litigation Centre*,[228] the latter confirmed South Africa's international obligations and the jurisdictional fact of it having jurisdiction to not only investigate but also prosecute such crimes where extra-territorial jurisdiction is created expressly by the statute or otherwise.

In this regard, Section 15 of the POCDATARA Act expressly sets out the legal provisions of jurisdiction in respect of offences under the Act. These include:

- Where the accused is arrested in South Africa
- Where the accused is ordinarily resident in South Africa
- Where the offence was committed outside the Republic and the accused is found in the Republic
- Where the accused is not extradited
- Where there is no application for his/her extradition

3.5 Consular rights

The terrorist conventions and protocols also obligate states parties that, in exercising their discretion in relation to the *aut dedere aut judicare* principle, decide in favour of prosecuting the offender, to entitle the offender to:

- Communicate without delay with the nearest appropriate representative of the state of which he/she is a national; or with a representative of a state that is otherwise entitled to protect his/her rights; or, if the offender is a stateless person, a representative of the state in the territory in which that person habitually resides
- Be visited by a representative of that state
- Be informed of the aforementioned rights

The aforementioned consular rights, albeit phrased somewhat differently and provided for in most, if not all, the conventions and protocols discussed in Part 2, are intrinsically linked to the rights enshrined in Article 36 of the Vienna Convention.[229]

After his conviction and before sentencing, Okah brought an application before the trial court requesting the noting of special entries of irregularities[230] that were alleged to have occurred during his trial but that were not reflected on the record and that rendered his trial unfair.[231] One of the grounds advanced by the accused read as

follows: 'The applicant had not been warned of his rights in terms of Article 7(3)(a), (b), (c) of the International Convention for the Suppression of Terrorist Bombings.'[232]

The accused, placing reliance on *La Grand*[233] *and Avena,*[234] argued that had he been advised of his consular rights in terms of Article 7(3), a different solution would have been found in dealing with his matter. The aforementioned consular rights are analogous to that provided for in Article 36 of the Vienna Convention on Consular Relations, as discussed earlier.

The Court in *S v Okah*,[235] in analysing the accused's application, held that:

> The precepts for a fair trial under our Constitution allow, for example, evidence obtained unconstitutionally to be tendered in a court of law without necessarily undermining the fairness or legality of the particular trial. It is, therefore, trite that an irregularity is not viewed in vacuo, but must be seen in the light of all the relevant surrounding circumstances.[236]

The Court dismissed Okah's application as frivolous and absurd, although he had not been advised of his rights in terms of Article 7(3) either immediately after his arrest or at any stage thereafter, and not even after his conviction. In this regard, the court held that the failure to advise the accused of his Article 7(3) rights did not render his trial unfair, nor did it amount to an irregularity or an injustice, as the accused was regarded as persona non grata in Nigeria; he could not be extradited as Nigeria still imposed the death penalty, and as such, South Africa was obligated to invoke mechanisms to prosecute him domestically; the Nigerian consular representative was present throughout the trial; and South Africa had formally obtained evidence and witnesses from Nigeria that was used in the trial against the accused and who testified against him, including very senior Nigerian government officials. Without the Nigerian government's assistance the accused would not have been arrested and prosecuted in South Africa.

3.6 Concluding remarks

The Okah matter emphasises that prosecutors and law enforcement officials are required to be vigilant at all times and be armed for all sorts of legal challenges. However, most importantly, it signified that two African states with vastly different law enforcement authorities, histories, cultures, and social-economic and political circumstances can co-operate in the fight against terror.

Chapter 4

Other experiences and challenges

4.1 Angola

Attack on the Togo National Football Team, case no. 426-C2010

On 8 January 2010 two buses transporting the Togo national football team to the 2010 African Cup of Nations football tournament were attacked by gunmen from the Front for the Liberation of the Enclave of Cabinda (FLEC) in Cabinda, Angola. Two people died and eight sustained injuries. Two suspects were arrested the same day.

Investigations revealed that the leaders of the FLEC – over 30 people living in Congo-Brazzaville, the DRC, Gabon, France, Luxembourg, Portugal and Belgium – had ordered the attack. This resulted in international warrants of arrest being issued for the leaders, as well as applications for their extradition to Angola.

One of the accused was acquitted, while the other was subsequently convicted on charges of armed rebellion, murder and attempted murder, and sentenced to an effective 24 years' imprisonment. 'Armed rebellion' has since been criminalised as terrorism, in accordance with Article 19 and 20 of Law n.7/78.

The Angolan authorities found that:

- Investigations were poorly conducted
- Both prosecutors and investigators failed to explore electronic evidence
- International co-operation was inefficient
- No responses were received in respect of applications for the extraditions and letters rogatory submitted

- There was a lack of capacity and training in the investigation and prosecution of international terrorism matters
- There was little to no collaboration and networking with international prosecutors

4.2 Namibia

S v Calvin Liseli and 119 others, case no. 32/2001

On 2 August 1999 the Caprivi Liberation Army (CLA) launched unanticipated attacks on an army base, a border post and the police station of Katima Mulilo, the provincial capital of the Caprivi Region, Namibia, and occupied the state-run radio station. Fourteen people were killed in the subsequent fighting between rebel and government forces. A state of emergency was declared in the province, and the government arrested alleged CLA supporters. A total of 132 suspects were arrested and charged with high treason, murder and a host of other offences. The trial has lasted over a decade and is yet to be concluded at the time of writing, with many rulings being delivered, including on jurisdiction.

The Namibian authorities learned the following lessons:

- Not to prosecute too many accused
- The prosecution should get involved in the investigation as early as possible to assist the police in identifying and collecting admissible evidence
- To make use of identification parades in the identification of suspects
- The collection of incriminating evidence against accused should be audio and visually recorded
- The recording of incriminating evidence should take place in the presence of an objective third party who can corroborate the evidence to the magistrate
- A witness protection programme should be in place to assist vulnerable witnesses whose evidence is essential

4.3 Uganda

Joan Kagezi, a Ugandan prosecutor, lists the following challenges in prosecuting terrorism and related offences:

- Many terrorist groups operate across borders, necessitating investigations having to be conducted across borders. The gathering of evidence in some territories may be challenging due to disharmony in laws or the lack of enabling laws for law enforcement agencies, thereby hampering co-operation.
- Witnesses from foreign jurisdictions may need protection, as more often than not they and their relatives face physical and psychological intimidation.
- Co-ordination of cross-border investigations is required.
- There is a lack of common standards and accepted practices in the actual supervision of the investigation.
- The bureaucracies involved hamper evidence collection.
- Most witnesses/victims of terrorism are traumatised and interviewing them often just aggravates their situation. Others may be re-traumatised in the course of the investigation. Victims are usually apprehensive about participating in trials for fear of their safety, or see no benefit in participating in the trial process since the exercise will not repair the damage they suffered.
- International co-operation in the protection of witnesses and their related persons is a necessary component of normal co-operation between prosecution services. It is important that prosecutors and investigators develop arrangements with other jurisdictions for the safe examination of witnesses at risk of intimidation or retaliation.
- Disharmony in laws hinders co-operation among states. Uganda still invokes the death penalty and countries that do not are often reluctant to extradite or offer mutual legal assistance.
- Cultural barriers often hinder victims from co-operating. Some communities may even stigmatise the witnesses who come forward to co-operate with prosecutors and investigators. For example, in Uganda women are traditionally not supposed to stand up to men, and most witnesses of

abduction are apprehensive about giving testimony. These factors influenced the girlfriends of the accused in the terrorism case of July 2010.

- Investigators and prosecutors are psychologically affected by the nature of the cases they work on.
- The initial stages of major cases involve many stakeholders, resulting in a lack of co-ordination or different actors wanting to highjack the process for different reasons. Lack of control under one manager has an extremely negative impact on the investigation and successful prosecution. A number of times, senior officers take up the responsibility of collecting evidence from foreign jurisdictions and are reluctant to take part in the court proceedings, which has a negative impact on the case.
- Unnecessary challenges or preliminary objections from the defence at times delay hearings, yet victims and the public are also entitled to speedy justice. This demoralises witnesses and the public.

4.4 Tanzania

Extradition applications in Kampala bombings

Uganda submitted two extradition requests to Tanzania in relation to suspects involved in the Kampala bombings of July 2010, which claimed the lives of 76 people.

In the first matter, Seleman Hijar Nyamandondo, a Tanzanian national living in Arusha, had been in police remand for about a month following his arrest on a provisional arrest warrant issued at the Nakawa Magistrate's Court in Kampala, Uganda for his alleged involvement in the Kampala bombings. The competent authority of Uganda initially submitted the extradition request on charges of aiding and abetting terrorism contrary to Section 8 of the Anti-Terrorism Act 2002 of Uganda, which provides for the death penalty in case of a conviction. The same offence is punishable by 15 years' imprisonment in Tanzania. As a result the initial extradition application was refused. Further investigations revealed that he was involved in an actual killing. Hence the charge of aiding and abetting was substituted with that of murder and attempted murder contrary to sections 188, 189 and 204 of the Ugandan penal code, resulting in

the accused's extradition. The Tanzanian authorities also acceded to a request for MLA by seizing a Toyota Land Cruiser used by the accused to transport explosives to Uganda. This vehicle was used as an exhibit by the Ugandan authorities.

In the second matter, Mohamed Ali Mohamed, a Kenyan citizen, was also extradited to Uganda to face terror charges.

The Tanzanian authorities experienced the following challenges in both matters:

- The accused were respectively remanded in police custody for periods ranging from several days to about a month before being brought to court, resulting in habeas corpus applications.
- The Extradition Act of Tanzania affords the accused the right to appeal within 15 days. Both accused were extradited to Uganda before the expiration of the statutory period. This resulted in the accused filing constitutional petitions in Uganda, challenging the legality of their extraditions in that they were denied the right to appeal before being extradited.

Part 5

Witness protection

Mr Dawood Adam and Adv. Shaun Abrahams
Special Director for Witness Protection, Priority Crimes Litigation Unit, National Prosecuting Authority of the Republic of South Africa

Index

Aim and objective

The strength of the prosecution's case is largely dependent on the reliability of admissible evidence and on the recollection of the viva voce evidence of its witnesses, which must ordinarily be presented in open court, in the presence of the accused, and be subjected to cross-examination. This is inherent in the right to a fair trial and the principle of open justice.

In most terrorism, organised crime, corruption and transnational serious crime cases, witnesses are reluctant to collaborate with law enforcement authorities by providing key information, witness statements and testifying due to legitimate fears for their and/or their related persons' safety or threats to their lives. Prosecutors, investigators or courts are thus regularly called upon to invoke necessary measures to safeguard key witnesses and their related persons, thereby not only protecting the witnesses concerned but also securing and protecting the integrity of reliable and admissible evidence.

The aim and objective of this section is to familiarise prosecutors with the concept of witness protection, and to discuss best practices on the African continent and the UN Guidelines on Witness Protection in order for prosecutors to:

- Understand the concept and the need for witness protection
- Appreciate best practices on witness protection

Chapter 1

Introduction

The emerging trends and increase in transnational crimes such as terrorism, money-laundering, piracy, cybercrime, trafficking in persons and drugs, organised crime, corruption and other international crimes (e.g. genocide, crimes against humanity and war crimes), pose a threat to global peace and security and, more particularly, hinders economic development, the rule of law and political stability on the African continent.

Criminal justice responses hereto depend significantly on the testimony of witnesses who can detail the accused's involvement in the commission of the gravest and most serious and complex crimes known to mankind. Without the reliable testimony of key witnesses who can testify without fear of reprisal, the chances of the successful investigation and prosecution of the aforementioned crimes are extremely low. This often results in acquittals, dismissals, the threatening and killing of witnesses, the obstruction and/or defeating of justice and, ultimately, the failure of justice. A culture of impunity can thus be expected to prevail in the absence of effective witness protection, which inevitably negates the rule of law.

Due to the serious nature of the crimes, the power and profile of some accused and the sophistication of terror groups and organised crime syndicates, witnesses are often fearful of the consequences of participating in the investigation or prosecution process. The protection of witnesses and their related persons who provide crucial and significant testimony must therefore guarantee protection from reprisal against themselves and their related persons. Cases that have come before the ICC, the International Criminal Tribunal of Rwanda (ICTR), the Special Court for Sierra Leone and the International Criminal Tribunal for Yugoslavia (ICTY) reflect the significant challenges faced in securing the co-operation of witnesses in high-profile cases and the potential disastrous consequences for witnesses who have not been protected. Numerous witnesses have withdrawn their testimony amid security concerns and

claims of intimidation. In other instances, witnesses have vanished or are reported to have been killed or been subjected to bribery.

Witness protection measures are an essential element of a state's arsenal against organised crime. States can only positively respond to the safeguarding of witnesses and protect the integrity of their evidence by having formal legislation or policies domestically on witness protection services that make provision for a framework from which states or authorities can render witness protection services, both domestically and transnationally.

Most states in Africa lack the required laws, institutions and/or capacity for effective witness protection. Despite the slow pace in establishing witness protection regimes, many African countries have acknowledged the need for such services, and have declared their intention to advance the development of witness protection in their national jurisdictions. However, to date only South Africa, Kenya, Namibia, Mozambique, Rwanda and Uganda have made progress in the establishment of functioning witness protection programmes in Africa.

Current status of witness protection programmes

Angola	Keen to develop
Democratic Republic of Congo	Keen to develop
Egypt	Criminal code
Ethiopia	Law: developing institution
Kenya	Law and WPA compliment
Mozambique	Law: no institution
Morocco	Law: limited capcity
Namibia	Draft law: no institution
Nigeria	Draft law: limited capacity
Rwanda	Law and limited capacity
South Africa	Law and OWP
Tanzania	Keen to develop
Uganda	Draft law: due to come to RSA OWP July 2015, Kenya WPA will also assist

Chapter 2

The role of the United Nations

Article 24 of UNTOC[237] obligates states parties to take appropriate measures to provide effective protection from retaliation or intimidation to witnesses who provide testimony in cases involving transnational organised crime. These measures include:[238]

- The physical protection of witnesses and their related persons
- The relocation of witnesses and their related persons
- The non-disclosure or limitations on the disclosure of the identity and whereabouts of witnesses
- The introduction of evidentiary rules that permit the testimony of witnesses to be given in a manner that ensures their safety, but which also pays due regard to the fair trial rights of an accused
- The entering into agreements or arrangements between states parties in respect of the relocation of witnesses

UNCAC[239] calls upon states parties to take appropriate measures to protect witnesses against retaliation or intimidation aimed at preventing them from presenting their testimony.[240] This convention also makes provision for the protection of witnesses to be extended to family members[241] or persons close the witness. It proposes certain measures for consideration, which include:

- The institution of physical security procedures, e.g. the relocation of witnesses and non-disclosure of information relating to the witnesses' identity and/or whereabouts

- The creation and utilisation of evidentiary rules to ensure the witnesses' safety during courtroom testimony
- The signing of agreements between states parties so as to facilitate the transnational relocation of witnesses

UNTOC also presupposes that states parties should take appropriate measures to protect witnesses in criminal proceedings related to crimes covered by the convention and its protocols, which include the following categories of crime:

- Participation in an organised criminal group
- Money-laundering
- Corruption, particularly corruption in the public sector
- Defeating and/or obstructing justice
- Trafficking in persons
- Illicit manufacturing of and trafficking in firearms, parts and/or components of firearms, and ammunition
- Migrant smuggling
- Other serious crimes as defined in the convention that encompass a transnational element, along with the involvement of an organised criminal group and/or entity

In this regard, witness protection is particularly important to the global initiatives to combat and fight the scourge of terrorism. Terrorist entities often operate in a clandestine manner, which makes it extremely difficult to use successfully traditional investigative measures and techniques to gather crucial evidence or information or to disrupt their actions, plans and/or initiatives. As such, the only way of breaching terrorist entities' activities is to use justice collaborators or human sources to infiltrate these entities in legitimate law enforcement undercover operations. Ordinarily, justice collaborators would benefit from some sort of immunity or substantially reduced sentences for their testimony. More often than not, these witnesses have to be placed in a witness protection programme or in protective custody.[242]

The UN,[243] long before drawing up UNTOC and UNCAC and after studying the formal and informal witness protection initiatives of various countries, created the *Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime*.[244] Countries are increasingly enacting legislation and/or adopting policies to protect witnesses (and their related persons) whose evidence is crucial to a successful prosecution or investigation and where co-operation with law enforcement authorities or testimony in court of law would endanger their lives or those of their related persons,[245] thereby creating a suitable platform for a witness to give testimony or co-operate with law enforcement authorities without fear of intimidation or reprisal.

The protection afforded to witnesses may simply include the following:

- Providing a police escort to and from interviews and court
- Relocating the witness to a temporary residence, e.g. a safe house
- Using modern communication technology for the witness's testimony, e.g. video conferencing

However, in other cases where the co-operation of witnesses is critical to a successful prosecution, extraordinary measures may be required to ensure the witness's safety in circumstances where the criminal entity is extremely powerful, with tentacles reaching almost everywhere. In these instances, resettlement of the witness under a new identity and in a new, undisclosed place of residence, domestically or internationally, may be the only viable remedy.[246]

Chapter 3

Witnesses

Witnesses may be classified into three main categories, namely:[247]

- Justice collaborators
- Victim witnesses
- Other types of witnesses

Justice collaborators are persons who had participated in an offence connected with the criminal organisation and/or who possess important knowledge in relation to the organisation's structure, modus operandi, activities and domestic and international links. Ordinarily, justice collaborators enjoy lenient sentences or immunity from prosecution, as well as witness protection, which is considered an extremely powerful tool in the successful prosecution of organised crime cases.[248] However, this practice does raise ethical issues, as it may be perceived that criminals are rewarded for their crimes.[249]

Victim witnesses[250] 'are those persons who, individually or collectively have suffered harm, including physical or mental injury, emotional suffering, economic loss or substantial impairment of their fundamental rights, through acts or omissions that are in violation of criminal laws operative in Member States, including those laws proscribing the criminal abuse of power'.

Ordinarily, there is general agreement that these types of witnesses should receive assistance before, during and after their participation in a trial, to ensure their physical safety and for in-court protection measures to be applied. Victim witnesses may also be included in a witness protection programme if all other conditions are fulfilled, i.e. value of testimony; absence of other effective means of protection; existence of serious threats; and the personality of the witness.

Other participants are the categories of people who are involved in a criminal case but who are also subject to danger and/or threats, such as judges, prosecutors, undercover agents, interpreters and informants.

Assistance and protection measures afforded to witnesses instil confidence in them to come forward and testify, which in turn instils confidence in the administrators, the proper administration of justice and the rule of law. In many instances, a witness's security concerns may be sufficiently addressed through:

- Assistance before and during the trial
- Police measures to enhance physical security
- Court procedures to ensure the witness's safety in giving testimony

Witness protection programmes are essentially for those extraordinary, important cases where the threat against a witness is so serious that protection and support cannot be secured by any other means and where the witness's evidence is crucial to the prosecution's case or the investigation.

It is advisable that security measures be considered in all instances where witnesses believe that there is an imminent threat or danger directed at them as a result of their involvement in assisting law enforcement authorities in a criminal case. Measures one should consider implementing include:

- Arranging a temporary change of residence, including temporary accommodation in safe houses
- Organising close protection, regular patrolling around the witness's residence, an escort to and from court and the provision of emergency contacts
- Changing a telephone number or having an unlisted number assigned to the witness
- Monitoring mail and telephone calls
- Installing security devices at the witness's residence
- Providing electronic warning devices
- Using discreet premises to interview and brief the witness

Witness protection is more often than not an essential component of the successful prosecution of organised crime and terrorism. In fact, it is integral to states in Africa's ever growing willingness to address terrorism, corruption and transnational organised crime. The protection of witnesses from intimidation is crucial to the integrity and success of the process. The primary objective of witness protection is to protect the physical security of witnesses for the purpose of securing their testimony in the criminal justice process.

It is widely accepted that states generally have an obligation to provide assistance and protection to persons who collaborate with law enforcement and/or the criminal justice system in enhancing the administration of justice. The kind of assistance or protection provided in each given case depends largely on the type of witness, the nature of the crime and, more importantly, the level of threat or intimidation.

Witness protection programmes are essentially established to address the inability of regular police protection measures to provide a secure environment for witnesses willing to testify against powerful accused. Their success have had an immense impact in securing crucial evidence and have made witness protection a key element in efforts to effectively fight organised crime and terrorism.

Domestic laws and the social, socio-economic, cultural and political environment, along with various states' crime typographies, inter alia, have a significant impact on how states address the issue of witness protection. The aforementioned differences reflect the nature and extent of witness protection that states are able to provide.

Some of the most fundamental elements crucial to creating and operating witness protection programmes or initiatives are, among others:

- A defined law or policy for designing a methodology to carry out operations
- Adequate and sustainable financing
- Strict personnel qualifications and vetting procedures
- The maintenance of the programme's integrity
- Co-ordination and collaboration with key stakeholders in judicial, law enforcement and other government agencies, including intelligence, correctional services, social welfare and security, internal or home affairs, etc.

- Operational and financial accountability and transparency (only for auditing, due to the level of classification of the secure environment within which witness protection operates)
- The appropriate assistance in safeguarding the information disclosed
- The ability to offer assistance to national and international law enforcement agencies

In this regard, admission criteria to a witness protection programme depend significantly on:

- The severity of the threat to the witness
- The seriousness of the crime in respect of which the witness is testifying or assisting law enforcement
- The importance of the testimony
- The witness's willingness to co-operate
- The witness's suitability for being included in the programme in terms of psychological, mental and medical conditions

From a practical and administrative perspective, it is advisable for witness protection programmes or initiatives to:

- Exist and operate independently of law enforcement, particularly the investigation
- Enjoy operational autonomy from the regular police
- Be guaranteed secrecy and security of information
- Not be subjected to political influences in the work of the programme

In reference to international relocations, it is advisable for states to:

- Develop agreed minimum standards on international relocation
- Simplify witness application and admission procedures
- Harmonise regional and national legislation and/or policies

- Create networks of witness protection agencies to establish direct contact among relevant officials
- Enhance training standards for personnel
- Develop common criteria for the determination of living standards and benefits for witnesses relocated to other countries

Chapter 4

Good practices and case studies

South Africa was the first country in Africa to have a witness protection scheme. Prior to its development, Section 185A of the Criminal Procedure Act[251] provided for the voluntary detention of witnesses. This section was rather oppressive in nature and was regularly used by the former apartheid government to coerce witnesses into testifying in political trials and in providing information in investigations into the activities of liberation fighters, supporters and entities. Under this scheme, witness protection was managed by the prosecutor, while the protection of the witness was a police function. The management of a witness's affairs and services rendered in relation thereto was largely racially based in favour of the white minority that governed the country. This law was widely abused and often led to the violation of both witnesses' and accused's fundamental human rights.

After attaining democracy in 1994, the new South African government recognised the deficiencies and constitutional impediments inherent in Section 185A, which resulted in a drastic overhaul of the country's witness protection scheme.

In 1996, the South African cabinet adopted the National Crime Prevention Strategy, which recognised the protection of witnesses as a key tool in securing co-operation and evidence from threatened and intimidated witnesses, and that the witness protection scheme envisaged under Section 185A had been a weak link in the country's criminal justice system. The recommendation for witness protection also came from the Truth and Reconciliation Commission, which called for the development of new witness protection legislation that provides for an independant witness protection office. Similarly, the government appreciated the need for a witness protection scheme to be aligned to its priorities in the fight against serious crime and that it should be in compliance with international witness protection requirements.

In 2000, Section 185A was repealed by the promulgation of the Witness Protection Act 1998 (Act 112 of 1998), which, inter alia, provided for the following:

- The establishment of a national independent covert office.[252] The OWP is presently headed by a national director[253] and has branch offices in South Africa's nine provinces.
- Witness protection, according to the new act, is not a prosecution or police function, so as to ensure the independence and integrity of the office for witness protection and that of the witness on the programme.
- The regulation, functions and duties of the OWP director, including the power to decide on admissions to the programme.[254] The director's decision to refuse an application or to discharge a witness may be reviewed by the Minister of Justice.
- The identification of the nature of crimes in respect of which witnesses may request protection[255] and the procedure to be followed during applications.
- That where civil proceedings are pending against a protected person, such proceedings may be dispensed with by a judge in chambers under an ex parte application to prevent disclosure of the identity or whereabouts of the witness or to achieve the objectives of the Act.[256]
- Offences and severe penalties for any disclosure or publication of information in relation to persons admitted to the programme or OWP officials so as to ensure the safety of protected witnesses and programme officials.[257]
- That the Minister of Justice may enter into agreements with other countries or international organisations regulating the conditions and criteria for the relocation of foreign witnesses to South Africa and the admission of a witness to South Africa's witness protection programme.[258]

Further significant features of the OWP include the following:

- Witnesses must agree to enter the programme voluntarily
- There must be reasonable belief of harm ensuing
- Witnesses cannot under any circumstances be detained in a detention facility, albeit a police or prison cell
- The OWP functions covertly to secure integrity and independence

- The OWP's functions are not limited to criminal proceedings, but are extended to commissions, tribunals, inquest proceedings and organised crime enquiries
- The OWP promotes the criminal justice system by providing protection, support and related services to vulnerable and intimidated witnesses, to enable witnesses to provide an essential service without fear of intimidation, harm or danger to them or their related persons
- The OWP has developed and implemented world-leading specialised close protection of personnel training at SAQA Level 5
- The OWP ensures strict special auditing by the Auditor-General (and has had unqualified audit reports for the past 12 years)
- The OWP ensures a co-ordinated law enforcement approach and provides training to prosecutors and police
- The OWP contributes towards witness psychological/trauma management during court proceedings and creates a court environment that allows witnesses to provide testimony comfortably
- The OWP is vigilant regarding in-court intimidation
- The OWP uses technology to determine threats and work in proximity with co-ordinated law enforcement authorities to thwart these

The OWP has been instrumental in the development of witness protection initiatives in a number of African countries and tribunals by providing training to the ICTR, Chad, Malawi, Namibia, Uganda, Kenya, Zambia and Nigeria.

The OWP nevertheless acknowledges that it has some challenges in South Africa, i.e.:

- More protectors are required to comply with international best practice, which is one protector to one witness
- It faces increased budgetary requirements
- The need for a strategic war room

The OWP rendered key assistance to international witnesses in the well-publicised prosecution of *S v Okah*[259] in which the accused, a Nigerian national, was prosecuted in South Africa under the *aut dedere aut judicare* principle for his role as the leader of MEND in the bomb attacks in Warri, Nigeria on 15 March 2010 and

at the 50th Independence Day celebrations at Eagle Square, Abuja. Although the prosecution had listed 261 witnesses in the indictment[260] it only called 33, of whom 27 came from Nigeria and the rest from South Africa. These witnesses included the Minister for the Niger Delta, rehabilitated former Niger Delta militant commanders and militants, doctors, businessmen, co-perpetrators and/or co-conspirators[261] and senior Nigerian law enforcement and government officials. Due to security concerns, the OWP accommodated some of the witnesses at the commencement of the trial, and a number of witnesses, including the collaborators, were immediately admitted to the witness protection programme upon their arrival in South Africa.

In South Africa, the Department of Justice and Correctional Services is responsible for accommodating foreign prosecution witnesses. As a result of the security concerns surrounding the trial and safety of the witnesses, the OWP conducted a security assessment of the hotel identified by the department and found the security inadequate. As a result, the OWP deployed teams of protectors who collected witnesses from OR Tambo International Airport and safely transported them to their respective places of safety, guesthouses and/or hotels. At the request of the prosecutor, the OWP took witnesses to the various places in weekends. As a result OWP protectors had to work overtime for long periods of time throughout Johannesburg and Pretoria where their consultations took place, largely after hours and at the duration of the trial. The OWP also rendered in-court assistance to witnesses, the prosecution and the judge during the trial, which averted any attempts at witness and/or prosecution and/or judicial officer intimidation.

Prior to their arrival in South Africa, eight key witnesses (justice collaborators) were in the protective custody of the Department of State Security in Abuja, Nigeria for fear of being killed and/or victimised and/or intimidated by persons directed by the accused to do so and by the accused in the corresponding Nigerian matter.[262] Nigeria did not have a witness protection programme and, as a result, the witnesses were voluntarily in protective custody. Through their lawyers they had entered into formal agreements with the Nigerian Department of State Security. These witnesses had communicated their interest in testifying in South Africa on the premise that they would be admitted to the South African witness protection programme. Although they had had discussions in this regard with Nigeria's Attorney-General, the Director of Public Prosecutions and the Director-General of State Security Services in Nigeria, the witnesses said on 1 October 2012, the date the trial started in South Africa, that they were only prepared to travel to South Africa once they and their lawyers had consulted with the South African prosecutor and the head of the OWP,

and in the event that their security concerns in South Africa were satisfied. As a result, three weeks into the trial, the prosecutor and the head of the OWP travelled to Abuja, Nigeria on 19 October 2012 to address the witnesses' safety and security concerns and secure their co-operation. The witnesses arrived in South Africa on 23 October 2012 and were immediately taken into the witness protection programme and returned to Nigeria after the conclusion of their evidence.

During this impromptu visit to Nigeria, the head of the OWP rendered assistance to the Nigerian authorities by comprehensively explaining how the OWP operates and providing a legislative breakdown of witness protection laws from various countries, along with the UN's Good Practices for the protection of witnesses in criminal proceedings involving organised crime, to the Nigerian authorities. He also shared some of his practical knowledge and experience on this topic with the Nigerian authorities. To enhance co-operation between South Africa and Nigeria and to impart practical and technical skills, the head of the OWP invited seven senior Nigerian officials from the Department of State Security to work with his team, which had been deployed to assist with the protection of the witnesses in protective custody in Nigeria. This invitation was accepted. Today, Nigeria has a draft Bill on Witness Protection and has developed the practical capacity to put an Office for Witness Protection into operation.

Nigeria's Attorney-General and Minister of Justice formally extended the country's gratitude for the assistance given by South Africa in the successful prosecution of the Okah matter. The Institute for Security Studies (ISS) also commended the work of the NPA in the prosecution of the Okah matter. Although taking cognisance of the logistical nightmare the prosecution faced in bringing witnesses from Nigeria, the presiding judge later remarked on how impressed he was with the state's swiftness in having witnesses readily available to testify. Okah's successful prosecution could not have been achieved without the selfless assistance of the OWP team, who made many personal sacrifices at short notice to safeguard witnesses, the prosecution and the judge, and assisted the prosecution by making witnesses available for consultations after hours for long periods at a time. Had it not been for the swift and professional manner in which they executed their duties, the trial would not have concluded as speedily and efficiently as it had. The successful prosecution in this matter and the assistance rendered to Nigeria in relation to the development of witness protection legislation and a witness protection programme must be construed as a victory for Africa in our fight against terrorism and a key contribution to South Africa's efforts in the global fight against transnational organised crime.[263]

Chapter 5

Key challenges

- The increase in transnational organised crime and its close nexus to terrorism has had an effect on the nature of witness protection. The ever-evolving technology and the ease of access to the Internet, emails, social media, mobile phones, in particular smart phones, tracking devices, interception devices and software have increased the ease with which witnesses can be traced. In this regard, it must be stressed that witnesses can only be traced remotely if they or their related persons or persons with whom they have been in communication, use any of the aforementioned devices and are tracked, followed or traced as a direct result thereof. The Internet and social media can also be used to identify a witness or their related persons.
- States have increased security measures at controlled and uncontrolled border posts as a direct result of terrorism. To this end, they have implemented biometric systems to fingerprint and face-print and even eye-print travellers travelling into and out of their countries. Although this an extremely positive and much welcomed development, it does pose problems for transnational co-operation between states on the protection of witnesses and will, in given circumstances, require the co-operation of various government departments.
- States' political will to develop legislation and/or policies, to make funds available and to create the necessary infrastructures for witness protection schemes will have a positive impact on the use of this prerequisite tool in the fight against terror and transnational organised crime.

Part 6 and 7

Financing of terror
and
Asset forfeiture or recovery in terror financing

Index

Aim and objective

It is a truism that terrorists and/or terrorist entities or persons who espouse such values cannot operate without funds. It thus is incumbent on law enforcement authorities to curb any access thereto. The aim and objective of this section is to allow prosecutors to:

- Understand what amounts to terror financing
- Comprehend the tools and methods available to trace assets that amount to terrorist financing
- Understand freezing, seizing and confiscatory processes
- Understand the role of financial intelligence centres/agencies
- Understand the obligations imposed on financial institutions and entities
- Acknowledge and appreciate best practises

This section is written in two parts: the first, part 6, deals with the crime of financing terrorism and the second, part 7, with the freezing and forfeiture of assets connected therewith.

Part 6

Financing of terror

Adv. Chris Macadam
National Prosecuting Authority of the Republic of South Africa

Index

Chapter 1

Introduction

Stated simply, terror financing relates to the financial support of terrorism and/or the conduct of those who incite, plan or engage in terrorist activities. Such conduct is causally connected and ancillary to terrorism and terrorist activities. Put another way, how terrorism is defined will determine what activities constitute terror financing. The inability of the international community to reach a consensus on a uniform definition of terrorism is a well-documented fact.[264] This section will firstly demonstrate how the international community has sought to overcome this conceptual difficulty by agreeing that financial prohibitions should apply to activities connected with a set of defined acts of violence or coercion. Secondly, it will deal with the criminalisation of terror financing and issues directly connected thereto.

Chapter 2

The obligation to criminalise

It is generally accepted that the International Convention on the Suppression of the Financing of Terrorism[265] constitutes the first international counter-terrorism instrument that specifically focuses on the criminalisation of terror financing.[266]

This convention gives effect to UN General Assembly Resolution 51/210[267] calling upon all states to take steps to prevent and counteract the financing of terrorists and terrorist organisations, whether or not such financing is done directly or indirectly.

Although reference is made to terrorism and the financing of terrorism in the preamble of the convention, the acts required to be criminalised are not defined with reference to terrorist terminology. The following offences are created in terms of the convention:

> **Article 2 creates the offence of**
>
> 'by any means, directly or indirectly, unlawfully and willingly providing or collecting funds with the intention that they be used or in the knowledge that they are to be used in full or in part to carry out
>
> (a) any act which constitutes an offence within the scope of and as defined in one of the treaties listed to the annex;
>
> (b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature of context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.'

The convention, protocols and treaties mentioned in the annex will further be referred to as the universal counter-terrorism instruments (UCTI). Defining the

offences in the above manner dispenses with the need to formulate a definition of terrorism. The convention also criminalises participation in the above offences and makes the traditional inchoate crimes applicable to them.[268]

In Article 1 'funds' are defined as 'assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit'.

The above definition is extremely broad and is not limited to financial instruments. It could therefore arguably be interpreted to include, for example, weapons or safe houses. How assets are defined has a direct bearing on what may be frozen, as is elaborated on in the section dealing with freezing and forfeiture.

The supply of the funds is criminalised even if they only partially contribute to the commission of the activities criminalised in Article 2 and where the person is acting only indirectly.[269] Due to the fact that Article 2.1 refers to wilful conduct, with the intention or knowledge that the funds are intended to carry out the offences, it is clear that the perpetrator is required to have a subjective guilty knowledge. Corporate entities are also subject to the above criminalisation provisions.[270]

The convention places extensive obligations on the states parties in respect of freezing and confiscating funds, extraterritorial jurisdiction, extradition and MLA. Another significant feature is the placing of extensive measures on financial institutions aimed at detecting the flow of funds through them,[271] including:

- Identifying clients
- Reporting suspicious transactions
- Maintaining financial records
- Supervising money transmission agencies
- Controlling the cross-border transportation of cash and bearer-negotiable instruments

All states parties to the convention are under a legal duty to implement its provisions. The Terrorism Prevention Branch of UNODC assists UN member states

to develop effective counter-terrorism capabilities, including guidance on how to implement the convention.

UN Security Council resolutions are binding on all UN member states. At its 4 385th meeting on 28 September 2001, the UN Security Council adopted Resolution 1373, which directs all states to:

- Prevent and suppress the financing of terrorist acts
- Criminalise the wilful provision of funds with the intention that they be used to carry out terrorist attacks
- Ensure that all persons who participate in the financing, planning, preparation or perpetration of terrorist acts are brought to justice
- Become parties to the relevant international conventions and protocols relating to terrorism, including the International Financing Convention

Although the call is made to criminalise the financing of terrorism, terrorism itself is not defined in the text of the resolution. The requirement, however, to ratify and implement the Financing Convention and other UCTI ensures that, as a bare minimum, the activities proscribed therein must be criminalised by all states.

UN Resolution 1373 (2001) also led to the creation of the CTC in order to bolster the ability of member states to prevent terrorist attacks within their borders and across regions. The CTC is assisted by the CTED, which conducts expert assessments of member states and facilitates counter-terrorism technical assistance to countries.[273] The UN Security Council has on several occasions commented on the work of the CTC and CTED.[274]

In subsequent resolutions the UN Security Council has reiterated member states' obligation to prevent and suppress the financing of terrorist acts. For example, UN Resolution 1963 of 20 December 2010 calls on member states to criminalise the wilful possession or collection (by any direct or indirect means) of funds intended to be used to carry out terrorist attacks. In UN Resolution 2133 of 27 January 2014 the UN Security Council addressed kidnapping and hostage-taking by terrorist groups for the purpose of raising funds. In this regard all member states were called upon to prevent terrorists from benefitting directly or indirectly from ransom payments. The UN Security Council accepted that ransom payments were one of the sources of income supporting the recruitment of terrorists and which enhanced

the operational capacity to carry out terrorist attacks and future kidnappings for ransom. This raises the question as to whether the payment of a ransom demand constitutes terror financing. The broad language of the Financing Convention and Resolution 1373(2001) would not be inconsistent with such an interpretation. The International Convention against the Taking of Hostages (1979 Hostage Convention) is one of the conventions that must be implemented in terms of both the Financing Convention and Resolution 1373 (2001), which requires that states establish hostage-taking as an offence.

Resolution 2133 (2014) also noted the increased use of information and communication technologies (in particular the Internet) for the purpose of financing terrorist activities. To this end, the UN Security Council has confirmed its support for the work of the Financial Action Task Force (FATF) in the field of anti-money-laundering and terrorist financing frameworks.[275]

The UN General Assembly has also adopted a global counter-terrorism strategy,[276] and one of its measures is the combating of terrorist financing.

The Commonwealth, a voluntary association of 53 states (including members of this association), in 2002 adopted a plan of action on terrorism (CPAT) through the Commonwealth Heads of Government. The CPAT focuses on providing member states with legislative frameworks and building capacity among prosecutors and within law enforcement agencies.[277] Terror financing is addressed in these processes.

As alluded to earlier, the UN Security Council has commented on the work of the FATF. The FATF is an inter-governmental body, established by its member states in 1989. Its mandate is to set standards and to promote the 'implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation and other related threats to the integrity of the International Financial System'.[278]

The FATF has issued 40 recommendations on combating money-laundering and nine special recommendations dealing with the financing of terrorism. It has called on all countries to implement measures to bring their national systems into compliance with these recommendations. States cannot avoid compliance with FATF recommendations on the basis that they are not members of the FATF. This

is because the FATF imposes counter-measures on states whose deficient money-laundering and terror financing systems pose a threat to the international financial sector.

The FATF's nine special recommendations on terrorist financing require action to be taken by states in the following areas:

- The implementation of the Financing Convention and the UN Security Council resolutions relating to the financing of terrorist acts, especially Resolution 1373 (2001)
- The criminalisation of the financing of terrorism, terrorist acts and terrorist organisations (these offences must also be defined as predicate offences for money-laundering)
- The freezing and confiscating of terrorist assets
- Reporting of suspicious transactions
- International co-operation through mutual legal assistance and extradition
- Alternative remittance
- Wire transfers
- Non-profit organisations
- Cash couriers

Of fundamental importance is Special Recommendation II, which is not limited to the financing of terrorist acts but also applies to the financing of terrorist organisations. In this regard it goes beyond the ambit of Article 2 of the Financing Convention and Resolution 1373 (2001).

A new role player in the international counter-terrorism organisations is the Global Counterterrorism Forum (GCTF). The GCTF does not issue binding guidance to states, but its work has been commended by the UN Security Council and it has held workshops in conjunction with the UNODC. The GCTF strives to facilitate capacity building within states. Of relevance to terrorist financing, reference is made to the following activities of the GCTF:[279]

- The Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector – Good Practice 15 calls for the criminalisation of terrorist financing in line with the Financing Convention and the FATF Special Recommendations
- The Workshop on Effective Counterterrorism Investigation and Prosecution while Respecting Human Rights and the Rule of Law (Bangkok, November 2013) co-hosted with UNODC – terror financing was emphasised in the preventative criminal offences
- The Algiers Memorandum on Good Practices on Preventing and Denying the Benefits of Kidnapping for Ransom by Terrorists – this memorandum deals extensively with kidnapping for ransom and sets out 15 recommended good practices, one of which involves denying terrorists and terrorist organisations the benefits of ransom

Directly applicable to African states are the counter-terrorism frameworks of the OAU and other regional multilateral bodies. In 1992 the OAU, at its 28th Ordinary Session in Dakar, adopted a Resolution on the Strengthening of Cooperation amongst African States in which it pledged to combat terrorism. At its 30th Ordinary Session in Tunis, the OAU adopted the Declaration on the Conduct of Inter-African Relations, which rejected all forms of terrorism. These initiatives led directly to the 1999 OAU Convention on the Prevention and Combating of Terrorism[280] (OAU Convention).

The OAU Convention contains several provisions that relate directly to terrorist financing:

- The definition of a terrorist act includes any sponsoring of or contribution to the commission of the act.[281]
- States parties are required to criminalise the offences referred to as terrorist acts in the convention.[282]
- States parties are further required to refrain from 'any acts aimed at organising, supporting, financing, committing or inciting to commit terrorist acts'.[283]
- States parties are obligated to strengthen exchanges of information relating to sources of funding for terrorist acts or groups.[284]

- States parties are further obligated to ratify the international agreements listed in the annexure.[285]

(The annexure listed the same conventions as were listed in the Financing Convention, and added the Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction of 1997.) These conventions are therefore binding upon all OAU member states. The Financing Convention was not listed, as the OAU Convention preceded it.

In July 2004 in Addis Ababa, the OAU adopted a Protocol[286] to the OAU Convention, which inter alia made provision for the organisation to provide technical assistance to member states on matters relating to the combating of financing of terrorism.

The work of the FATF on the African continent is reinforced by two FATF-style regional bodies, namely the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA). The GIABA was established by ECOWAS and has 15 members. The ESAAMLG has 14 members and was admitted as an associate member of the FATF in June 2010. The 2012/2015 Strategic Plan of the ESAAMLG commits it to a number of initiatives aimed at strengthening members' implementation of counter-terror financing measures.[287] The GIABA Strategic Plan for 2011/2014 commits the organisation to ensuring the adoption of standards for the financing of terrorism in accordance with the FATF Recommendations.[288]

On 1 May 2014, the heads of state of the East Africa Community (EAC) directed that its Regional Council of Ministers implement a regional counter-terrorism strategy to stabilise the region.[289] ECOWAS has as part of its peace and security sector developed counter-terrorism programmes and collaborates with the UN system and other international partners on border security measures. In February 2013, ECOWAS adopted a Political Declaration on a Common Position against Terrorism, which included a terrorism strategy and implementation plan. In terms of the declaration, all member states are required to condemn 'terrorism and related offences such as incitement to and financing of terrorism'.[290]

The Southern African Regional Police Chiefs Cooperation Organisation (SARPCCO) has adopted a Draft Model Law on Counter-Terrorism, which addresses the issue of terror financing.[291]

All the international bodies referred to above have drawn attention to the connection between terrorism, organised crime and money-laundering, the significance of which will be dealt with in the following section.

Chapter 3

Criminalisation

The ultimate objective of a counter-terrorist financing regime is to prevent the flow of funds and other material support to terrorists and thereby prevent terrorist attacks and disrupt the functioning of terrorist organisations. The criminalisation of terrorist financing seeks to punish those who supply such funds or material support.

The issue of how terrorism is defined becomes of critical importance at this juncture. As is evident from the preceding section, states are under an obligation to criminalise specific identified conduct and the financing thereof. In the light of FATF Special Recommendation 2, consideration must also be given to the financing of terrorist organisations.

Several of the multilateral organisations referred to above have drafted model laws to assist states in enacting domestic legislation or have issued guidance. A primary concern is how terrorist activities may be distinguished from ordinary criminal acts. Jurists would, for example, find it difficult to classify as terrorism theft of cables by a thief for self-enrichment, even if a disruption of an essential service resulted.

The African Model Anti-Terrorism Law, adopted by the OAU at its 17th Session at Malabo in 2011,[292] defines as a terrorist act any offence referred to in the UN and AU Counter-Terrorism Instruments, committed with a political, religious or ideological cause.

The effect of introducing a political or other motive is that the activities required to be criminalised in terms of the relevant international instruments would not be regarded as terrorism if such a motive were lacking, even if all the elements defined in the international instruments were present. Potentially such criminalisation would constitute non-compliance with international obligations.

In order to overcome this obstacle, the laws referred to above then have as a separate category of offences the activities proscribed in the international instruments. These offences are described as ‘convention offences’, which do not

require a political or other motive. The terrorist financing provisions apply to both the terrorism and convention offences.

An alternative approach is found in the Model Provisions on Money Laundering, Terrorist Financing, Preventive Measures and Proceeds of Crime jointly issued by the UNODC, the Commonwealth and the International Monetary Fund (IMF), which defines as a terrorist act any offence committed in terms of certain of the UCTI[293] or any other act intended to cause death or serious bodily injury to any person not taking an active part in hostilities in a situation of armed conflict for the purpose of intimidating a population, government or international organisation.[294] The terrorist financing provision then applies to the commission of terrorist acts or to the funding of terrorist organisations and their members.

The question arises as to whether a *lex specialis* is necessary to criminalise the financing of terrorism and/or convention offences. Certain states apply a doctrine of common purpose, which makes any person who in any way contributes to the commission of the crime with the knowledge that his/her act will further the offence, guilty of that offence. Such a doctrine would dispense with the need for a *lex specialis* for the financing of such crimes, since the financing was an integral part of the commission of the crime itself. This doctrine would, however, not constitute compliance with FATF Special Recommendation 2, which requires criminalisation of the provision and collection of funds for terrorist organisations and members thereof regardless of the intended use. Consequently the legislation referred to above makes provision for stand-alone terrorist financing offences in addition to defining terrorism so as to include accomplice participation and inchoate activities.

To this end, the UNODC/Commonwealth/IMF law defines the terrorist financing offence in the following terms:

> '(2) Any person who by any means, directly or indirectly, [wilfully] provides or collects funds, or attempts to do so, with the intention that they should be used or in the knowledge that they are to be used in whole or in part:
>
> (a) in order to carry out a terrorist act; or
>
> (b) by a terrorist to facilitate that person's activities related to terrorist acts or membership in a terrorist organization; or
>
> (c) by a terrorist organisation
>
> commits an offence.'

Other sections make the offence applicable to accomplices and do not require the commission of the terrorist offences as a prerequisite for the offence.

The issue of what constitutes a terrorist organisation raises essentially the same debate as what constitutes an act of terrorism. The UNODC/Commonwealth/IMF model law gives a specific definition of terrorist organisation, consistent with its definition of terrorist acts. Terrorist organisations may range from large, well-organised, paramilitary structures to small, isolated groups of extremists. A proper criminalisation would have to cover the whole range of organisations.

As a consequence of UN Security Council Resolution 1267, the UN Security Council established a committee to impose sanctions on persons listed by it as being members of either al-Qaeda or the Taliban or persons or entities associated with such organisations. In terms of the sanctions, the designated individuals, entities or organisations are subject to an asset freeze, travel ban and arms embargo. In terms of the asset freeze, states are required to freeze without delay 'the funds and other financial assets or economic resource derived from property owned or controlled directly or indirectly'.[295] In South Africa, for example, the president publishes the list of designated entities by the UN Security Council in a domestic proclamation so as to give effect to the UN Security Council listings. South African law makes its terrorist financing provision also applicable to the supply of funds to entities on the al-Qaeda/Taliban list. Recently the UN Security Council has adopted a policy of issuing separate resolutions in respect of the Taliban and al-Qaeda.[296]

Certain states, for example the US, have also adopted a listing process for persons identified as either terrorists or for terrorist organisations not falling within the ambit of the 1267 regime and imposing targeted financial sanctions on them. There is considerable controversy as to whether other states should give effect to such listings.

The Financing Convention requires that guilty subjective knowledge be criminalised, which is consistent with the UNODC/Commonwealth/IMF model law. In contrast, and as an example, South African terror financing laws makes reference to imputed knowledge, which is determined on an objective standard, based on reasonableness that is then imputed to the accused irrespective of whether he/she in fact had such knowledge.

Recommendation 29 of the FATF's Recommendations Relating to Money Laundering requires that states establish FIUs for the receipt and analysis of

suspicious transaction reports and other information relating to money-laundering and terrorist financing, supplied by reporting entities. This is in line with the provisions of the Financing Convention and other international instruments requiring financial institutions to apply due diligence to the execution of transactions in order to ensure that such transactions are not facilitating the commission of crimes. Financial institutions are required to report any such suspicious activity to the designated FIU, which in turn must transmit such information to the relevant law enforcement agencies for investigation. In order for this reporting regime to be effective, criminal sanctions should be applied to financial institutions that fail to comply with their reporting obligations. It is for this reason that, for example, in the OAU and UNODC/Commonwealth model laws, provisions are made for the establishment of an FIU and for offences relating to the reporting of transactions. Through the Egmont Group, international sharing of information is possible between national FIUs.

In South Africa, for example, the objective knowledge standard would enable the successful prosecution not only of individuals who were careless in supplying and making funds available but also of financial institutions that failed to detect that transactions flowing through their institutions were in fact linked to terrorist financing. Although the test of reasonableness is objective, it is nevertheless determined with reference to the circumstances of the specific accused, e.g. a different test would apply to a lay person as opposed to a financial institution. In *R v Khawaja*,[297] the Supreme Court of Canada defined the reasonable test in the following terms:

> 'The determination of whether a reasonable person would view conduct as capable of materially enhancing the abilities of a terrorist group to facilitate or carry out a terrorist activity hinges on the nature of the conduct and the relevant circumstances.'

A thought-provoking publication dealing with the monitoring of financial transactions in order to combat terrorist financing is the thesis by Albert L Kao entitled *Increased anti-money laundering banking regulations and terrorism prosecutions*,[298] in which the author analysed the prosecutions for terrorism in the US after the implementation of banking regulations in line with the FATF standards. This was to establish whether the regulations resulted in terrorist financing being detected or supported other charges. The author's conclusion was that the

regulations had limited effects on countering terrorist financing. This conclusion was informed by the fact that the terrorist-financing regulations were based on anti-money-laundering banking regulations, which failed to take into account the distinction between the objectives of criminal organisations and terrorists. In the case of criminal organisations, the focus is on the concealment of large sums of money for profit. In the case of terrorists, the objective is to use violence to further political or ideological objectives. The author's conclusions do have some merit. Booking a room for a night in a guesthouse for the purpose of a planning meeting or purchasing cheap electrical switches from a hardware shop in order to assemble an explosive would not be captured in the suspicious reporting regimes. Similarly, a businessman sympathetic to a terrorist cause and using his legitimate business assets would pass the customer verification requirements with flying colours. Finally, many of the financial counter-measures are dependent on the use of formal financial structures and, as the typologies in the following section illustrate, terrorists often make use of informal and unregulated financial mechanisms.

It is for each APA state to determine how it criminalises terrorist financing, provided that, as a minimum, the international obligations referred to above are met.

As indicated, all the international bodies referred to emphasise the close links between terrorism, organised crime and money-laundering. In fact, the UNODC/Commonwealth/IMF model law criminalises both money-laundering and terror financing under one law. It is important, however, to note two important distinctions between terror financing and money-laundering. Firstly, money-laundering is universally regarded as being the concealment of proceeds of criminal offences. It therefore only comes into play once an offence has been committed and the proceeds thereof are either concealed, managed or retained/received. By contrast, terrorist financing comes into play as soon as funds are channelled to terrorist organisations for the purpose of carrying out future terrorist attacks. Terrorist financing may therefore be committed before the commission of certain terrorist offences. Secondly, terrorist financing may have a perfectly legitimate origin, e.g. a wealthy business person might decide to donate a portion of his/her legitimate income to terrorists. In practice, however, the offences could be intertwined. For example, certain terrorist acts generate income (e.g. a ransom demand) that constitutes the proceeds of crime, hence triggering money-laundering offences. The proceeds of crime could then be used to finance further terrorist acts, thereby constituting the offence of terrorist financing. It may well be that a terrorist financing investigation could originate from a money-laundering investigation before the link to terrorism is established.

Chapter 4

Factors conducive to successful prosecutions

A terrorist financing law that is fully compliant with international obligations is not on its own sufficient to guarantee successful prosecutions. Prosecutions for terrorist financing may be either reactive or proactive. In the case of the former, the evidence of the financing is only detected after the attack has taken place and such a charge would be added to the main charge of terrorism. In the case of the latter, the actual attack could be prevented. Obviously the focus of an effective terrorist financing prosecution should be on prevention.

All the international instruments imposing an obligation to criminalise terrorist financing also require that the funds in question be frozen and confiscated. An efficient asset forfeiture regime is therefore also a critical requirement.

With the advent of electronic technology, funds can be moved throughout the world simply by accessing the Internet or utilising electronic money transfer systems. All the international instruments referred to above require the terrorist financing provisions to be of extraterritorial effect under certain circumstances and to give effect to the *aut dedere aut judicare* principle. In order to cover the field of activities sought to be prosecuted in a specific jurisdiction, the state intending to exercise jurisdiction should have extensive extraterritorial laws. Linked thereto is an obligation to have effective MLA and extradition regimes supported by informal co-operation and liaison.

Due to the use of electronic technology in the transfer of funds, effective laws relating to the gathering and admissibility of electronic evidence are also essential.

It is also prudent that there be proper legal mechanisms for obtaining financial information from financial institutions and other entities, including being able to access foreign financial evidence.

The terrorist financing law should also be supported by a solid body of other criminal offences. Of particular importance are offences relating to money-laundering, organised crime, movement control and the regulation of financial transactions, including cross-border ones.

Finally, intelligence and undercover operations can play a crucial role in detecting financing at an early stage and preventing terrorist attacks and recruitment from taking place. In the following section examples of successful sting operations can be found in certain of the typology reports.

Chapter 5

Case studies and typologies

This section simply seeks to illustrate the various forms in which terrorist financing has manifested itself in practice.[299] A number of extremely informative typology reports are set out first and with specific case law thereafter.

In February 2008, the FATF published a report entitled *Terrorist Financing*.[300] This report dealt comprehensively with all aspects relevant to the topic and is invaluable to any prosecutor wishing to familiarise him/herself with terrorist financing. The report draws a distinction between the funding of specific terrorist attacks and the broader costs of establishing and maintaining a terrorist organisation. In this regard, the conclusion was that the former costs were infinitely cheaper than the latter ones. The report recorded that the Embassy bombings in Kenya and Tanzania cost US$50 000, whereas the Madrid train bombings only cost US$10 000. The report further identified the following sources of funds for terrorists:

- Charities
- Mass media outlets
- Diversion from legitimate charities
- Sham charities
- Legitimate business
- Self-funding raising of funds from criminal proceeds[301]
- Safe havens, failed states and state sponsors

These conclusions were supported by reference to various case studies reported to the FATF. An extremely interesting case study was one provided by the UK, where Internet websites promoting terrorism were funded with funds stolen from hacked credit card accounts and money-laundering through online gambling sites.

In another case reported by the UK, a terrorist logged on to illegal Internet sites that bought and sold credit card information and passed stolen credit card information to a computer expert, who created various websites used for terrorist purposes.

The report also illustrated the modus operandi of moving terrorist funds, and identified the following mechanisms, among others:

- Formal financial sector
- Cash couriers
- Alternative remittance systems
- Charities and non-profit organisations

The aforementioned conclusions were supported by case studies provided to the FATF. It is interesting to note that in almost all of the case studies the evidence pointed to the financing spreading over several different countries, making it extremely difficult to link the origin of the funds to the ultimate terrorist recipient.

In October 2013, the FATF and GIABA published a joint report entitled *Terrorist financing in West Africa*,[302] which provided examples of terrorist financing through the following mechanisms:

- Trade and other profit-generating activities
- non-governmental organisations and charitable organisations
- Smuggling of arms and currencies by couriers
- Drug trafficking

The report highlighted the terrorist financing techniques of the Nigerian terrorist organisation Boko Haram. An interesting case study was the one involving a Boko Haram member who also owned a telecommunications company. Not only did he use a portion of his profits to support Boko Haram, but he also supplied SIM cards and cell phones to members of the organisation. This demonstrates the fact that terrorist financing funds may often have a legitimate origin. The report also established that much of the terrorist financing activities took place outside Nigeria. The most recent investigations into the terror financing *modi operandi* used by Boko Haram revealed that the group largely used the services of human couriers.

In 2013 the GIABA also published a report, entitled *The nexus between small arms and light weapons and money laundering and terrorist financing in West Africa*.[303]

The report reached the conclusion that 'the financing of terrorism through the supply of illicit small arms was naturally interlocked'. It also provided information on the broader raising of terrorist funds in the region. In the Niger Delta funding came primarily from oil bunkering.[304] In Côte d'Ivoire funds were raised from arms smuggling, kidnapping ransoms, cigarette smuggling and illicit narcotics. The report also acknowledged information supplied by the UNODC to the effect that al-Qaeda had forged 'mutually beneficial links with West African crime networks particularly in Nigeria'. In this regard, use was made of document forgery, human trafficking and illicit trade in weapons, diamonds and drugs. Al-Qaeda was also implicated in illicit diamond trade in Sierra Leone and Liberia.

In October 2003, the FATF published a report entitled *The role of* Hawala *and other similar service providers in money laundering and terrorist financing*.[305] *Hawala* is generally regarded as a means of remitting money bypassing the formal financial institutions. Obviously this raises terrorist financing concerns, because many of the financial counter-measures are only triggered by accessing the formal financial sectors. *Hawala* schemes are extremely prevalent in APA states. The report identified the following factors as making Hawala schemes vulnerable to terrorist financing:

- Lack of regulatory supervision
- Movement of cash across multiple jurisdictions outside of banking systems
- Use of businesses that are not regulated financial institutions
- Mingling of legal and illegal proceeds in the same transaction

The report's findings were based on various case studies. One of the most interesting cases was that relating to a Pakistani national residing in the US. In a sting operation his money remitter business was used to transfer substantial amounts of money to Canada, England, Spain, Pakistan, Japan and Australia. In another case a person was convicted in a US federal court for operating an unlicensed money business between the US and Pakistan. One of the money transfers was used to fund an attempted car bombing in New York's Time Square.

In 2010, the UNODC published the *Digest of terrorist cases*.[306] In a chapter entitled 'Financing and other forms of support to terrorism', information was provided as to how a number of prominent terrorist attacks were funded, which included the following:

- The bombing of the London transport system in July 2005 apparently cost less than £8 000. The attack was self-funded by the leader of the terrorist group, using funds from overdrawn bank accounts, credit cards and a personal loan.
- The infamous 11 September 2001 attack apparently cost al-Qaeda US$500 000, which was directly financed. Use was made of money transfer techniques as well as cash and travellers' cheques. Financing activities in preparation for the attack took place in the US, Pakistan, Germany, Afghanistan, the United Arab Emirates (UAE) and Saudi Arabia. Major cash withdrawals were made from ATMs in the US, drawn from a UAE bank account.
- In the case of the Madrid train bombings, the explosives were obtained from a mining operation in exchange for quantities of narcotics. Vehicles used to execute the attack were either purchased with cash or stolen. An official investigation by the Spanish government after the bombings concluded that the financial counter-measures prescribed by the FATF would not have detected any of the financing activities.

Turning to case law, samples of a few very relevant decisions have been selected from the UK, Australia, Canada and the US.

In the matter of the appeal between The Crown Prosecution Service and IK, AB, and KA, the accused were charged with conspiring to provide property, which included money, false identification and travel documents, that was to be used for the purpose of terrorism. The accused were at the time members of the Libyan Islamic Fighting Group, a 1267 listed entity. The accused had successfully raised the defence of double jeopardy, because of previous proceedings relating to forgery. The Appeal Court, however, refused to uphold the ruling on double jeopardy, because it was of the view that the forgery offences were not substantially the same as the evidence supporting the terrorist offences. The Appeal Court also commented on the terrorist offences in the following terms:

> These are grave offences. It is in the public interest that they be tried unless there are compelling reasons to the contrary. … The delay between arrest, charge and trial has not been exceptional and has not been the

fault of the prosecuting or investigating authorities. By their very nature international terrorist offences are complex and take longer to investigate than most domestic offences. The authorities are dependent to a considerable extent on foreign agencies who will have their own priorities.

The aforementioned case is extremely significant, because, as previously indicated, evidence establishing terrorist financing may only be established from the investigation of other terror-related charges.

The Commonwealth Director of Public Prosecutions in Australia has conducted a number of prosecutions relating to terrorist financing.[307] These include the following:

- In the case of Vinayagamoorthy, Yathavan and Rajeevan, the accused were convicted of making assets available to the Liberation Tigers of Tamil Eelam and were sentenced to suspended sentences of imprisonment ranging from 12 to 24 months.
- Operation Pendennis related to the arrest of a number of persons who were members of a local, unnamed terrorist organisation that sought to commit a terrorist act. One of the objectives of the group was to commit an act of terrorism in Australia to force the government to withdraw its troops from Iraq and Afghanistan. The prosecution relied extensively on intercepted conversations between the accused. Certain of the members of the group were convicted of intentionally providing resources to a terrorist organisation, whereas others were found guilty of attempting to intentionally making funds available to it.
- In the case of Joseph Terrance Thomas, the accused was charged with having intentionally received funds from a terrorist organisation, intentionally providing resources to a terrorist organisation to assist in the preparing of terrorist attacks, both in Australia and abroad, and being in possession of a falsified passport. He was convicted on the receiving of funds and false passport offences, but acquitted on the charges of providing resources to a terrorist organisation. On appeal, however, his convictions were set aside on the basis that the confessions he had made in Pakistan were not voluntary. A retrial was directed, resulting in his conviction on the falsified passport offence, in respect of which he was sentenced to nine months' imprisonment.

The Canadian case of *R v Khawaja*[308] dealt with an accused who had become obsessed with Osama bin Laden and his cause and had communicated with an American who had supplied material support to al-Qaeda, as well as with the leader of a terrorist cell in the UK. The accused, inter alia, offered them support, provided funds, designed a remote arming device and recruited a woman to facilitate transfers of money. The trial court convicted the accused of certain offences that would fall within the ambit of terrorist financing. Canadian law also required proof of a political, religious or ideological purpose, objective or cause. The trial judge ruled that this motive clause was unconstitutional. The reasons advanced were extremely compelling and prosecutors and APA states that have such a provision should take cognisance thereof. In this regard, the court in *Khawaja* concluded as follows:

> 'The average person would be hard pressed, I daresay, to recount much about the motives of the perpetrators of some if not all of these notorious crimes. Just what political, religious or ideological objectives or causes the perpetrators felt they were supporting with their actions is largely lost on the populations affected. And for good reason. It really doesn't matter. Such terrorist acts cannot be appreciated by the imputation of rational principles to the perpetrators anyway. And are the acts any less terrorizing, intimidating or insidious for our failure to fathom and spotlight the inspiration of the perpetrators? I can see no compelling benefit or justification for the political, religious or ideological provision that can be waived against its freedom infringing impact. The provision is in my view inconsistent with the Charter and is therefore constitutionally invalid.

On appeal the accused tried to argue that the motive clause constituted a violation of the charter (Canadian Constitution) because of its inroad into the freedom of beliefs and opinions.

> The Appeal Court rejected this argument, because it found that the activities targeted by the terrorism laws related to conduct involving acts or threats of violence. Such acts were excluded from constitutional protection, which only recognised non-violent expression of political, religious or ideological views. The Appeal Court therefore did not accept the trial court's finding of unconstitutionality.

In the matter of The United States of *America v Mousa Mohammed Abu MARZOOK and Others*:[309]

The defendant was charged with providing material support in the form of currency and personnel to Hamas, which had been designated by the Secretary of State as a foreign terrorist organisation. The first issue of importance is that the definition of material support or resources was not limited to currency or money instruments, but also included 'financial securities, financial services, lodging, training, expert advice or assistance, safe houses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials'. This broad definition is in line with several of the model and state laws I have referred to previously. The accused had raised several legal challenges to his indictment, inter alia alleging that the above definition:

- Was overbroad
- Was vague
- Violated the right to freedom of association
- Required a special intent that applied to all the elements of the offence

The accused had placed major reliance on the fact that 'Hamas was a multi-dimensional organisation that, in addition to its unlawful aims, provided humanitarian and social services to Palestinians in the Gaza Strip and West Bank'. His challenge was, however, rejected and the judgement highlighted the following:

- The government's interest in preventing terrorism is not only important but is paramount
- The government has a substantial interest in curbing the spread of terrorism
- Foreign organisations that engaged in terrorist activities are so tainted by their criminal conduct that any contribution to such an organisation facilitates that conduct
- Terrorist organisations use funds for illegal activities regardless of the intent of the donor and consequently liability must be attached to all donations to foreign terrorist organisations

- Support given to a terrorist organisation can be used to promote the organisation's unlawful activities, regardless of donor intent. Once the support is given, the donor has no control over how it is used

The Court specifically failed to attach any weight to any humanitarian or lawful activities undertaken by Hamas by accepting the following:

> [A]ll material support given to [foreign terrorist] organisations aids their unlawful goals. Indeed, … terrorist organizations do not maintain open books. Therefore, when someone makes a donation to them, there is no way to tell how the donation is used. Further, … even contributions earmarked for peaceful purposes can be used to give aid to the families of those killed while carrying out terrorist acts, thus making the decision to engage in terrorism more attractive. More fundamentally, money is fungible; giving support intended to aid an organisation's peaceful activities frees up resources that can be used for terrorist acts.

The court rejected the argument relating to vagueness on the basis that the indictment had alleged specific conduct performed by the accused, constituting material support. Insofar as the argument relating to the specific intent was concerned, the court concluded that although the offence required knowledge on the part of the accused (that he knew that the recipient was a foreign terrorist organisation or was engaged in terrorist activities), it was not necessary to prove further that the donor specifically intended to further the organisation's terrorist activities.

This judgement is significant because states are under an obligation to criminalise funding not only for the purpose of carrying out terrorist attacks but also for terrorist organisations and members thereof.

In the matter of *The United States of America v Mohamad Youssef Hammoud and Others*:[310]

> The accused was convicted of various offences, all connected to his support for Hezbollah, a designated foreign terrorist organisation. The accused and members of his family had become members of a cigarette smuggling operation, involving the smuggling of cigarettes from North Carolina to Michigan

and selling them without paying taxes. The value of the cigarettes was US$7,5 million and the State of Michigan was deprived of US$3 million in tax revenues. The accused attended prayer services where the attendees were urged to donate money to Hezbollah. The accused then proceeded to make such donations. Although the majority of the court confirmed the conviction and sentence, a dissenting judgement ordered a retrial, because it found that the trial court had failed to instruct the jury on the specific intention required to sustain a conviction for material support.

Although certain international instruments only require subjective guilty knowledge, certain state laws impute objective standards of reasonableness to an accused irrespective of his/her subjective knowledge. This case illustrates how important it is to define the knowledge requirement for terrorist financing.

Part 7

Asset forfeiture or recovery in terror financing

Adv. Chris Ndzengu
National Prosecuting Authority of the Republic of South Africa

Index

Chapter 1

Introduction

The Preamble of the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of Proceeds from Crime[311] acknowledged that serious crime had become an increasingly international problem and that modern and effective methods should be used on an international scale to combat serious crime. It recognised the deprivation of criminals' proceeds of crime[312] as one of those effective methods.[313]

This convention was updated and expanded to include measures to prevent financing of terrorism and was subsequently replaced by the 2005 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of Proceeds from Crime and on the Financing of Terrorism.[314] This new convention illustrates a very significant step against combating terrorism, by attacking its financing on a broad front and ensuring that logistical terror cells cannot find financial safe havens anywhere in Europe.

The main concern that preceded the adoption of the UN International Convention for the Suppression of Financing of Terrorism[315] was the global escalation of acts of terrorism in all its forms and manifestations. This convention obligates states parties to, inter alia:

- Criminalise specific acts domestically
- Establish jurisdiction over such offences
- Prosecute or extradite persons alleged to have committed the offence of terrorism
- Engage in co-operation and mutual legal assistance with regard to its objectives

Article 2 criminalises the act of providing or collecting funds with the intention or knowledge that these funds will be used to carry out a terrorist attack. Article 8 requires member states to adopt the measures necessary for the identification, freezing, seizure and confiscation of targeted funds, which can then be used to compensate the victims of offences and their families.

The speed with which this convention was ratified by member states illustrates the heightened commitment of the international community to combat terrorism, especially in the aftermath of the events of 11 September 2001. Increasingly, international terrorist activities have become interlinked with other modern scourges such as drug trafficking, the proliferation of small arms and kidnapping for ransom. This convention recognises that financing is at the heart of terrorist activity, in all its forms, and paves the way for concerted action and close co-operation among law enforcement agencies, financial authorities and states to combat this.

UN Security Council Resolution 1368 (2001)[316] called on the international community to redouble its efforts to prevent and suppress terrorist acts by increased co-operation and implementing fully the relevant international anti-terrorist conventions and resolutions.

Two of the FATF's Counterterrorist Financing Recommendations are particularly relevant because they address countries' sanctions obligations. Firstly, the FATF recommends that countries criminalise the financing of terrorism, terrorist acts and terrorist organisations. The purpose of this recommendation is to ensure countries have the legal capacity to prosecute and apply criminal sanctions to people who finance terrorism. Secondly, it recommends that each country should implement measures to freeze without delay funds or other assets of terrorists in accordance with the UN resolutions. Each country should also adopt and implement measures, including legislative ones, that would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations.

Chapter 2

The AU Convention

The plan of action in respect of the AU Convention echoes a need for African states to act jointly, share information on the activities and movement of terrorist groups, and exchange expertise and resources. Member states are required to amend national legislation, aligning it with the AU Convention. Member states undertook to operationalise the Financing Convention by taking all measures to detect, identify and freeze or seize any funds used or allocated for the purpose of committing terrorism. States without legal frameworks in this regard are expected to introduce legislation and criminalise terror finance domestically. This undertaking extends to the confiscation of movable and immovable property intended for the financing of terrorism acts or that may give shelter to terrorism groups and elements, and access to their support networks.

States ought to be persuaded to escalate their counter-terrorist responses to an approach that is based in the ordinary police and criminal justice system, i.e. a rule of law and rights-based approach. This is important for co-operation. Implementation of such approaches should be as uniform and widespread as possible. Terrorism and its financing require ongoing review of the validity of the strategies states put into place.

Terror financing comes from states or organisations and wealth-generating activities. This funding has both legitimate (e.g. fundraising for the diaspora, community or charitable donations) and illegitimate or illegal sources (e.g. drug trafficking, racketeering, money-laundering, human trafficking, abduction with ransom demands, trafficking in precious stones and arms trafficking). Terrorists mix these funds and use them in small amounts at different times. Mechanisms to combat the financing of terror have to be both preventative and reactive. In addition to criminalising the financing of terror, each state is expected to seize and forfeit to the state such funds and instruments used or intended to be used to finance it.

Chapter 3

Asset recovery or forfeiture

Asset forfeiture or recovery of assets is based on the rationale that no person should benefit from wrongdoing, which accords with the common law principles of:

- Unjustified enrichment at the expense of others
- No person should benefit from actions that are regarded as reprehensible

Asset recovery or forfeiture manifests itself in the following two ways:

- **Criminal forfeiture,** which is the recovery of proceeds of unlawful activities and is invoked when a suspect is to be charged or has been charged or prosecuted, and there are reasonable grounds to believe that a conviction may follow and that a confiscation order may be made. It is thus conviction-based forfeiture. It is not really different from the UK asset forfeiture law.
- **Civil forfeiture,** which is the recovery of proceeds of unlawful activities and removal from public circulation of instruments or assets used in the commission of crime where the guilt of the wrongdoer is not relevant. It is also known as non-conviction-based forfeiture. Most countries file asset forfeiture applications such as restraints, confiscations, realisation, preservations and forfeiture in the high court.

South Africa, for example, has both types of forfeitures.[317] These provisions are ordinarily implemented by the Asset Forfeiture Unit within the NPA.

Ordinarily, a definition of property should include:[318]

- Real or personal property of any description
- Tangible or intangible
- An interest in any real or personal property
- Funds, cash, assets
- Any other property, however acquired
- Any type of financial resource, including cash or the currency of any state, bank, financial institution, credits, traveller's cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit or any other negotiable instrument in any form, including in electronic or digital form

Chapter 4

Case studies and typologies

In *NDPP v Elran*,[319] the Constitutional Court, in reference to South Africa's domestic laws introduced to combat organised crime and the removal of the fruits of crime and property used to commit crime, commented as follows:

> 'We should embrace POCA as a friend to democracy, the rule of law and constitutionalism – and as indispensable in a world where the institutions of State are fragile, and the instruments of law sometimes struggle for their very survival against criminals who subvert them.'

In *NDPP v Cook*,[320] the court held that the key purposes of forfeiture orders were to:

- Remove the incentives to commit crime
- Deter persons from using or allowing property to be used in crime
- Eliminate or incapacitate some of the means by which crime is committed
- Advance the ends of justice by depriving those involved in the crime of the property concerned

In *Shaik*, the Court held that the primary purpose of confiscation orders is:

- Not to punish offenders but to ensure that they do not enjoy the fruits of their crimes
- To deter criminals from committing crimes
- To prevent criminals from committing crimes in the future, as they would not have the financial means to do so

In the matter of *Joseph Cicippio and Edward A Tracy*:[321]

> Joseph Cicippio was abducted in September 1986 and held for five years by militants from Hezbollah, the Lebanese paramilitary and political group sponsored by Iran, while Edward A Tracy was abducted in October 1986. Tracy and Cicippio, both Americans, were held hostage in Beirut in the 1980s. Both men were released in 1991, having been chained, beaten and threatened with death or maiming. They used Canadian courts to go after millions of dollars in Iranian government assets. In a historic ruling, an Ontario court ordered the seizure of more than US$7 million worth of bank accounts and property belonging to Iran, and the return of the assets to victims of militant groups that it bankrolled. The court further ordered the liquidation of two of Iran's Canadian bank accounts and a pair of properties, one in Ottawa and one in Toronto. This legal victory was made possible by the Canadian Parliament's 2012 passing of the Justice for Victims of Terrorism Act, which scrapped state immunity from civil lawsuits for countries deemed to be supporting terrorism.
>
> As a result of the Court's ruling, the Cicippio and Tracy families will receive a share of a Scotiabank account containing US$1,65 million and a Royal Bank account with €330 000 (US$511 220). Both were held in the name of the Iranian Embassy in Ottawa, which was forced to close after the Canadian government suspended diplomatic relations and expelled Iran's envoys. The judgement also seized offices in Toronto, valued at US$1,1 million for tax purposes, and in Ottawa, assessed at US$3,9 million. Both sites operated as ostensible Iranian cultural centers.

In the following three Canadian cases[322] the Iranian government was pursued for damages due to militant groups it supported:

- Alann Steen and the family of David Jacobsen: Steen was abducted in Beirut in 1987 and held for nearly five years, while Jacobsen was kidnapped in 1985 and released 17 months later. The plaintiffs won US$343 million and US$6,4 million respectively in US courts but could not collect.
- Sherri Wise, a Vancouver dentist, was injured in 1997 during a Hamas suicide bombing in Jerusalem. She launched a lawsuit in British Columbia in September 2013, the first case originating under Canada's new Justice for Victims of Terrorism Act.

- The family of Marla Bennett, a graduate student from California who was killed in a 2002 bombing by Hamas at Hebrew University in Jerusalem. Her relatives won a US$12,9 million judgment but could not get at any Iranian assets in the US.

Part 8

Cyberterrorism and the use of electronic evidence in prosecutions

Jason Jordaan
Consultant for the ISS, Republic of South Africa

Index

Aim and objective

The use of emails, the Internet, computers, laptops/notepads, tablets and mobile phone devices, etc. has far-reaching ramifications. The electronic footprints of persons using mobile phones can be traced from service providers globally. In the same manner, one can trace Internet protocol (IP) addresses and the use of the Internet, computers, laptops/notepads, tablets and other devices globally. These devices are used not only to communicate but also to commit transnational organised crimes associated with terrorism.

The aim and objective of this section is to provide a brief understanding of cyberterrorism and the value of electronic evidence.

Chapter 1

Introduction

The world has changed significantly in the last few decades, as technology and information systems have become part of the daily fabric of human existence around the globe. Africa as a continent is in many ways playing catch-up with the rest of the developed world in this regard, but in other areas we have become early adopters of technologies, ahead of the rest of the world. This mix of lagging behind in some areas while being at the cutting edge in others in relation to technology and information systems, has created a uniquely African digital environment in which we go about our daily lives while increasingly being connected to the global world.

This connected world of pervasive technology has brought with it significant improvements to the lives of many. Computers have improved our ability to perform various functions and have become part of our daily lives. The Internet allows us to connect to each other and access information on a global scale in a manner that was impossible only a few years ago. Cellular communications and smart phones have literally placed the world in our hands.

However, as much as ordinary people gain from the interconnected world that has been created by this technological renaissance, so have those with malicious motives and mindsets. As the Internet becomes more pervasive in all areas of human endeavour, individuals or groups can use the anonymity afforded by cyberspace to threaten citizens, specific groups, communities and entire countries without the threat of capture, injury or death to the attacker that being physically present would bring.

Terrorist groups make use of computers, the Internet and mobile phone networks to make their activities easier, and of even greater concern is the fact that this interconnected world makes terrorist attacks facilitated via the Internet a real possibility. For terrorists, cyber-based attacks have distinct advantages over physical

attacks. They can be conducted remotely, anonymously and relatively cheaply, and they do not require significant investment in weapons, explosives and personnel. At the same time the effects can be widespread and profound.

Prosecutors play a vital role in addressing cyberterrorism by preparing and presenting cases against the perpetrators. To do so, however, prosecutors must be familiar with the concepts of cyberterrorism and how the Internet and other communications technologies are used to facilitate terrorist activities.

Any case involving cyberterrorism or the use of the Internet to facilitate terrorism will involve digital evidence (as will just about any other type of crime these days). To effectively utilise digital evidence as a form of evidence in court, prosecutors need to be familiar with the concept of digital evidence, where it can be found, and how it should be handled and processed by investigators and forensic specialists to ensure its admissibility and reliability in court.

Chapter 2

The challenges of prosecuting cyberterrorism

In the matter of *H, WS v W,N*,[323] a South African court held that:

> It is the duty of the courts to harmoniously develop the common law in conformity with enshrined constitutional principles. 'The pace of the march of technological progress has quickened to the extent that the social changes that result therefrom require high levels of skill not only from the courts, which must respond appropriately, but also from the lawyers who prepare cases … for adjudication.'

The above passage could not apply more to prosecutors.

In this regard, there are a number of practical challenges that a prosecutor needs to take into consideration when dealing with cyberterrorism. Perhaps the biggest two are locating and securing the evidence, and the capacity of law enforcement to conduct the investigations.

The nature of cyberterrorism is such that the persons launching cyberattacks or otherwise facilitating the activities of terrorist groups do not have to reside in the countries that they are attacking or where they are facilitating terrorist activities. When using the Internet an attacker could be on the other side of the globe. Whether it is the attackers or facilitators that are not located in the physical jurisdiction of the prosecutor, it is certain that many of the computers or servers that store crucial digital evidence are not located in a local jurisdiction, which poses major challenges.

> Consider the following two scenarios. In the first, the terrorists make use of Gmail to communicate with each other, and investigators have identified several Gmail accounts used by the suspects. It is critical that investigators retrieve

the emails that have been sent and received from these accounts, and obtain the incoming IP addresses of when the users of the account connect to Gmail. In the second, the same group of terrorists launch an attack on a government target, but the terrorist hackers are located in another country. They connect to a computer that they have compromised in a second country, which then connects to a computer that they have compromised in a third country, which then is used to launch a cyberattack against critical infrastructure in the target country.

In both of these scenarios the crucial evidence needed to prove the case is located in a foreign jurisdiction, and without it the case cannot be proved in a court of law. The second problem is that many types of digital evidence, such as logs, are not stored for long periods of time, so time is often of the essence in obtaining digital evidence.

Prosecutors will thus need to be familiar with the procedures for obtaining evidence from other jurisdictions' MLA treaties. In many instances, investigators will not be familiar with these, and as such prosecutors will also have to play a role in educating them. If a country is a signatory to the European Convention on Cyber Crime, there are also procedures that can be utilised to preserve evidence quickly while waiting for relevant assistance. It is crucial that prosecutors are familiar not only with these procedures but also with which countries they can be used.

The second significant concern in dealing with cyberterrorism is the capacity of law enforcement investigators to conduct the investigations, and the capacity of forensics practitioners to examine and analyse the digital evidence involved. Prosecutors are dependent on these role players to prepare the cases for court, and the highly technical nature of cyberterrorism, or the facilitation of terrorist activities via the Internet, means that many law enforcement investigators are not skilled in investigating them. In addition, many forensic laboratories do not have the expertise or resources to deal with digital evidence correctly.

Chapter 3

Digital evidence

A key element necessary to prove a case in court is evidence: without evidence, no conviction is possible. As computers and digital devices have become a fundamental part of our society, so too has their role, and the digital information contained in them, become part of the terrorism problem.

> Digital information is information that exists in a binary state, and that can be used to store, transmit and process almost any other type of information such as letters, numbers, words, pictures, sound and video material. Prosecutors need a good understanding of digital evidence.

Computers, information systems, communication devices and other digital devices are now used as tools to commit terrorist acts or facilitate them, as the targets of terrorist activity, and for potentially storing digital evidence that can prove or disprove legal issues in dispute.

> The prosecution environment has therefore fundamentally changed and any prosecutor must now be comfortable with understanding and using digital evidence.

Evidence is the admissible information used by a court of law to reach a decision on any matter brought before it for adjudication. Digital evidence is merely another type of evidence that a court can use in reaching a decision in cases.

The proliferation of digital devices and the expansion of the Internet mean that digital evidence can be present in virtually any case – it is not limited to so-called computer crimes but is relevant to the investigation of almost any crime, specifically terrorism. Digital evidence is now a fundamental part of many investigations, for example

SMS messages sent between two terrorists planning an attack, videos made from a mobile phone recording the movement of police officers outside a building that terrorists plan to attack, emails used to recruit suicide bombers, etc.

The increase in potential digital evidence means that prosecutors need to understand its nature and value, and in many instances this requires them to embrace a new approach to prosecutions where the traditional physical and witness-based evidence is augmented with digital evidence.

Usually investigators will not themselves seize raw data at the scene of an incident, as it is generally found on devices capable of storing it such as computers, mobile phones, etc.

> In many ways obtaining data is like obtaining a fingerprint, in that the investigator protects or secures the item containing the fingerprint, and the fingerprint itself is lifted by a fingerprint expert. With digital evidence, the investigator often simply secures the storage device and the data is obtained by a digital forensic examiner.

A digital forensic examiner is a forensic scientist who specialises in the forensic examination of digital evidence and the devices containing that digital evidence. Generally digital forensic examiners have a degree in computer science or a similar field, and often a postgraduate qualification in digital forensics. They also have extensive specialist training in digital forensics and in general information technology. Another factor to take into account regarding digital forensic examiners is that they must keep up to date with changes in technology, unlike some of the more traditional forensic sciences. Often, individuals who have only received training in using digital forensic tools such as EnCase or FTK are considered qualified digital forensic examiners, but without the fundamental computer science and digital forensic science skills and knowledge this is erroneous. It is like expecting a person who was trained in using a particular spreadsheet application such as Excel to be a qualified accountant, simply by virtue of their being proficient in Excel.

3.1 Defining digital evidence

Evidence can be defined as anything that tends to logically prove or disprove a fact at issue in a judicial case.[325] In other words, it is anything that can assist in establishing guilt or innocence. Digital evidence is defined as information of a legal

probative value that is either stored or transmitted in a digital form.[326] It is thus any data stored or transmitted using a computer that supports or refutes a theory of how an offence occurred, or addresses a critical element thereof such as intention or alibi. Digital evidence includes any computer hardware (containing data), software or data that can be used to prove the who, what, when, where, why or how of an allegation being investigated.

Essentially, digital evidence is any data stored or transmitted in a digital format (binary) that can be used in a criminal prosecution to either prove or disprove any aspect of the case.

> At its core, digital evidence is nothing more than strings of numbers that computing systems process and interpret. The numbers that a computer system understands are binary, which is essentially a number system using only two digits: a 0 (think of it as a light switched off) and a 1 (think of it as a light switched on). These ones and zeroes are known as bits. Eight bits make a byte and various bytes can be interpreted by computer systems to be characters, numbers and more. These ones and zeroes form the building blocks of everything we create, store, view, hear and transmit on a computer or mobile phone.

For example, the name Jason consists of five letters, one of which is a capital letter. Using ASCII encoding, which is commonly used on most computer systems, each letter would be represented by a single byte of data, which consists of eight binary bits, the 0s and 1s. These binary numbers are as follows:

J	01001010
a	01100001
s	01110011
o	01101111
n	01101110

Thus the name Jason as a computer understands it is simply a binary number: 010010100110000101110011011011110110111**0**. Everything that is stored, transmitted, heard or viewed on a computer is nothing more than binary numbers that the computer interprets and presents in a form we understand and can use.

Examples of digital evidence include:

- Digital photographs
- Digital video (including from CCTV cameras)
- Emails
- Text messages (including SMS, MMS, BBM, WhatsApp, etc.)
- Websites and pages
- Documents and spreadsheets

3.2 The nature of digital evidence

Digital evidence is by its very nature fragile and can easily be altered, damaged or destroyed through improper handling or examination.[327] There are a number of inherent challenges to the use of digital evidence in court. Perhaps the most significant is the ease with which it can be manipulated or altered, either intentionally or accidentally, without leaving any obvious signs of what has happened.[328]

The ease with which data is altered can be illustrated using the binary number example of the name Jason. Jason is binary number 010010100110000101110011 0110111101101110. If the last bit of the binary number is changed from 0 to 1, we would get the following:

J	01001010
a	01100001
s	01110011
o	01101111
o	01101111

So changing just one bit of information changes the number, which changes the name from Jason to Jasoo. Thus changing a single bit of data can cause a significant change to the information that we rely upon as evidence. It is for this reason that digital evidence should only be collected by those who have been trained to do so.

The simple act of switching on a computer may alter hundreds of files without the investigator even being aware of it, thereby contaminating digital evidence. Opening a potentially suspicious file may alter the metadata associated with that file, thereby altering the file. Metadata is essentially 'data about data', for example, the date that a particular file was created. Simply copying a suspicious file from a suspect's computer to another storage device, such as a USB thumb drive, alters the file. All of these actions are the digital equivalent of tramping over the evidence in a physical crime scene by walking around on it. Unfortunately these are all too common events, performed by investigators who do not understand the nature and fragility of digital evidence.

However, the very nature of digital evidence also mitigates these risks:[329]

- Digital evidence can be duplicated exactly, and a copy can be examined as though it were the original. Thus the copy can be examined without the need to examine the original data and potentially alter it.
- Using mathematical one-way hashing allows any alteration of digital evidence to be determined by comparing the hash values of the copies to the original.
- Digital evidence is difficult to destroy. Simply deleting the files and data does not actually remove it, and traces are left that can be recovered using specific forensic procedures.
- When criminals try to destroy digital evidence, copies and associated latent evidence can still remain in places that they are not aware of, due to how modern computer systems, servers and networks work.

Digital evidence is valuable and should be treated no differently than traditional physical evidence; with respect and care, and while the methods used in its recovery, handling and processing may seem complex and costly, when used correctly they produce evidence that is both compelling and cost effective. As with any other type of physical evidence, the improper handling or forensic processing of digital evidence can destroy its court value, including making it inadmissible as evidence.[330]

The information created and stored on a computer or digital device can be seen as a double-edged sword from a digital forensics perspective, as not only can it provide compelling evidence in a variety of investigations but it can also introduce

a level of complexity that can trip up even experienced digital forensic examiners. The problem with digital forensic evidence is that it is often technically complex, and the legal system's lack of technical awareness has led to some presiding officers making inappropriate assumptions because they are not always in the best position to evaluate the reliability of the digital evidence. The best way that this can be addressed is to make use of experienced and well-trained digital forensic scientists who can interpret and explain the evidence to the court.

3.3 Uses of digital evidence

Digital evidence can be used to answer certain fundamental questions relating to a case under investigation, including what happened when, who interacted with whom, the origin of a particular item of evidence, and who was responsible for it.

While many people only consider digital evidence in a typical computer crime such as hacking or malware distribution, digital evidence is present in virtually every incident that is investigated. Digital evidence can be used to determine the answers to a number of questions, such as:

- When something happened in a time sequence or timeline, for example when a particular email was sent or read, or when a particular file was printed. For example, in an investigation into a terrorist plot the times when particular communications were made to members of the terrorist cell could be used to determine the command structure.
- Who interacted with whom, establishing links between two parties, including which user was chatting to a person in an Internet chat room, or who had sent emails to each other. For example, it can be used to establish with whom a terrorist had been talking online to share attack plans.
- From where a particular digital evidence item originated. For example, on which computer did a particular document originate?
- Which user account was responsible for a particular transaction or event. For example, which user account had been logged onto the computer when money was transferred from one bank account to another using Internet banking?
- Reconstructing exactly how a particular offence took place, for example, how a terrorist hacker managed to gain access to a secured computer network.

The complexity of these information systems means that individual items of digital evidence may have multiple interpretations, and as such corroborating information may be required to reach a factually correct conclusion.[331] Consider a case where a person is suspected of downloading pictures of a secured site that is the planned target of a proposed terrorist attack, and an examination of his computer finds pictures of the site of the planned attack in the Internet cache. This evidence may be interpreted that the user visited a website and viewed these pictures as part of a terrorist plan, but the logs for the web browser of the computer show that on the date that the websites were opened on the computer, the website from which the photos came was only accessed for a millisecond, as were a number of other websites in rapid succession. In other words, each website was opened for a split second, far faster than a person could do so. A further examination shows that the computer has been infected with a virus that rapidly opened up random websites, which included the site containing images of the targeted location, and that the user of the computer was not responsible at all. If only the initial interpretation had been considered, it would have been incorrect, and an innocent person could have been prosecuted and/or punished and the actual terrorists not identified.

While digital evidence can be used to answer a number of questions relevant to a legal action, the one question that it cannot answer conclusively is who was using a particular device at any particular time. While it may be possible to make a circumstantial determination, it must always be kept in mind that digital evidence cannot physically link a suspect to an action. In other words, digital evidence is not physical evidence that can individualise a person as can be done with a fingerprint or DNA, and thus it cannot prove who was at the keyboard of a computer or using a mobile phone when a particular file was created or SMS sent. It can only link a device to a specific set of digital evidence that was created or stored on that device. However, this does not change the value that digital evidence brings to an investigation.

3.4 Sources of digital evidence

Digital evidence can exist on any electronic device or storage media (such as optical, magnetic or solid state media) that is capable of processes or storing digital information. In our modern society we store photos, documents, videos, messages and much more on electronic devices, we communicate with them, and our daily lives have become intertwined with technology. As technology develops, new devices capable of storing digital information and new storage mediums may

become commonplace, and as such, investigators should try to stay up to date with technological developments. Take, for example, mobile phones, which have become commonplace. We use them not only to talk to each other but also to take photos, send emails and access the Internet. Every mobile phone is a potential source of digital evidence now, and who is to say what new digital technology will be commonplace in the future? The digital information on a mobile phone can help to create a profile of the user of the device in the sense of the patterns in using specific applications, habits when the mobile phone or applications are used, etc. – it becomes the owner of the device's electronic footprint.

Digital evidence can generally be considered to come from one of the following distinct categories of electronic devices or storage mediums:

- Desktop computers
- Portable computers (including laptops, netbooks and tablets)
- External or portable hard drives
- Mobile and smart phones
- Portable media players
- USB thumb drives
- Digital cameras
- Flash memory cards
- CD or DVD disks

Uncommon electronic devices and storage media are those that are not as common in broader society, or those items that generally are not considered as a source of digital evidence in investigations. These include:

- Server computers
- Printers containing internal memory or digital media storage capacity
- Telephone answering machines or telephones with these capacities built in
- Digital voice recorders
- GPS devices
- Digital video recorders
- Dedicated computer game consoles

The rapid development in technology and digital devices may result in many devices that are currently considered uncommon becoming common, and even outdated in only a few years. It is thus important that prosecutors constantly update their knowledge about new technology and digital devices that come onto the market and the potential that they may have for digital evidence.

Protected devices and media are those common and uncommon devices and media that are designed to prevent unauthorised access of usage through the use of some security mechanism, which can include biometric devices such as fingerprint readers or iris scanners, or devices that require a security access 'token' such as an encoded access card or a dongle.

Electronic devices and storage media can be disguised, either commercially or through a process of 'moding' to look like something else. For example, in one case, a USB thumb drive containing incriminating digital evidence was designed to look like a piece of sushi, and found stored in the suspect's refrigerator.

The use of wireless networking technology has also aided the concealment of certain electronic devices such as wireless routers and wireless network storage devices, and there have been examples of these devices being hidden in ceilings or crawlspaces, as they no longer need network cabling to be accessed.

3.5 The admissibility and relevance of digital evidence

For evidence to be useable in court proceedings, it must be both relevant and admissible. If evidence is not relevant or admissible it may not be considered in the case before court, as it may unfairly prejudice or give an unfair advantage to one of the parties.

Relevant evidence is evidence that can prove or disprove any of the facts at issue in the case. When one looks at how individuals use their computers and other mobile devices, it is clear that traces of most of our lives can be found on them. However, there can be a huge amount of data on a standard computer of smart phone, most of which may not be relevant to a case under investigation. For example, a single gigabyte of data (1GB) is the equivalent of 212 000 A4 pages of information, and thus it is very easy to be overwhelmed by the sheer volume of data that people can load onto their personal computers and smart phones, leading to the possibility of using digital evidence that is not relevant. It is very important that prosecutors limit themselves to only using digital evidence that is relevant to their case. What is meant here by relevant is evidence that is relevant to the case under investigation.

Relying on evidence that may ultimately be ruled irrelevant in legal proceedings could undermine a case considerably.

Evidence, including digital evidence, is ruled either admissible or inadmissible. Admissible evidence is evidence that meets all regulatory and statutory requirements and has been correctly obtained and handled. Evidence that is deemed inadmissible in a legal proceeding cannot be considered by the court. The two quickest methods that an inexperienced investigator can apply that will result in evidence not being admissible in court are to collect evidence in an illegal manner, or to modify it after it has come into the possession of the investigator/examiner. To ensure admissibility, it is critical that the legal requirements are complied with, which would include the rules relating to search and seizure, the maintenance of proper chain of custody, and ensuring that the digital evidence is not altered in any way.

In this regard, a noteworthy case study is the decision of the US Supreme Court in the matter of *Riley v California*:[332]

> David Riley was stopped by officials for a traffic violation, which led to his arrest on weapons charges. The arresting officer searched Riley and seized his mobile phone from his pants pocket. The officer accessed the phone and observed the repeated use of a term associated with a street gang. The phone was later further examined by a gang expert officer. Riley was charged with the shooting. He moved to suppress the evidence. The trial court denied the motion, resulting in his conviction. The California Court of Appeal later confirmed Riley's conviction. Riley appealed to the US Supreme Court.
>
> The US Supreme Court simultaneously considered the arrest of Brima Wurie [United States v Wurie 728 F.3d 1 (1st Cir. 2013), reh'g en banc denied, No. 11-1792, 2013 WL 4080123 (1st Cir. July
>
> 29, 2013)], who was arrested after police had observed him participating in a drug sale. Wurie's phone was seized and accessed, which resulted in a search warrant being obtained for Wurie's residence where police found drugs, firearms and cash. Photographs and videos in relation to a shooting that had occurred a few weeks earlier were also found on the phone. Wurie also unsuccessfully attempted to suppress the evidence. He was convicted, but this was overturned by the First Circuit Court.

The US Supreme Court held that:

'Police generally may not, without a warrant, search digital information on a phone seized from an individual who has been arrested' and that searches must fall within one of the specific exceptions to the Fourth Amendment's warrant requirements.

Practitioners are advised to apply the principles in *Riley* in conformity with their own domestic laws, principles and constitutions.

Digital forensic examiners and investigators make a number of other common mistakes that can render digital evidence inadmissible, including:[333]

- Failing to create and maintain the proper documentation through all stages of the digital forensic process
- Inadvertently modifying digital evidence
- Failing to maintain the chain of custody
- Failing to realise when they have reached the limits of their knowledge and asking for advice

Investigators should never access any computer, mobile phone or other electronic device themselves to look for possible information of value, as they will very likely alter the evidence at a fundamental level. To illustrate this point, in one investigation the investigators had seized a USB thumb drive when they arrested a suspect, and later decided to plug it into a computer to view the files. They opened several files, found some that were relevant to their investigation and then handed the USB thumb drive to digital forensic practitioners to extract the evidence for court purposes. However, the forensic examination of the USB flash drive showed that several of the files had been opened and inadvertently modified after having been taken into possession. This created a problem with the integrity of the evidence, as it could not be proven that the evidence had not been altered or manipulated by the investigators to incriminate the suspects.

Key issues to consider when making use of digital evidence in court include:

- The reliability of the manner in which the digital evidence was generated, stored or communicated
- The reliability of the manner in which the integrity of the digital evidence was maintained
- The manner in which the origin of the digital evidence was established

These issues address at a fundamental level the need for establishing a proper chain of evidence and establishing the reliability of the digital evidence using cryptographic means such as mathematical hashes. Essentially, mathematical hashing is a digital forensic technique that creates a digital fingerprint of a single file, or even an entire digital storage medium, and if even one byte of data is changed it can be established that the data has been altered, as the mathematical hash would no longer match that originally made. While it is generally the responsibility of the digital forensic practitioner to perform the hashing functions, investigators can still play a crucial role in ensuring that the court can give due evidential weight to the digital evidence.

It is noteworthy to read the judgement in the matter of *Motata v Nair N.O. & Ano*,[334] in which a South African judge emphasises the test for the admissibility of electronic evidence and the purpose for which such evidence is tendered.[335]

3.6 The relationship between digital evidence and digital forensics

Key factors in ensuring the admissibility, and in certain instances the relevance, of digital evidence involve processes based on the practices of criminalistics and forensic science. In relation to digital evidence, digital forensics is a critical component in bringing this evidence to court, as the use of digital forensics follows certain standard procedures. These procedures tend to persuade the court to admit digital evidence and give due and proper evidential weight to it. As digital forensics is a specialised field, the courts have tended to treat evidence presented as a result of a digital forensic process as expert witness evidence, similar to that presented by a scientist.

Digital forensics provides for an expert witness to show the court that the digital evidence that is produced in court is exactly the same as when it was first seized. This is a critical component of ensuring admissibility. Various bodies have

established universal standards and procedures for digital forensic experts to ensure that they provide guidance to courts on the admissibility of digital evidence.

The Association of Chief Police Officers in the UK has developed four basic principles for computer-based digital evidence, to aid in the acceptance of digital evidence and the forensic examination thereof in a court of law, which have become widely accepted in the digital forensics discipline.[336] These are:

- No action taken by an investigator or examiner should change data held on a computer or storage media that may subsequently be relied upon in court.
- In circumstances where an investigator or examiner must access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- An audit trail or other record of all processes applied to computer-based digital evidence must be created and preserved, and it must be detailed enough to allow another independent digital forensic examiner to use these documents and achieve the same results by following processes documented therein.
- The person in charge of an investigation has the overall responsibility for ensuring that these principles are adhered to.

The principles established by the Association of Chief Police Officers in effect set the fundamental ground rules for dealing with digital evidence, and provide a mechanism to improve the admissibility of digital evidence in courts of law.

The procedures to collect physical evidence must also be very rigorous and established, in order to protect it from contamination or destruction, or from claims that it was tampered with or handled improperly, and to establish and preserve the chain of custody.

By following established forensic science practices, this fragile and easily altered form of evidence can be demonstrated to be authentic, whereas failure to follow these established procedures could result in the digital evidence being excluded from a court of law, or at the very least being given limited evidential value. In many respects, digital evidence is simply another form of latent evidence, which must be handled using accepted forensic science principles within appropriate legal boundaries.

Chapter 4

Digital forensics

Digital forensics began as a discipline in the mid-1980s as US federal law enforcement agencies saw the increasing use of computers in crimes.[337] In the early 1990s the International Association of Computer Investigative Specialists created the first documented set of guidelines for digital forensics,[338] followed by the Association of Chief Police Officers, the International Organization on Digital Evidence, the Scientific Working Group on Digital Evidence, and the International Federation of Information Processing Working Group 11.9 on Digital Forensics.

Initial conceptual approaches to digital forensic practice were fragmented, which perpetuated the viewpoint that there was no standard approach to digital forensic practice, but the development of common conceptual approaches was necessary for digital forensics to be considered a valid forensic science discipline.[339] In 2003 digital forensics joined mainstream forensic science when the American Society of Crime Laboratory Directors-Laboratory Accreditation Board recognised it as a fully-fledged forensic science discipline.[340] Digital forensics has since become widely recognised as a valid forensic discipline.

The practice of digital forensics did not start in a forensic laboratory, but developed as a result of police detectives and investigators around the globe who realised in the early days of computing that computers may be sources of evidence. Digital forensics accordingly developed in an ad-hoc manner, rather than a scientific one, but this has changed, and the development of digital forensics is increasingly scientific in nature. Digital forensics is now a valid scientific discipline, subject to the rigours and expectations of the greater field of forensic science.[341]

Digital forensics could be described as the application of scientific knowledge from the fields of computer science and information systems for a legal application.

In recent years, courts have begun to recognise digital forensics as a legitimate scientific method for discovering and proving facts that can be used as evidence before a court of law, thereby endorsing the validity of the scientific discipline.

4.1 Defining digital forensics

Digital forensics involves the preservation, identification, extraction and documentation of digital evidence stored as data or magnetically encoded information. In essence, digital forensics is about evidence from computers, digital media or digital devices that can stand up to scrutiny in court. The objective of digital forensics is in essence quite simple, namely to recover, analyse and present digital evidence in such a way that it is usable as evidence in a court of law.[342]

Another definition of digital forensics is that it is the science of acquiring, preserving, retrieving and presenting data that has been processed electronically and stored on computer media.[343] In yet another definition, digital forensics is the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events, or helping to anticipate unauthorised actions.[344]

A key factor in the various definitions of digital forensics is the scientific nature of digital forensics, which is a strong indication of the prevailing viewpoint that digital forensics is considered a scientific, or at the very least an applied science, discipline. Digital forensics could thus more appropriately be named digital forensic science.

A key factor in the forensic science process used in digital forensics is to ask one or more specific investigative or legal questions, which are ultimately translated into scientific questions.[345] These scientific questions should be asked by the forensic scientist in response to questions posed by the investigator in the case, and should be asked before evidence is examined or analysed by the forensic scientist.

Other factors in the practice of forensic science include the concepts of reproducibility, validation and verification. Reproducibility is one of the primary means by which forensic scientists validate each other's results and thus combat the occurrence of scientific fraud, and can lead to the formalisation of scientific standards into commercial products. Validation is defined as confirmation by way of an examination and demonstrating objective evidence that a particular forensic tool, technique or procedure functions correctly and as it was intended to. Verification is

defined as the confirmation of a validation with forensic laboratory tools, techniques and procedures.

In conducting a forensic science examination and analysis of evidence, a number of broad tests should be applied to the evidence so that the scientists can satisfy themselves and others that the results of their analysis are correct in the context of the case at hand. Broad tests that should be applied to any forensic evidence include:[346]

- Is the evidence authentic? Does the evidence come from where it is said to have come?
- Is the evidence reliable? Can the story that the evidence tells be believed, and is that story consistent? Are there any reasons to doubt that the computer on which digital evidence was found was not working correctly?
- Is the evidence complete? Is the story that the evidence tells complete? Are there any other stories that the evidence may tell that have a bearing on the case?
- Is the evidence free from interference and contamination?

To ensure that digital forensic evidence meets these tests, any approach to digital forensic science, by both investigators handling potential sources of digital evidence and digital forensic examiners, should include:

- Procedures that are well defined to address the various digital forensic tasks performed during the various phases of the digital forensic process, as discussed below.
- Anticipation that the methodology used will be criticised by the opposition's legal counsel in court on the grounds of failing to demonstrate authenticity, reliability, completeness and possible contamination as a result of the forensic examination. To counter this, detailed documentation must be maintained for all processes and actions related to the evidence in question.
- The possibility that repeat tests will be carried out, possibly by forensic experts hired by the other side.
- Checklists to support each methodology used, to ensure consistency.

- Anticipation of any problems relating to formal legal tests of admissibility by the opposition's counsel. To counter this, the relevant legal authority must be obtained prior to any examination, and detailed documentation be kept.
- The acceptance that any method used could almost certainly be subject to later modification or improvement due to the rapid changes in technology in the field of digital forensics. This is especially relevant when cases take a long time to go to trial from the time that the digital forensic examination has been performed, and in the time period leading up to the trial new methods, tools or techniques have been developed that could give more accurate results.

4.2 The digital forensics process

At a fundamental level the principles and processes of forensic science as a discipline are applicable to the field of digital forensics. In addition to these, the application of the scientific method of analysis is critical to classify digital forensics as a forensic science.

The scientific analysis method in digital forensic science involves four distinct stages:[347]

- Gathering information and making observations about the evidence. This phase involves verifying the integrity and authenticity of the evidence, reviewing the evidence, data carving, and key word searching. This phase is typically known as a digital forensic examination.
- Forming a hypothesis to explain the observations in the previous stage.
- Evaluating the hypothesis. This phase involves testing the hypothesis to determine if it is true, and if it is not to revise the hypothesis and look at further tests.
- Drawing conclusions and communicating findings.

The scientific analysis method used in digital forensic science is cyclic and may require a digital forensic examiner to repeat steps until a correct conclusion can be determined. For example, if tests and experiments disprove the hypothesis, a new one must be formed and evaluated.[348] In effect, experimentation is a natural part of the digital forensic process.

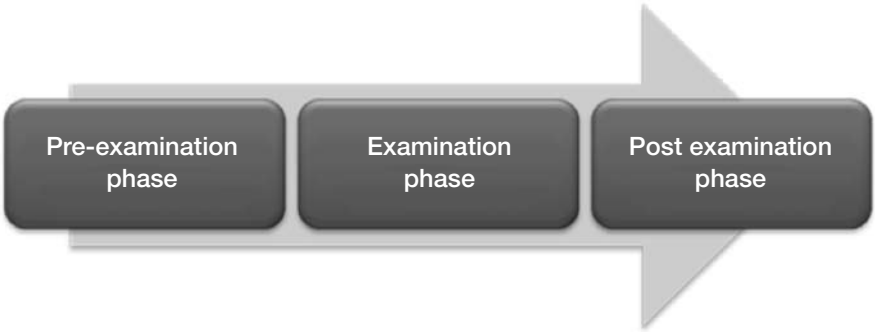
Although every digital forensic examination will differ based on the data being examined, the objectives of the investigation, the resources available, and other factors such as the skill, knowledge and experience of the digital forensic practitioner, when applying the scientific analysis method to a digital forensic examination the underlying fundamental process remains the same.

Fundamental to the digital scientific analysis method are the principles of repeatability and reproducibility, which are key requirements in forensics. The scientific analysis method also provides a valuable means to ensure that incorrect conclusions are not made based on incomplete or inconsistent methods being applied.

Digital forensic science is a process with a number of distinct stages, and it is crucial that digital forensics be understood within that context. Investigators, digital forensic examiners and prosecutors play different but complementary roles in this process, and these roles and responsibilities will be discussed in detail.

The entire digital forensic process can be separated into three broad phases: a pre-examination phase, an examination phase, and a post-examination phase, each of which follows sequentially, as illustrated in Figure 1.

Figure 1: Digital forensics phases



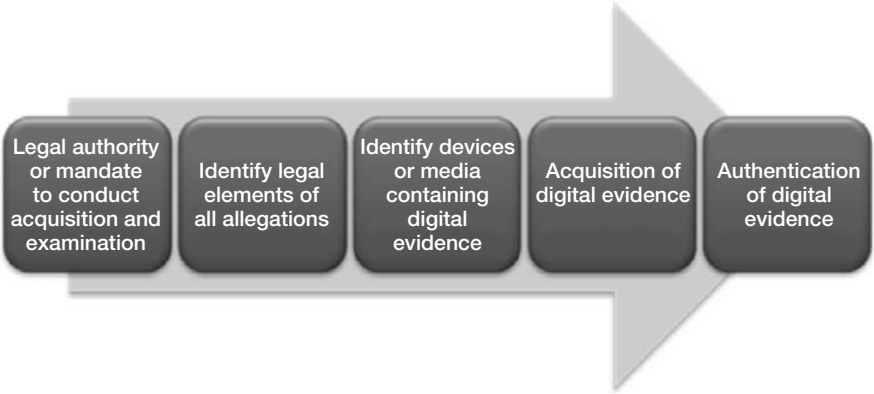
4.2.1 The pre-examination phase

The pre-examination phase of the digital forensic process consists of five specific processes that must be completed before any digital evidence can be examined by a digital forensic examiner. These are:

- Obtaining the legal authority or mandate to acquire and examine the digital evidence
- Identifying all the legal elements of all the allegations that you are investigating in terms of your legal authority
- Identify all possible devices or media that may contain potentially relevant digital evidence in terms of your legal authority
- Forensically acquiring the digital evidence from the identified devices or media
- Forensically authenticating the digital evidence acquired

Each of these processes follows sequentially on each other, as illustrated in Figure 2.

Figure 2: Processes in the pre-examination phase



The *first* step is to ensure that you have the correct legal authority to forensically acquire any digital evidence, and then to examine and analyse it. This step is traditionally performed by the investigator, who has to obtain the necessary legal authority.

In the context of a digital forensic examination, appropriate authority includes:

- A search warrant
- A subpoena or other court order
- Consent from a person who can legally consent to the acquisition and examination

The issue of consent as legal authority does have some potential challenges, especially in an organisational environment such as a business, where the accounting authority that is accountable for all assets, including computers, can consent to these computers being examined by virtue of their belonging to the organisation. However, while the business may own the computers, it may not actually be in a position to consent to the examination of data, especially if the data on those computers is the private data of the relevant user. If there is no policy in place within the organisation that specifically states that all data on the organisation's computers can be accessed and examined by the organisation, a user could claim that he/she had a right to privacy. It is crucial in this instance that the investigator obtain a copy of the written policy, as well as either a copy of the user's employment contract in which he/she agrees to abide by all policies or a copy of a signed acknowledgement that he/she has read or received the policy.

The *second* step is for the investigator to identify all the legal elements of each allegation being investigated and brief the digital forensic examiner, so that the digital forensic examiner has a good idea of what digital evidence may be legally relevant to the case at hand.

Not only does the legal authority authorise the acquisition and examination of the digital evidence, but it also limits the scope of the potential digital evidence that may be used in subsequent legal proceedings. To ensure that only relevant digital evidence is ultimately presented in legal proceedings, investigators need to know the exact legal elements of each allegation and inform the digital forensic examiner of the types of digital evidence that should be considered.

With the legal authority in place, and a clear understanding of the allegations being investigated, the *third* step requires investigators and digital forensic examiners to identify potential sources of digital evidence, so that these can either be seized and forensically imaged and examined off-site, or forensically imaged on site. In other words, if conducting a search and seizure, investigators would have to identify electronic devices such as computers, mobile phones, etc. that could contain the digital evidence they seek. Considering the number of potential sources of digital evidence, due diligence must be taken that all potentially relevant evidence is obtained. When one considers that a single 8GB SD memory card, the size of a postage stamp, could contain 1,6 million pages of information, and that it could be hidden virtually anywhere, searches must be especially thorough.

Unless the physical devices and media containing the digital evidence are forensically imaged on site by a digital forensic examiner, these will have to be seized by the investigator and taken to a digital forensic examiner for processing.

When encountered, these devices should be treated with as much care as any other physical item that is to be forensically examined. The following general principles, if adhered to, will ensure the best chance of evidence being recovered in an uncontaminated and therefore acceptable manner.

The majority of computers found during searches are desktop or laptop PCs. These machines usually consist of a screen, keyboard and main unit (with slots for CDs and DVDs or other storage devices). Other devices are becoming more widespread, in particular tablet computers. These can hold large amounts of data, often in storage areas not immediately obvious to the investigator.

When considering the seizure of desktop or laptop computers, the approach taken will largely depend on whether the computers are powered on at the time of seizure. Regardless of whether or not the computer is switched on or not, the investigator must keep detailed notes of everything that is done with regard to any computer evidence.

If the computer is not powered on, the following steps should be taken when seizing the items:

- Secure the area in which the computer is found, and move any people on the scene away from the computer and any of its wires and cables, as well as from any power plugs.
- Check to ensure that the computer is off. The monitors may simply be switched off, or the computer may be in sleep mode.
- Label and photograph all of the components of the computer, including the cables and where they are plugged in, and the ports into which they are plugged, or at the very least draw a diagram, so that the computer can be reconstructed in the digital forensic laboratory at a later date.
- Unplug the computer from the power socket. If the computer is a laptop, remove the internal battery (if possible) from it as well.
- Seal all of the components into properly labelled evidence bags.

- Search the area surrounding the computer for diaries, notebooks or even pieces of paper that may contain user names and passwords for the computer.
- If the owner of the computer is present, he/she should be interviewed to try to determine whether any passwords are used on the computer, and if so, what these are.
- Under no circumstances must an investigator switch on the computer.

If the computer is powered on, and no digital forensic examiner is present, the following steps should be taken when seizing the items:

- Secure the area in which the computer is found, and move any people on the scene away from the computer and any of its wires and cables, as well as from any power plugs.
- If the computer is connected to a network, whether or not via a cable or wireless connection, immediately contact a digital forensic examiner (it is always advisable for the investigator to have the telephone numbers of several digital forensic examiners on hand) for advice on how to proceed.
- If the computer screen is on, photograph the screen and its contents. If the screen is off, move the mouse or touch the touchpad (in the case of a laptop computer) to restore the screen and photograph it.
- Label and photograph all of the components of the computer, including the cables and where they are plugged in, and the ports into which they are plugged, or at the very least draw a diagram, so that the computer can be reconstructed in the digital forensic laboratory at a later date.
- Remove the power supply from the back of the computer without closing down any programs or shutting down the computer. The reason for doing this is that it prevents any changes from being made to running programs or any other data on the computer.
- Unplug the computer from the power socket. If the computer is a laptop, remove its internal battery (if possible), as well.

- Allow the equipment to first cool down before placing it into properly labelled evidence bags.
- Search the area surrounding the computer for diaries, notebooks or even pieces of paper that may contain user names and passwords for the computer.
- If the owner of the computer is present, he/she should be interviewed to try to determine whether any passwords are used on the computer, and if so, what they are.
- Under no circumstances should the user or owner of the computer be allowed to access the computer while it is on, and the investigator should not act on any advice that she is given by bystanders or the suspect in relation to the computer.

Following the above-mentioned process with computers that are powered on will result in the loss of some digital evidence, and if the data on the computer is encrypted it will likely mean that the evidence will not be usable. It is therefore strongly advisable when seizing computers to rather make use of a trained digital forensic examiner, or an investigator who is specifically equipped and trained to seize digital evidence from powered-on computer systems.

If the computer to be seized is a server, it is advisable that the seizure is only done by a trained digital forensic examiner, as simply pulling the plug will cause considerable damage to the data and possibly the device.

Mobile phones are commonplace, and seizing them requires investigators to follow the following steps to ensure the integrity of the digital evidence contained on them:

- Handle the cell phone like any normal piece of physical evidence, so as to preserve fingerprint and DNA evidence.
- Under no circumstances should the cell phone be accessed by the investigator, as this will alter evidence on the phone.
- If the cell phone is powered on, it must be placed in a Faraday bag or be wrapped in several layers of aluminium kitchen foil. This will, however, increase the power consumption of the phone and drain the battery quickly,

so it is vital that the phone be transported to the digital forensic laboratory for examination as quickly as possible. If the phone is off, do not switch it on.

- The power cables and connecters for the cell phone should be seized.
- Seal the cell phone and all of it cables and power supply in an appropriate evidence bag.
- The owner or user of the cell phone should be interviewed to determine whether or not he uses an access code to access the phone. If possible, this code should be obtained.

When transporting the items seized, it is crucial that they be secured and not placed near any strong magnetic sources such as car speakers, and they should be protected from physical shocks. They should also be kept clean of excessive dust and heat, and should not be exposed to any liquids.

Once the electronic device containing potential digital evidence has been identified, a forensic image should be made of it by a digital forensic examiner. In this *fourth* step, a digital forensic examiner acquires one or more forensic images of the data contained on the electronic device using a variety of specialised digital forensic software and hardware. This can be done either on or off site, depending on the circumstances. A forensic image is an exact duplicate of all of the data contained on the electronic device, and from a mathematical point of view is identical, and is thus considered original evidence and not a copy. Forensic imaging should only be done by a qualified digital forensic examiner or by an investigator who has received training in the forensic imaging of digital evidence and has the necessary tools to perform this function.

The *final* step of the pre-examination phase is to authenticate the forensic image of the digital evidence and verify that it is a mathematically identical duplicate of the source data. If the forensic images are not authenticated, it means that the digital evidence has not been correctly acquired. This process should be performed by a digital forensic examiner – if this is not done, the digital evidence could easily be challenged in court.

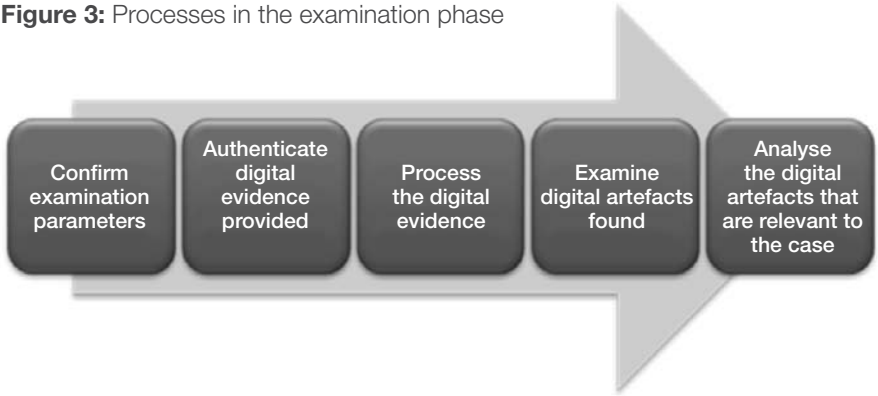
4.2.2 The examination phase

The examination phase of the digital forensic process consists of five specific processes that need to be completed before a thorough digital forensic examination has been conducted. If all of these steps are not conducted, the evidential value of any digital evidence processed will be deficient. These steps are:

- Confirm the legal parameters of the examination as established by the legal authority used to acquire the digital evidence
- Authenticate the forensic images received for examination
- Process the forensic images using standardised digital forensic processes and methods
- Examine and identify the individual digital artefacts uncovered during the processing of the forensic image, to determine and confirm their relevance to the case under investigation
- Analyse and individualise the digital artefacts identified as relevant, and interpret all of this evidence

Each of these processes follows sequentially on each other, as illustrated in Figure 3.

Figure 3: Processes in the examination phase



The *first* step is to confirm the legal parameters of the examination, ensuring that the correct legal authority is in place and that all of the elements of the legal issues being investigated are understood. While this may seem to be a duplication of steps in the pre-examination phase, it is quite common that the digital forensic examiner who examines the digital evidence is not the same person who acquired the digital evidence, and thus they need to confirm the legal authorisation and legal elements themselves for purposes of the examination.

It is important that investigators work with the digital forensic examiners to ensure that the digital forensic examiners understand the legal parameters of the investigation and focus on the objectives of the case at hand.

The *second* step is to authenticate the forensic images received for examination and compare the mathematical hash of the forensic image when it was made with the mathematical hash of the forensic image received to ensure that they are the same (this shows that the digital evidence has not been altered from acquisition to examination).

Once the forensic images have been authenticated by the digital forensic examiner, they will be processed using a number of digital forensic processes or methods to identify digital artefacts that may be relevant to the investigation. As each case is different, there is no one single standardised set of processes. Examples of some of the typical digital forensic processes that may be done during the processing step include:

- Reviewing files in various user accounts, so as to get an overview of in what files and actions the user has been engaged.
- Making a full text index of all textual data contained in the forensic images for the purposes of key word searches. This allows the digital forensic examiner to rapidly find any files that contain a particular word or phrase that may be relevant to the investigation.
- Recovering and reconstructing deleted files. Files that are simply deleted can often be recovered using specific digital forensic processes.
- Reviewing graphic files. A review of the graphic files found can often identify scanned documents or pictures of interest to the investigation.
- Identifying encrypted or password-protected files, and attempting to decrypt them or otherwise access them.
- Reviewing log files and other system files so as to be able to reconstruct what has taken place.

Once potentially relevant digital artefacts have been identified during the processing step, they are examined by the digital forensic examiner, often in conjunction with the investigator, to identify those data artefacts that are relevant to the investigation. Considering the amount of data that may be found during processing, this step is crucial to identify relevant evidence, so that the court that will ultimately evaluate the evidence will not be inundated with irrelevant evidence. The examination phase essentially answers the 'what' question.

With the relevant data artefacts identified, the digital forensic examiner needs to analyse these data artefacts to answer the 'who, what, when, where, and how'

questions, and to test this evidence in terms of the scientific method. It is during this step that the data artefacts are essentially interpreted by the digital forensic examiner to explain their relevance to the case and highlight their relevant evidential value.

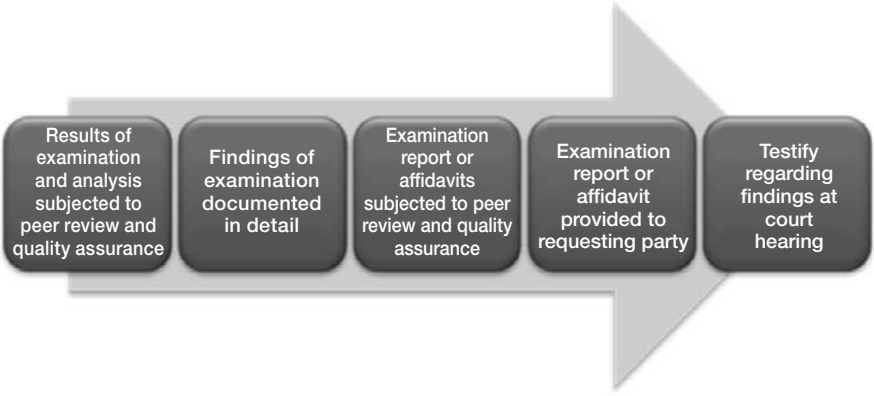
4.2.3 The post-examination phase

The post-examination phase of the digital forensic process consists of five specific processes that need to be completed, ultimately leading to the presentation of the digital evidence uncovered in court. These steps are:

- The results of the digital forensic examination process are reviewed by peers to ensure the accuracy and quality of the processes followed and the interpretations made.
- The digital forensic examiner documents the entire examination in detail in an affidavit or report.
- The digital forensic examiner's affidavit or report is then reviewed for quality assurance purposes.
- The finalised affidavit or report is provided to the investigator who requested the digital forensic examination.
- The digital forensic examiner's evidence is presented in court.

Each of these processes follows sequentially on each other, as illustrated in Figure 4.

Figure 4: Processes in the post-examination phase



Once the digital forensic examination phase has been completed, the work of the digital forensic examiner should be peer reviewed to check the accuracy of processes used and the correctness of interpretations made. This acts as a form of quality assurance to aid in the court's reliance on the digital evidence. If errors are identified, these can be corrected before the digital forensic examination is finalised.

With the peer review completed, the digital forensic examiner documents the entire digital forensic examination for court purposes. This must be a detailed enough record that another digital forensic examiner could follow the entire process used and make the same findings, but also written in such a way that it is easily understandable. This record usually has various annexures, including data artefacts and other digital evidence that will be court exhibits. The digital forensic examiner records her examination in the form of an affidavit or report. In general, affidavits, whether sworn or affirmed, are the preferred method of documentation.

The affidavit or report of the digital forensic examiner should then be reviewed for accuracy before it is released. At the least, another forensic examiner should review it, but ideally it should be reviewed by a prosecutor who understands digital forensics and digital evidence. This acts as a final quality assurance check before the digital forensic examiner's report or affidavit is released to the forensic examiner who had requested the digital forensic examination.

Ultimately the entire digital forensic process is concluded when the digital forensic examiner's evidence is presented and tested in court. A key factor for the prosecutor is understanding the evidence and ensuring that the evidence has been handled and examined using the necessary processes, as discussed above. The technical complexity of digital evidence can often be misunderstood, and prosecutors need to work with their technical witnesses to ensure that they present their evidence in a clear and understandable manner. Due to the often-complex technical nature of digital forensic evidence, when testifying it is important that the digital forensic examiner is able to translate these complex issues into easily understandable ones, so that the evidence can be understood in court and acted on accordingly.

A method that has worked well in conveying these complex topics is to try to find a common frame of reference and relate the complex topic to that frame of reference. To illustrate this, consider the concept of hacking. The analogy for hacking is housebreaking, which is a commonly understood crime. Table 2 shows how this can be used.

Table 2: Comparison between housebreaking and hacking

Housebreaking	Hacking
The criminal observes the victim's home to see what security measures are in place, and the comings and goings of the occupants.	The criminal identifies and scans the external facing IP addresses of the organisation to determine what ports are open and what services are running.
The criminal determines that a side window of the house has security bars, but they are screwed in with ordinary screws that are easily and quickly removed using a normal screwdriver, thereby allowing the criminal to gain access to the interior of the house.	The criminal identifies that the organisation is running a known vulnerable service on a particular port, and determines that it has not been patched. The criminal directs a specifically crafted series of data packets to the port that are designed to exploit that service and create a backdoor into the system through security.
The criminal, who is now inside the house, begins to look around for items of value that he can steal.	The criminal begins to search around for files that may be of value to him, so that he can copy them.
The criminal leaves the house with the stolen items.	The criminal leaves the network with the stolen data.

When dealing with cyberterrorism and digital evidence, the roles and responsibilities of the prosecutor are no different than that in any other case, and it is important not to be intimidated or overwhelmed simply because the issues are technically complex. Always remember that crime is a people problem, not a technological one.

Chapter 5

Conclusion

Cyberterrorism is a legitimate terrorist threat, as is the use of the Internet by terrorist groups, and it has the potential to become a significant threat going forward as our world grows smaller and more connected through technology.

Prosecutors can no longer effectively prosecute terrorists without considering all of the possible sources of digital evidence that may offer them proof. It is crucial that prosecutors understand digital evidence, where to find it, and how it can help them in their investigations. Overlooking or failing to consider digital evidence means that potential evidence that could prove or disprove a case will not be taken into account.

Not only must prosecutors be familiar with digital forensics, they must also understand the digital forensic science processes required to correctly collect, examine and analyse it. Understanding this means that they will be able to effectively use and evaluate digital evidence for court purposes.

Notes

1 Article 1, para 3.

2 Did not enter into force.

3 The League of Nations' 1937 Convention for the Prevention and Punishment of Terrorism.

4 Which are binding on all member states.

5 Antonio Cassese, Specific sub-categories of international terrorism as a discrete international crime (Terrorism as an international crime), *International criminal law*, (2nd ed), Oxford University Press, 30 April 2008, para 8.4, 169–170.

6 http://www.un.org/en/sc/ctc/docs/conventions/Conv1.pdf

7 Article 1, para 3 – 'an aircraft is considered to be in flight from the moment when power is applied for the purpose of take-off until the moment when the landing run ends'. Also see Article 5, para 2.

8 Article 1, para 4 – The convention is not applicable to military, customs or police aircraft.

9 Article 5, para 1.

10 Article 2.

11 Article 3, para 1 and 2 (Also see Article 16, para 1).

12 Articles 6–10.

13 Article 13.

14 Extradite or prosecute.

15 Vienna Convention on Consular Relations of 1963, which was signed on 24 April 1963 but became effective on 19 March 1967.

16 http://www.un.org/en/sc/ctc/docs/conventions/Conv2.pdf

17 Article 3, para 2.

18 Article 4, para 1 (a).

19 Article 4, para 1 (b).

20 Article 4, para 1 (c).

21 Article 4, para 2, read with Article 8.

22 Article 7.

23 Article 10.

24 Article 6.

25 http://www.un.org/en/sc/ctc/docs/conventions/Conv3.pdf

26 Article 1, para 1.a and b.
27 Article 1, para 1.c and d.
28 Article 1, para 2.
29 Article 3.
30 Article 5, para 1.a.
31 Article 5, para 1.b.
32 Article 5, para 1.c.
33 Article 5, para 1.d.
34 Article 5, para 2, read with Articles 6.1, 6.4, Article 7 and Article 8.
35 Article 6.
36 http://www.un.org/en/sc/ctc/docs/conventions/Conv4.pdf
37 Article 2, para 3.
38 Article 2, para 1.
39 Article 1.
40 Article 3, para 1.a.
41 Article 3.1.b.
42 Article 3.1.c.
43 Article 3.2, read with Article 7 and 8.
44 http://www.un.org/en/sc/ctc/docs/conventions/Conv5.pdf
45 Article 4.
46 Article 5, para 2, read with Articles 6.1, 6, 2, 7 and 8.
47 Article 6, para 3.
48 http://www.un.org/en/sc/ctc/docs/conventions/Conv6.pdf
49 Article 7.
50 Article 8, para 1.a.
51 Article 8, para 1.b.
52 Article 8, para 2.
53 http://www.un.org/en/sc/ctc/docs/conventions/Conv7.pdf
54 Article II.
55 http://www.un.org/en/sc/ctc/docs/conventions/Conv8.pdf
56 Article 7, para 3.
57 Article 9.
58 Article 3 *bis*.
59 Article 3 *ter.*
60 Article 3 *quater*.
61 Article 5 *bis.*
62 http://www.un.org/en/sc/ctc/docs/conventions/Conv9.pdf
63 Article 2 *bis*

64 http://www.un.org/en/sc/ctc/docs/conventions/Conv10.pdf

65 http://www.un.org/en/sc/ctc/docs/conventions/Conv11.pdf

66 Article 4.

67 Article 2.

68 Article 3.

69 Article 6.

70 Article 7.

71 Article 8.

72 Article 10.

73 Article 15.

74 Article 11.

75 Article 12.

76 Article 14.

77 http://www.un.org/en/sc/ctc/docs/conventions/Conv12.pdf

78 These are the Aircraft Convention, Civil Aviation Convention, Internationally Protected Persons Convention, Hostage Convention, Nuclear Convention, Civil Aviation Protocol, Maritime Navigation Convention, Safety of Fixed Platforms Protocol and the Terrorist Bombing Convention.

79 Article 4.

80 Article 6.

81 Article 7.

82 http://www.un.org/en/sc/ctc/docs/conventions/Conv13.pdf

83 Article 2.

84 Article 6.

85 Article 14.

86 Article 1.

87 Article 8.

88 Article 10.

89 Article 11.

90 http://www.un.org

91 http://www.un.org

92 http://www.un.org

93 http://www.un.org

94 Article 4.

95 Article 5.

96 Article 6.

97 Article 7.

98 Article 8.

99 Article 8.

100 Established under Article 9.

101 Convention relating to the Status of Refugees, adopted on 28 July 1951.

102 Adopted on 31 January 1967.

103 Article 2.

104 Article 5.

105 Article 6.

106 A/RES/60/288, http://www.un.org

107 http://www.un.org

108 https://treaties.un.org/doc/db/Terrorism/OAU-english.pdf

109 Article 1, paragraph 3.

110 Article 2.

111 Article 3, para 1.

112 Article 3, para 2.

113 Articles 4 and 5.

114 Article 6.

115 Article 7.

116 Adopted by the Third Ordinary Session of the Assembly of the African Union, Addis Ababa, 8 July 2004.

117 Article 2.

118 Article 3.

119 http://www.au.int/en/sites/default/files/PROTOCOL_STATUTE_AFRICAN_COURT_JUSTICE_AND_HUMAN_RIGHTS.pdf

120 Adopted at the 23rd AU Summit, Malabo, 15–16 May 2014.

121 Article 28G of the statute.

122 Article 28N of the statute.

123 Article 6 of the protocol, Article 46E of the statute.

124 Article 28A, para 3 of the statute.

125 Article 46A *bis* of the statute.

126 Article 46B, para 1 of the statute.

127 Article 46B, paras 2–4 of the statute.

128 Article 46C of the statute.

129 Article 46D of the statute.

130 Article 46E *bis*, para 2.

131 Article 46F of the statute.

132 Article 46H, para 1 of the statute.

133 Article 46H, para 2.

134 Article 46H, para 3 and 4 of the statute.

135 Article 46J *bis* of the statute.

136 Article 46K of the statute.

137 Commonly referred to as the central authority.

138 Mutual Legal Assistance in Criminal Matters: Court of Appeal, Ontario, Canada. 2001

139 SADC Protocol on Extradition, http://www.sadc.int/files/3513/5292/8371/Protocol_on_Extradiction.pdf

140 ECOWAS Convention on Extradition, http://documentation.ecowas.int/download/en/legal_documents/protocols/Convention%20on%20Extradition.pdf

141 http://secretariat.thecommonwealth.org/Internal/190714/190932/38061/documents/

142 Each state has its own procedural law on extradition, and practitioners must be familiar with it.

143 The ECOWAS Convention on Extradition permits 20 days for the submission of the formal request; the SADC Protocol on Extradition permits 30 days; and the IGAD Convention on Extradition permits 30 days.

144 Some treaties, for example the UN conventions, do not provide a time limit and will be governed by the domestic law of the requested state. Those in the requesting state will need to check this before submitting a request to make sure that, following the arrest, there is enough time to prepare and submit the necessary documents.

145 In some instances the sentence threshold may vary (two years or more) either under the relevant treaty or under the domestic law of a state. Practitioners should, therefore, check the relevant treaty and any declaration/reservation made by a state party.

146 Such cases can be rather complex as the transposition of conduct from the requesting to the requested state is sometimes far from easy. One approach is to transpose only the conduct that occurred in the requesting state to the requested state, leaving the conduct that occurred in other states *in situ*, and then determining if the transposed conduct amounts to an extradition crime.

147 Both items can be accessed at http://www.unodc.org/unodc/en/organized-crime/transfer-of-sentenced-persons.html and http://www.unodc.org/documents/organized-crime/Publications/Transfer_of_Sentenced_Persons_Ebook_E.pdf

148 In exceptional circumstances, transfer can be considered for a shorter sentence.

149 Article 12 of the CoE Convention on the Transfer of Sentenced Persons: http://conventions.coe.int/Treaty/en/Treaties/Html/112.html

150 The Supreme Co*urt of Canada in United States of America v. Cotroni; United States of America v. El Zein* (an extradition request for Cotroni and El Zein, both Canadian nationals) set out some practical matters to take into account in determining jurisdiction.

151 Making the Decision: Which Jurisdiction Should Prosecute? Eurojust Guidelines, Annual Report 2003: http://www.eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202003/Annual-Report-2003-EN.pdf

152 International Association of Prosecutors (IAP), Prosecutorial Guidelines for Cases of Concurrent Jurisdiction, Making the Decision – *'Which Jurisdiction Should Prosecute?'* 21 May 2014: http://www.iap-association.org/IAP/media/IAP-Folder/IAP_Guidelines_Cases_of_Concurrent_Jurisdiction_FINAL.pdf

153 Signed in Luanda, Angola on 3 October 2002 in Luanda by various African states.

154 Came into force on 29 September 2003, and ratified by many African countries.

155 Adopted on 8 September 2006.

156 Guidelines on the Role of Prosecutors, adopted by the 8th United Nations Congress in the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, 27 August – 7 September 1990; Layton David, The prosecutorial charging decision, *Criminal Law Quarterly,* 46, 2002, 446–482, 449; Dandur and Yvon, The role of prosecutors in promoting and strengthening the rule

of law, Second World Summit of Attorneys General, Prosecutors General and Chief Prosecutors, Doha, Qatar, 14–16 November 2005 (Working paper III in archive with the researcher), 3; John F Terzano, Joyce A McGee and Alanna D Holt, Improving prosecutorial accountability: the justice project, 2009, 2, http://www.thejusticeproject.org/.

157 United Nations Guidelines on the Role of Prosecutors, adopted by the 8th United Nations Congress in the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, 27 August – 7 September 1990, para 11.

158 Ibid., para 11.

159 Ibid., para 12.

160 Ibid., para 13 (a).

161 Ibid., para 13 (b).

162 Ibid., para 13 (c) and (d).

163 Ibid., Para 15.

164 Ibid., para 16.

165 Ibid., para 20.

166 Bennett L Gershman, *Prosecutorial misconduct,* Deerfield, Il, New York, NY, Rochester, NY: Clark Boardman Callaghan, 1997, vii; Donald G Gifford, Equal protection and the prosecutor's charging decision: enforcing an ideal, *The George Washington Law Review,* 49, 1980–1981, 659–719, 669; Michael A Caves, The prosecutor's dilemma: obligatory charging under the Ashcroft memo, *Journal of Law and Social Challenges,* 9, 2008, 11 and 12.

167 American Bar Association (ABA) Standards for Criminal Justice: Prosecution Function and Defence Function standard 3-1.2(c), 1993; Michael A Caves, The Prosecutor's Dilemma: Obligatory charging under the Ashcroft Memo, Journal of Law & Social Challenges, Spring 2008, Lexis Nexis, 9, 2008, 1–23, 3

168 *S v Yengeni* 2006 (1) SACR 405 (T), para [51] – [53].

169 *Zhang v Canada* (Attorney General) 2007 FCA 201, para [13].

170 *Kostuch v Alberta* (Attorney General) 1995 6244 (AB CA), (1995), 128 D.L.R. (4th), 440 at 447.

171 *National Director of Public Prosecutions v Freedom Under Law* (617/14) [2014] ZASCA 58 (17 April 2014), para [19], [20], [28] and [29].

172 *Charles Hurd v. The People*, Supreme Court of Michigan, 25 Mich. 404, 415 – 16 (1872), 25 Mich. LEXIS 122, Heard on July 12, 1872, decided on October 8, 1872

173 John F Terzano, Joyce A McGee & Alanna D Holt, Improving prosecutorial accountability the justice project, 2009, 14, http://www.thejusticeproject.org/.

174 William C Gourlie, Role of the prosecutor: Fair Minister of Justice with Firm Conviction, 46 Sask. L. Rev. 293 (1981-1982), 37–38, Heinonline K Turner, The role of Crown Counsel in Canadian Prosecutions, 1962, 488 C.B.R.(Canadian Bankruptcy Reports)

175 *Boucher v The Queen* [1955] SCR 16 ((1955) 110 CCC 263); *S v Shaik and Others* 2008 (2) SA 208 (CC), para 67.

176 *S v Shaik and Others* 2008 (2) SA 208 (CC), para 67.

177 *S v Okah* 2013 JDR 0219 (GSJ), 21 January 2013, www.saffli.org.za; 2013 JDR 0874 (GSJ), see http://www.saflii.org/za/cases/ZAGPJHC/2013/85.html; *S v Okah* (SS94/11) [2013] ZAGPJHC 85 (20 March 2013).

178 Uyo Salifu, Henry Okah counter-terrorism ruling is a judicial triumph for South Africa and the continent, *ISS Today,* 1 February 2013, http://www.issafrica.org/iss-today/henry-okah-counter-terrorism-ruling-is-a-judicial-triumph-for-south-africa-and-the-continent.

179 Section 5 of the Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004

180 *The Federal Republic of Nigeria v Charles Tombra Okah and 3 Others*, Charge No.: FHC/ABJ/CR/186/2010 and FHC/ABJ/CR/187/2010

181 Section 16(1) of POCDATARA requires the written consent of the NDPP in order for a prosecution to be instituted in contravention of the Act.

182 *Bogaards v The State* (864/10) [2011] ZASCA 196 (21 November 2011), 27 par [52] – 28 par [54].

183 South Africa would not extradite a person to such a country due to constitutional impediments.

184 He would be subject to persecution.

185 Who also happens to be Nigerian Minister of Justice

186 Contravening Section 2.

187 Contravening Section 5(a).

188 Contravening Section 5(b).

189 Contravening Section 14(b), read with section 8(a).

190 Contravening Section 4(1)(f).

191 Contravening Section 3(a).

192 Contravening Section 14(a) read with section 2 of Act 33 of 2004.

193 *SERAP v the Federal Republic of Nigeria*, Court of Justice of the Economic Community of West African States (ECOWAS), ECW/CCJ/JUD/18/12) General List No ECW/CCJ/APP/08/09.

194 *Aniso & Others v The President and Commander-in-Chief of the Armed Forces of the Federal Republic of Nigeria & Others*, Federal High Court of Nigeria, Port Harcourt Judicial Division, FHC/PH/CP/11/2000.

195 *Mohamed and Another v President of the Republic of South Africa and Others* 2001(3) SA 893 (CC) at 895 A – B]

196 Aut dedere aut judicare: The Duty to Extradite or Prosecute in International Law, Introduction: the principle aut dedere aut judicare, 4, M Cherif Bassiouni and Edward M Wise, Netherlands, 1995, Martinus Nijhoff Publishers

197 Ibid., 3.

198 Ibid., 4.

199 *National Commissioner, South African Police Service and Another v Southern African Human Rights Litigation Centre and Another* 2014 (2) SA 42 (SCA), para [32] B–C.

200 The notion of international criminal law (ICL) (fundamentals of international criminal law), Antonio Cassese, *International Criminal Law*, 2nd ed, 2008, Oxford University Press, 3, para 1.1.

201 Antonio Cassese, 'General features of ICL' (fundamentals of international criminal law), ibid., 4, para 1.2.

202 *National Commissioner, South African Police Service and Another v Southern African Human Rights Litigation Centre and Another* 2014 (2) SA 42 (SCA), para [32] C; *Brownlie's Principles of Public International law*, 8th ed, James Crawford, Oxford University Press, 2012, 447

203 *National Commissioner, South African Police Service and Another v Southern African Human Rights Litigation Centre and Another* 2014 (2) SA 42 (SCA), para [32] C–D; J Dugard, Jurisdiction and international crimes, in J Dugard et al, *International law: a South African perspective*, 4th ed, Cape Town: Juta, 2011, 146.

204 *National Commissioner, South African Police Service and Another v Southern African Human Rights Litigation Centre and Another* 2014 (2) SA 42 (SCA), para [33]; The SS Lotus (France v Turkey) (1927) PCIJ Series A No 10, 18–19.

205 National Commissioner supra, at para [34],

206 Universal jurisdiction: Clarifying the basic concept, *Journal of International Criminal Justice*, Roger O'Keefe, Oxford University Press, 2004, 735, 736, http://jicj.oxfordjournals.org/content/2/3/735.full.pdf+html, http://documents.law.yale.edu/sites/default/files/O'Keefe%20-%20Universal%20Jurisdiction%20-%202004.pdf

207 *National Commissioner, South African Police Service and Another v Southern African Human Rights Litigation Centre and Another* 2014 (2) SA 42 (SCA), para [34].

208 Ibid, para [35]; J Dugard, Jurisdiction and international crimes, in J Dugard et al, International law: A South African perspective 4th ed, Cape Town: Juta, 2011, 148–154.

209 *National Commissioner, South African Police Service and Another v Southern African Human Rights Litigation Centre and Another* 2014 (2) SA 42 (SCA), para [34].

210 Ibid., para [34].

211 *R v Hape* [2007] 2 S.C.R. 292, 2007 SCC 26 at para 66

212 *National Commissioner, South African Police Service and Another v Southern African Human Rights Litigation Centre and Another* 2014 (2) SA 42 (SCA), para [36] B and D.

213 *The SS Lotus (France v Turkey*) (1927) PCIJ Series A No. 10, 19.

214 *National Commissioner, South African Police Service and Another v Southern African Human Rights Litigation Centre and Another* 2014 (2) SA 42 (SCA), para [37].

215 Ibid., para [39].

216 The notion of international criminal law (ICL) (fundamentals of international criminal law), Antonio Cassese, International Criminal Law, 2nd ed, 2008, Oxford University Press, 169–170, para 8.4.

217 Assented to on 4 February 2005.

218 Adopted by the OAU.

219 The following Articles are relevant: 1(a) and (b), 2 (c) – (f), 3(b) and (c), 4 and 5.

220 *National Commissioner, South African Police Service and Another v Southern African Human Rights Litigation Centre and Another* 2014 (2) SA 42 (SCA), para [35].

221 The conventions and protocols, including the OAU Convention on the Prevention and Combating of Terrorism, as referred to herein above and which is referred to in the POCDATARA Act.

222 *National Commissioner, South African Police Service and Another v Southern African Human Rights Litigation Centre and Another* 2014 (2) SA 42 (SCA), para [39].

223 *Glenister v President of the Republic of South Africa and Others* 2011(3) SA 347 (CC), paras [179] – [195] and para [202].

224 *Minister of Home Affairs and Others v Tsebe and Others* 2012 (5) SA 467 (CC) at paras [61] to [64]

225 Prevention and Combating of Corrupt Activities Act 2004 (Act 12 of 2004).

226 Implementation of the Rome Statute of the International Criminal Court Act 2002 (Act 27 of 2002).

227 *South African Litigation Centre & Another v National Director of Public Prosecutions* [2012] 3 ALL SA 198(GNP) at paras [27] and [32].

228 *National Commissioner, SAPS v SAHR Litigation Centre* 2014 (2) SA 42 (SCA), paras [32] – [56].

229 Vienna Convention on Consular Relations of 1963, signed on 24 April 1963 and becoming effective on 19 March 1967.

230 In terms of section 317 of South Africa's Criminal Procedure Act 1977 (Act 51 of 1977).

231 For the purposes of this chapter.

232 UN International Convention for the Suppression of Terrorist Bombings (Terrorist Bombing Convention), New York, 15 December 1997 [came into force on 23 May 2001].

233 La Grand (FRG. V US) 2001 I.C.J. 466 (Germany v US)

234 Avena and Other Mexican Nationals 2004 I.C.J. 12 (Mex. v US)

235 *S v Okah* 2013 JDR 0874 (GSJ), http://www.saflii.org/za/cases/ZAGPJHC/2013/85.html; *S v Okah* (SS94/11) [2013] ZAGPJHC 85 (20 March 2013).

236 Ibid., para 21.

237 UN Convention against Transnational Organised Crime, GAR 55/25, Annex I.

238 Ibid., Article 24, para 3 and 4.

239 UN Gen Assembly Resolution 58/4, annex.

240 Ibid., Articles 32, 33 and 37, para 4.

241 Also referred to herein as 'related persons'.

242 Protective custody is the term commonly used when witnesses are in the care or custody of police or law enforcement authorities either by agreement or under duress where that witness's evidence is crucial to a matter but where his/her life is in severe danger or threats directed at the witness will result in his/her non-co-operation.

243 Under the auspices of the UNODC.

244 United Nations Office on Drugs and Crime

245 UNODC, *Good practices for the protection of witnesses in criminal proceedings involving organized crime*, 1.

246 Ibid.

247 UNODC, *Good practices for the protection of witnesses in criminal proceedings involving organized crime*, Introduction.

248 Ibid.

249 International trends in the facilitation of witness co-operation in organized crime cases, Nicholas Fyfe and James Sheptycki, *European Journal of Criminology*, 2006, July, Volume 3, 347–349, Thompson Reuters

250 UN Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power (UN General Assembly Resolution 40/34), 29 November 1985

251 Criminal Procedure Act 1977 (Act 51 of 1977).

252 Now known as the Minister of Justice and Correctional Services.

253 Who is a Special Director of Public Prosecutions in the Office of the National Director of Public Prosecutions.

254 The director's decision is based on recommendations from the provincial office head and of the relevant officials from law enforcement agencies and the NPA.

255 The director has the discretion to approve protection for a witness in respect of any other proceedings if satisfied that the safety of the witness warrants protection.

256 The OWP address will serve as the address at which legal proceedings may be instituted with regard to such a witness.

257 The decision on whether any information is to be disclosed lies within the sole discretion of the director, after consideration of representations and prejudice to any other applicable law.

258 Any such relocation requires ministerial approval.

259 See Part 4, Chapter 3.

260 In terms of section 144(3)(a) of the Criminal Procedure Act 51 of 1977

261 Collaborators.

262 *The Federal Republic of Nigeria v Charles Tombra Okah and 3 Others*, FHC/ABJ/CR/187/2010.

263 Uyo Salifu, Henry Okah counter-terrorism ruling is a judicial triumph for South Africa and the continent, *ISS Today*, 1 February 2013, http://www.issafrica.org/iss-today/henry-okah-counter-terrorism-ruling-is-a-judicial-triumph-for-south-africa-and-the-continent.

264 Opening remarks of the Executive Director, UN Office for Drug Control and Crime Prevention, Conference on Countering Terrorism through Enhanced International Cooperation, 22–24 September 2000, www.unodc.org

265 International Convention on the Suppression of the Financing of Terrorism , New York, 1999 (the Financing Convention).

266 This convention was adopted at the fourth session of the UN General Assembly on 9 December 1999 and as at 30 April 2014 had 132 signatories and 185 parties (see www.treaties.un.org).

267 www.un.org/en/ga

268 International Convention on the Suppression of the Financing of Terrorism , New York, 1999

269 Article 2.1.

270 Article 5.

271 Article 18.

272 UNSCR 1373(2001), www.un.org. All other resolutions referred to are available on this site.

273 UN Security Council Counter-Terrorism Committee, www.unorg/en/sc/ctc.

274 See United Nations Resolutions 1787, 2129 and 2133.

275 See, for example, United Nations Security Counsel Resolutions 2129 (2014) and 2133 (2014). www.un.org

276 UN General Assembly document A/66/762

277 The Commonwealth, http://secretariat.thecommonwealth.org.

278 FATF, About the FATF, www.fatf-gafi.org.

279 www.thegctf.org

280 African Union Peace and Security, www.peaceau.org

281 Article 1.

282 Article 2.

283 Article 4.

284 Article 5.1.

285 Article 2, para b.

286 African Union Peace and Security, www.peaceau.org.

287 Eastern and Southern Africa Anti-Money Laundering Group, www.esaamlg.org

288 Inter Governmental Action Group against Money Laundering in West Africa, www.giaba.org

289 East Africa Community, www.eac.int

290 Economic Community of West African States, www.comm.ecowas.int.

291 Southern African Regional Police Chiefs Cooperation Organisation, www.sarpcco.org

292 African Union Peace and Security, www.peaceau.org.

293 Specific conventions are listed.

294 UN Office on Drugs and Crime, www.unodc.org.

295 UN Security Council Committee pursuant to resolutions 1267 (1999) and 1989 (2011) concerning al-Qaeda and associated individuals and entities, 1267/1989, www.un.org/sc/committees/1267.

296 UN Security Council Resolution 2082 (Taliban) and Resolution 2083 (al-Qaeda).

297 *R v Khawaja* 2012 SCC 69, [2012] 3 SCR 555.

298 Increased anti-money laundering banking regulations and terrorism prosecutions , Albert L Kao, Naval Postgraduate School (NPS), Monterey, California, March 2013

299 At most, this section may be regarded as a collage of material that may have been superseded by appeals, new case law and legislative amendments.

300 FATF, About the FATF, www.fatf-gafi.org.

301 Drug trafficking, credit card and cheque fraud, extortion, etc.

302 www.giaba.org FATF Report, Terrorist Financing in West Africa, October 2013

303 www.giaba.org The Nexus between Small Arms and Light Weapons and Money Laundering and Terrorist Financing in West Africa, GIABA Report, 2013

304 Other investigations also attributed funding to kidnapping for ransom and arms smuggling.

305 The role of Hawala and other similar service providers in money laundering and terrorist financing, October 2013, FATF Report, www.fatf-gafi.org http://www.fatf-gafi.org/topics/methodsandtrends/documents/role-hawalas-in-ml-tf.html

306 Digest of terrorist cases , United Nations office on Drugs and Crime (UNODC), January 2010, United Nations (UN), New York www.unodc.org (http://www.unodc.org/documents/terrorism/09-86635_Ebook_English.pdf)

307 www.cdpp.gov.au

308 R v Khawaja 2012 SCC 69, [2012] 3 SCR 555.

309 *The United States of America v Mousa Mohammed Abu MARZOOK and Others* 383 F.Supp.2d 1056, United States District Court, N.D. Illinois, Eastern Division.

310 *The United States of America v Mohamad Youssef Hammoud and Others* 381 F.3d 316; 2004 U.S. App. Lexis 19036; 65 Fed. R. Evid. Serv. (Callaghan) 338

311 Approved in September 1990.

312 By way of confiscation and mutual legal assistance, as set out in Articles 13 to 16.

313 Laundering offences are targeted in Article 6.

314 Adopted by the Committee of Ministers of the Parliamentary Assembly of the Council of Europe at its 925th meeting on 3 May 2005.

315 The 1999 Terror Finance Convention was adopted on 9 December 1999.

316 Adopted on 12 September 2001.

317 Contained in Chapters 5 and 6 in the Prevention of Organised Crime Act 1998 (Act 121 of 1998, or POCA). The aforementioned chapters are replicated in South Africa's domestic terrorism law, the POCDATARA Act.

318 For guidance to the states with no asset forfeiture and statutes against terror finance, it is prudent to see South African provisions in POCA and POCDATARA for assistance. Item 32A in Schedule I of POCA is about terrorism as defined in POCDATARA, and which defines property.

319 *NDPP v Elran* 2013 (1) SACR 429 (CC); 2013 (4) BCLR 379 (CC)

320 *National Director of Public Prosecutions V Ro Cook Properties (Pty) Ltd; National Director of Public Prosecutions V 37 Gillespie Street Durban (Pty) Ltd and Another; National Director of Public Prosecutions V Seevnarayan* 2004 (2) SACR 208 (SCA).

321 *Edward Tracy v. The Iranian Ministry of Information and Security,* 2014 ONSC 1696 (CanLII) — 2014-03-17, Superior Court of Justice — Ontario, *Edward Tracy v. The Iranian Ministry of Information and Security*, 2014 ONSC 3236 (CanLII), 2014 -05-28, Superior Court of Justice — Ontario.

322 *Steen v. Islamic Republic of Iran*, 2013 ONCA 30 (CanLII), 21 -01 2013, Superior Court of Justice — Ontario.

323 *Bennett Estate v. Iran* (Islamic Republic of), 2013 ONCA 623 (CanLII), Superior Court of Justice — Ontario, 11-10-2013.

324 *H, WS v W,N* South Gauteng High Court, Case No 10142/12, Judgment: 30 January 2013, para [8]. Also see: *Social media evidence: How to find it and how to use it.* American Bar Association (ABA), Section of Litigation, ABA Annual Meeting, August 8 – 12, 2013, San Francisco, California. *Griffin v. State* 419 Md. 343, 19 A.3d 415 (2011). *Griffin v. State*: Setting the Bar Too High for Authenticating Social Media Evidence, Brendan W. Hogan, University of Maryland Francis King Carey School of Law, 2012 http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1020&context=endnotes

325 Swanson, C. R., Chamelin, N. C., Territo, L., & Taylor, R. W. (2006). *Criminal Investigation* (9th ed.). New York: McGraw-Hill.

326 Ibid.

327 Casey, E. (2004). *Digital Evidence and Computer Crime* (2nd ed.). London: Academic Press.

328 Association of Chief Police Officers. (2003). Good Practice Guide for Computer-Based Electronic Evidence. London: Association of Chief Police Officers.

329 Casey, E. (2004). *Digital Evidence and Computer Crime* (2nd ed.). London: Academic Press.

330 Ibid.

331 Swanson, C. R., Chamelin, N. C., Territo, L., & Taylor, R. W. (2006). *Criminal Investigation* (9th ed.). New York: McGraw-Hill.

332 Casey, E., & Rose, C. W. (2010). Forensic Analysis. In E. Casey (Ed.), *Handbook of Digital Forensics and Investigation* (pp. 21-62). London: Academic Press.

333 RILEY v. CALIFORNIA ,US Supreme Court, Judgment: 25 June 2014.

334 Jones, A., & Valli, C. (2009). *Building a Digital Forensic Laboratory*. Burlington: Syngress.

335 *Motata v Nair N.O. & Another* 2009 (1) SACR 263 (T)

336 Also see Human Rights' Electronic Evidence Study, Final report February 2012, The Centre for Research Library, Global Resource Network, from the John D. and Katherine T. MacArthur Foundation

337 Association of Chief Police Officers. (2003). *Good Practice Guide for Computer-Based Electronic Evidence*. London: Association of Chief Police Officers.

338 Jones, A., & Valli, C. (2009). *Building a Digital Forensic Laboratory*. Burlington: Syngress.

339 Pollitt, M. (2008). Applying Traditional Forensic Taxonomy to Digital Forensics. In S. Shenoi (Ed.), *Advances in Digital Forensics* (pp. 17-26). Boston: Springer.

340 Rogers, M. K., & Seigfried, K. (2004). The Future of Computer Forensics: A Needs Analysis Approach. *Computers & Security,* 43 (2), 12-16.

341 Carrier, B. (2005). *File System Forensics.* Upper Saddle River: Addison-Wesley.

342 National Research Council. (2009). *Strengthening Forensic Science in the United States: A Path Forward*. Washington DC: National Academies Press.

343 Vacca, J. R. (2005). *Computer Forensics: Computer Crime Scene Investigation* (2nd ed.). Boston: Thomson.

344 Swanson, C. R., Chamelin, N. C., Territo, L., & Taylor, R. W. (2006). *Criminal Investigation* (9th ed.). New York: McGraw-Hill.

345 McKemmish, R. (2008). When is Digital Evidence Forensically Sound? In I. Ray, & S. Shenoi (Eds.), *Advances in Digital Forensics* IV (pp. 3-15). Boston: Springer.

346 Pollitt, M. (2008). Applying Traditional Forensic Taxonomy to Digital Forensics. In S. Shenoi (Ed.), *Advances in Digital Forensics* (pp. 17-26). Boston: Springer.

347 Vacca, J. R. (2005). *Computer Forensics: Computer Crime Scene Investigation* (2nd ed.). Boston: Thomson.

348 Casey, E., & Rose, C. W. (2010). Forensic Analysis. In E. Casey (Ed.), *Handbook of Digital Forensics and Investigation* (pp. 21-62). London: Academic Press.

Bibliography

Part 1

Atran, S. Mishandling suicide terrorism. *The Washington Quarterly* 27: 3, 2004.

Atran, S. The moral logic and growth of suicide terrorism. *The Washington Quarterly* 29: 2, 2006.

Beyler, Clara. Messengers of death: female suicide bombers. International Institute for Counter-Terrorism Research Paper, 12 February 2003, 1. Available at http://www.ict.org.il/articles/articledet.cfm?articleid=470.

Blachard, CM. Al Qaeda: statements and evolving ideology. CRS Report for Congress, 26 January 2006.

Botha, A. Political dissent and terrorism in Southern Africa. Institute for Security Studies (ISS), Paper 90, 2004.

Botha, A. Politics and terrorism: an assessment of the origin and threat of terrorism in Egypt. ISS, Paper 131, 2006.

Botha, A. *Terrorism in the Maghreb: transnationalisation of domestic terrorism.* ISS, Monograph 144, 2008.

Chaliand, Gerard and Blin, Arnaud. *The history of terrorism: from antiquity to al Qaeda.* Berkeley: University of California Press, 2007.

Club de Madrid Series on Democracy and Terrorism. *Addressing the causes of terrorism,* Vol. 1. The International Summit on Democracy, Terrorism and Security, 8–11 March 2005.

Club de Madrid Series on Democracy and Terrorism. *Towards a democratic response,* Vol. 3. The International Summit on Democracy, Terrorism and Security, 8–11 March 2005.

Courson, E. MEND: political marginalization, repression, and petro-insurgency in the Niger Delta. *African Security,* 4:1, 2011.

Cragin, K and Chalk, P. Terrorism and development: using social and economic development to inhibit resurgence of terrorism. RAND Corporation, 2003.

Cragin, K and Daly, SA. The dynamic terrorist threat: an assessment of group motivations and capabilities in a changing world. RAND Corporation, 2004.

Cronin, Audrey Kurth. Terrorists and suicide attacks. Washington DC: Congressional Research Service Report for Congress, 28 August 2003.

Davis, LE. Globalisation's security implications. RAND Corporation, 2003.

Dickson, D. Political Islam in sub-Saharan Africa: the need for a new research and diplomatic agenda. United States Institute of Peace, 2005.

Drake, CJM. The role of ideology in terrorists' target selection. *Terrorism and Political Violence,* 10:2, 1998.

Echevarria, AJ. Fourth-generation war and other myths. Strategic Studies Institute, 2005.

Ellis, JO. Terrorism: what's coming: the mutating threat. Memorial Institute for the Prevention of Terrorism, 2007.

Enders, W and Sandler, T. Patterns of transnational terrorism, 1970–99: alternative time series estimates, *International Time Series Quarterly,* 46:2, 2002.

Enders, W and Sandler, T. What do we know about the substitution effect in transnational terrorism?, in Silke A (ed.), *Researching terrorism: trends, achievements, failures.* Ilford: Frank Cass, 2004.

Fighel, Yoni. Palestinian Islamic Jihad and female suicide bombers, ICT, Research Paper, 6 October 2003, 1. Available at http://www.ict.org.il/articles/articledet.cfm?articleid=499.

Forum on Early Warning and Early Response. Responding to terrorism: implications for regional and global stability, 30 September 2001.

Fox, J. Religion and state failure: an examination of the extent and magnitude of religious conflict from 1950 to 1996. *International Political Science Review,* 25:1, 2004.

Ganor, Boaz. Suicide terrorism: an overview. International Policy Institute for Counter-Terrorism, Article, 15 February 2000.

Ganor, Boaz. *The counter-terrorism puzzle: a guide for decision makers.* London: Transaction Publishers, 2008.

Ganor, Boaz. The first Iraqi suicide bombing: a hint of things to come?. International Policy Institute for Counter-Terrorism, Article, 30 March 2003, 1. Available at http://www.ict.org.il/articles/articledet.cfm?articleid=477. Global Witness. For a few dollars more: how al Qaeda moved into the diamond trade, April 2003.

Grau, LW. Guerrillas, terrorists and intelligence analysis. *Military Review,* July/August 2004.

Gulf Research Centre. Security & terrorism: suicide bombing operations, 5, March 2007.

Gunaratna, Rohan. Suicide terrorism: a global threat. In Suicide terrorism in Sri Lanka. IPCS, Research Paper 5, August 2004.

Hafez, MM. Martyrdom mythology in Iraq: how Jihadists frame suicide terrorism in videos and biographies. *Terrorism and Political Violence,* 19:5, 2007.

Hall, JR. *Religion and violence: social processes in comparative perspective.* University of California, 2001.

Hartman, WJ. *Globalisation and asymmetric warfare.* Air Command and Staff College Air University, 2002.

Hoffman, Bruce. *Inside terrorism.* New York: Columbia University Press, 1998.

Hoffman, Bruce. Lessons of 9/11: testimony submitted to the committee record to the US Joint 11 September 2001 Inquiry Staff of the House and Senate Select Committees on Intelligence on 8 October 2002. Arlington: RAND, 8 October 2002.

Hoffman, Bruce. The logic of suicide terrorism. In Howard, Russell D and Sawyer, Reid L. *Terrorism and counter-terrorism: understanding the new security environment.* Guilford: McGraw-Hill/ Dushkin, 2004.

Hunt, E. Islamist terrorism in northwestern Africa: a 'thorn in the neck' of the United States?. *Policy Focus,* 65, 2007.

Hudson, RA. The sociology and psychology of terrorism: who becomes a terrorist and why?. The Library of Congress, 1999.

Iannaccone, LR and Berman, E. Religious extremism: the good, the bad, and the deadly. Institute for Security Technology Studies, 2002.

International Policy Institute for Counter-Terrorism. Female suicide bombers – an update, 7 March 2004. Available at http://www.ict.org.il/articles/articledet.cfm?articleid=508.

International Coordination for Cyber Crime and Terrorism in the 21st Century.

Available at http://www.stealth-iss.com/documents/pdf/stanford_whitepaper-V6.pdf

International Crisis Group. Islamism in North Africa 1: the legacies of history, 20 April 2004.

International Crisis Group. Islamism in North Africa 2: Egypt's opportunity, 20 April 2004.

International Crisis Group. Counter-terrorism in Somalia: losing hearts and minds?. Africa Report 95, 11 July 2005.

International Crisis Group. Islamist terrorism in the Sahel: fact or fiction?. Africa Report 92, 2005.

International Bank for Reconstruction and Development. *A decade of measuring the quality of governance: Governance Matters 2006.* Worldwide Governance Indicators, 2006.

International Organisation for Migration. International terrorism and migration, 2003.

Israeli Ministry of Foreign Affairs. Suicide terror: its use and rationalization, website, 23 July 2002. Available at http://www.mfa.gov.il/mfa/ go.asp? MFAH0m6k0.

Joshi, Charu Lata. Sri Lanka: suicide bombers. *Far Eastern Economic Review,* 1 June 2000, 2.

Jost, PM and Sandhu, HS. The Hawala alternative remittance system and its role in money laundering. Financial Crimes Enforcement Network, 2003.

Kimhi, Shaul and Even, Shmuel. Who are the Palestinian suicide terrorists?. *Strategic Assessment,* 6:2, September 2003, 7–9.

Lambakis, SJ. Reconsidering asymmetric warfare. *Joint Force Quarterly,* 36.

Lewis, JA. Assessing the risk of cyber terrorism, cyber war and other cyber threats. Center for Strategic and International Studies, 2002.

Lind, WS. Understanding fourth generation war. *Military Review,* September/October 2004.

Lutz, James M and Lutz, Brenda J. *Global terrorism.* London: Routledge, 2005.

Makarenko, T. Crime, terror and the Central Asian drug trade. *Harvard Asia Quarterly,* 6:3, 2002.

Makarenko, T. Terrorism and transnational organised crime: the emerging nexus. Transnational Violence and Seams of Lawlessness in the Asia Pacific: Linkages to Global Terrorism, Smith, P (ed), Honolulu: Asia Pacific Centre for Security Studies, 2002.

Martin, Gus. *Understanding terrorism: challenges, perspectives and issues.* London: Sage Publications, 2006.

Matthew, R and Shambaugh, G. The pendulum effect: explaining shifts in the democratic response to terrorism. *Analyses of Social Issues and Public Policy,* 5:1, 2005.

McAfee Virtual Criminology Report, Cybercrime: the next wave, 2007.

McCauley C, Moskalenko S and Van Son B. *Characteristics of lone-wolf violent offenders: a comparison of assassins and school attackers,* 7:1, 2013.

McComack, D. An African vortex: Islamism in sub-Sahara Africa. The Center for Security Policy, Occasional Paper 4, 2005.

Meigs, MC. Unorthodox thoughts about asymmetric warfare. *Parameters,* Summer 2003.

Metz, S and Johnson, DV. Asymmetry and US military strategy: definition, background and strategic concepts. Strategic Studies Institute, 2001.

Networks and Netwars: The Future of Terror, Crime, and Militancy. John Arquilla and David Ronfeldt (eds). RAND: National Defense Research Institute, 2001.

Nordas, R. State religiosity and civil war: how religious heterogeneity and the degree of separation between religion and state influence the risk of intrastate armed conflict. Norwegian University of Science and Technology, 2004.

Nunn, Sam. Thinking the inevitable: suicide attacks in America and the design of effective public safety policies. *Journal of Homeland Security and Emergency Management,* 1:4, Article 401, 2004.

Office for Democratic Institutions and Human Rights. Background paper on human rights considerations in combating incitement to terrorism and related offences. Vienna, 19–20 October 2006.

Office for Democratic Institutions and Human Rights. Protecting human rights while combating the use of the Internet for terrorist purposes. The Hague, 28–29 March 2006.

Okumu, W and Botha, A. Understanding terrorism in Africa: in search for an African voice. ISS, Seminar Report, 6–7 November 2006.

Okumu, W and Botha, A. Understanding terrorism in Africa: building bridges and overcoming the gaps. ISS, Seminar Report, 19–20 May 2007.

O'Neill, Bard E. *Insurgency and terrorism: inside modern revolutionary warfare.* Dulles: Brassey's, 1990.

Pape, Robert A. The strategic logic of suicide terrorism. *American Political Science Review,* 97:3, 2003.

Parry, Albert. *Terrorism: from Robespierre to the Weather Underground.* New York: Dover Publications, 1976.

Passas, N.: Fighting terror with error: The counter-productive regulation of informal value transfers. *Crime, Law and Social Change* 45 :4, 2006.

Paz, R and Terdman, M. Africa: the gold mine of al-Qaeda and global jihad. Intelligence and Terrorism Information Centre, Centre for Special Studies, 2006.

Porter, P. Shadow wars: asymmetric warfare in the past and future. *Security Dialogue,* 37:4, 2006.

Rabasa, AM et al. The Muslim world after 9/11. RAND Corporation, 2004.

Raman, B. Suicide & suicidal terrorism. South Asia Analysis Group, Paper 947, 12 March 2004. Available at http://www.saag.org/papers10/paper947.html.

Ramasubramanian, R. Suicide terrorism in Sri Lanka. IPCS, Research Paper 5, August 2004.

Record, J. Why the strong loose. *Parameters,* Winter 2005.

Rotberg, Robert I. *State failure and state weakness in a time of terror.* Washington DC: Brookings Institution Press, 2003.

Sageman, Marc. *Understanding terror networks.* Philadelphia: University of Pennsylvania Press, 2004.

Sageman, Marc. *Leaderless jihad: terror networks in the twenty-first century.* Philadelphia: University of Pennsylvania Press, 2008.

Schweitzer, Y and Ferber, SG. Al-Qaeda and the inter-nationalization of suicide terrorism. Jaffee Center for Strategic Studies, Tel Aviv University, 2005.

Schweitzer, Yoram. Suicide terrorism: development & characteristics. International Policy Institute for Counter-Terrorism, 21 April 2000. Available at http://www.ict.org.il/articles/articledet.cfm?articleid=112.

Sein, AJ. Confronting political violence: re-examining the influence of threat perception on policy responses to internal discord. Rice University Undergraduate Research Conference, 16–18 January 2004.

Shelley, LI. Organised crime, terrorism and cybercrime. Transnational Crime and Corruption Center, American University, 2002

Smith, RB. *Political extremism: left, center and right.* In I. L. Horowitz (Ed) Civil Society and Class Politics, Essays on the Political Sociology of Seymor Martin Lipset, New Brunswick: NJ, Transaction, 2004.

Steele, RD. The asymmetric threat: listening to the debate. *JFQ,* Autumn/Winter 1998.

Sprinzak, Ehud. Rational fanatics. *Foreign Policy,* 120, September/October 2000.

Suicide terrorism in comparative perspective. In *Countering suicide terrorism.* Herzilya: The International Policy Institute for Counter-Terrorism, Interdisciplinary Center, 2002.

Suicide terrorism: a global threat. *Jane's Intelligence Review,* 20 October 2000, 4. Available at http://www.janes.com/security/international_security/news/usscole/jir001020_1_n.shtml.

TNI Crime and Globalisation. Global enforcement regimes: transnational organised crime, international terrorism and money laundering. TNI Crime and Globalisation Seminar, Amsterdam, 28–29 April 2005.

United Nations Office on Drugs and Crime. *Forum on Crime and Society,* 4:1, 2 December 2004.

United States Institute of Peace. Islamic perspectives on peace and violence. Special Report, January 2002.

United States Institute of Peace. Islamic extremists: how do they mobilise support?. Special Report 89, July 2002.

United States Army Training and Doctrine Command. *A military guide to terrorism in the twenty-first century.* Fort Leavenworth, 2007.

US Army Training and Doctrine Command, Deputy Chief of Staff for Intelligence, Assistant Deputy Chief of Staff for Intelligence. DCSINT Handbook No. 1.03: Suicide bombing in the COE, August 2006.

Vatis, MA. Cyber attacks during the war on terrorism: a predictive analysis. Institute for Security Technology Studies, 2001.

Weimann, G. *www.terror.net: how modern terrorism uses the Internet.* United States Institute of Peace, Special Report 116, 2004.

World Bank and International Monetary Fund. Anti-money laundering and combating the financing of terrorism: Central and West Africa region. World Bank and IMF Global Dialogue Series, 2003.

Zabel, SE. The military strategy of global jihad. Strategic Studies Institute, 2007.

About the Africa Prosecutors Association

The Africa Prosecutors Association is a body of Prosecuting Services, Agencies and Authorities established to enhance cooperation and prosecutorial capacity in addressing serious and complex crimes in Africa. Through training and the sharing of best practices, the APA promotes peer-to-peer exchanges for harmonised, efficient and effective responses to complex and serious crimes.

About the ISS

The Institute for Security Studies is an African organisation that aims to enhance human security on the continent. It does independent and authoritative research, provides expert policy analysis and advice, and delivers practical training and technical assistance.

Acknowledgements

This guide was made possible with support from the United States Department of State. The ISS is also grateful for support from the members of the ISS Partnership Forum: the governments of Australia, Canada, Denmark, Finland, Japan, Netherlands, Norway, Sweden and the USA.

ISSN 1026-0404

9 771026 040004