UNODC
United Nations Office on Drugs and Crime

The use of the Internet
for terrorist purposes

In collaboration with the
UNITED NATIONS COUNTER-TERRORISM IMPLEMENTATION TASK FORCE

UNITED NATIONS OFFICE ON DRUGS AND CRIME
Vienna

THE USE OF THE INTERNET FOR TERRORIST PURPOSES

UNITED NATIONS
New York, 2012

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

"The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner."

Ban Ki-moon
Secretary-General of the United Nations

Foreword

Executive Director
United Nations Office on Drugs and Crime

The use of the Internet for terrorist purposes is a rapidly growing phenomenon, requiring a proactive and coordinated response from Member States.

The United Nations Office on Drugs and Crime (UNODC) plays a key role in providing assistance to Member States, in furtherance of its mandate to strengthen the capacity of national criminal justice systems to implement the provisions of the international legal instruments against terrorism, and does so in compliance with the principles of rule of law and international human rights standards. In particular, in 2011, the General Assembly, in its resolution 66/178, reaffirmed the mandate of UNODC to continue to develop specialized legal knowledge in the area of counter-terrorism and pertinent thematic areas, including the use of the Internet for terrorist purposes.

Despite increasing international recognition of the threat posed by terrorists' use of the Internet in recent years, there is currently no universal instrument specifically addressing this pervasive facet of terrorist activity. Moreover, there is limited specialized training available on the legal and practical aspects of the investigation and prosecution of terrorism cases involving the use of the Internet. The present publication complements the existing resources developed by UNODC in the areas of counter-terrorism, cybercrime and rule of law. It also addresses the importance of developing integrated, specialized knowledge to respond to the technical assistance needs of Member States in combating this continually evolving threat. UNODC is deeply grateful for the generous support of the Government of the United Kingdom of Great Britain and Northern Ireland, which made the publication of that work possible.

The publication, which is intended for use both as a stand-alone resource and in support of the capacity-building initiatives of UNODC, is aimed at providing guidance regarding current legal frameworks and practice at the national and international levels relating to the criminalization, investigation and prosecution of terrorist cases involving the Internet.

Terrorism, in all its manifestations, affects us all. The use of the Internet to further terrorist purposes disregards national borders, amplifying the potential impact on victims. By highlighting cases and best practices that respond to this unique challenge, the present publication has two aims: first, to promote a better understanding of the ways in which communications technologies may be misused in furtherance of acts of terrorism and, second, to increase collaboration among Member States, so that effective criminal justice responses to this transnational challenge can be developed.

Yury Fedotov
Executive Director
United Nations Office on Drugs and Crime

Secretary-General's
Counter-Terrorism Implementation Task Force

The Working Group on Countering the Use of the Internet for Terrorist Purposes of the Counter-Terrorism Implementation Task Force is aimed at coordinating the activities of the United Nations system in support of the United Nations Global Counter-Terrorism Strategy, adopted by the General Assembly in its resolution 60/288, in which Member States resolved to "coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet" and "use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard". The Working Group has identified three key themes for discussion: legal issues, technical issues and ways in which the international community might use the Internet more effectively to counter terrorism by exposing the fallacy of the terrorist message that violence is a legitimate way to effect political change.

The present study, produced by the United Nations Office on Drugs and Crime and conducted within the framework of the Working Group, owes much to the contribution and support of Member States. It takes discussion of the legal challenges to the next stage and adds significantly to the knowledge and expertise that the Working Group has accumulated and shared with Member States in that area. In particular, it provides important examples of Member State legislation dealing with terrorist use of the Internet and demonstrates, through real examples of legal cases, the difficulties faced by Member States in criminalizing and prosecuting such acts.

The Working Group is confident that the present report will help to identify the legislative areas in which the United Nations can assist in the implementation by Member States of the Global Counter-Terrorism Strategy in combating the use of the Internet for terrorist purposes.

Richard Barrett
Coordinator of the Analytical Support and Sanctions Monitoring Team
Co-Chair of the Counter-Terrorism Implementation Task Force Working Group on
Countering the Use of the Internet for Terrorist Purposes

Government of the United Kingdom

The United Kingdom has pioneered legislation to counter use of the Internet for terrorist purposes over the past decade; we have had considerable success in tackling online terrorist activity within the country's borders, while doing our utmost to uphold freedoms and benefits that the Internet has brought to our citizens.

However, we recognize that the threat is transnational by its very nature. Only by taking action together can the international community hope to tackle terrorist use of the Internet effectively.

The British Government therefore welcomes the opportunity to support UNODC in producing the publication that you are about to read. We hope that it will rapidly become a useful tool for legislators, law enforcement officials and criminal justice practitioners to develop and implement legal frameworks that will effectively disrupt terrorists' activities online. If so, it will make a valuable contribution to making our communities—both real and virtual—safer places.

Simon Shercliff
Head, Counter Terrorism (Ops)
Department Foreign and
Commonwealth Office

Sue Hemming OBE
Head of the Special Crime and Counter
Terrorism Division
Crown Prosecution Service

Contents

Background

Technology is one of the strategic factors driving the increasing use of the Internet by terrorist organizations and their supporters for a wide range of purposes, including recruitment, financing, propaganda, training, incitement to commit acts of terrorism, and the gathering and dissemination of information for terrorist purposes. While the many benefits of the Internet are self-evident, it may also be used to facilitate communication within terrorist organizations and to transmit information on, as well as material support for, planned acts of terrorism, all of which require specific technical knowledge for the effective investigation of these offences.

It is a commonly accepted principle that, despite the heinous nature of their acts, alleged terrorists should be afforded the same procedural safeguards under criminal law as any other suspects. The defence of human rights is a core value of the United Nations and a fundamental pillar of the rule-of-law approach to the fight against terrorism. The present publication accordingly highlights the importance of respect for the principles of human rights and fundamental freedoms at all times and, in particular, in the context of the development and implementation of legal instruments related to countering terrorism.

The United Nations Office on Drugs and Crime (UNODC), as a key United Nations entity for delivering counter-terrorism legal and related technical assistance, actively participates in the Counter-Terrorism Implementation Task Force, thus ensuring that the counter-terrorism work of UNODC is carried out in the broader context of, and coordinated with, United Nations system-wide efforts. In January 2010, the Task Force's Working Group on Countering the Use of the Internet for Terrorist Purposes initiated a series of conferences involving representatives from Governments, international and regional organizations, think tanks, academia and the private sector to evaluate the use of the Internet for terrorist purposes and potential means to counter such use. The objective of the Working Group initiative was to provide Member States with an overview of the current nature of the challenge and to propose policy guidelines, projects and practical guidance regarding legal, technical and counter-narrative aspects of the challenge. Working Group conferences were held in Berlin in January 2010, Seattle (United States of America) in February 2010 and Riyadh in January 2011.

In furtherance of its mandate "to develop specialized legal knowledge in the area of counter-terrorism … and to provide assistance to requesting Member States with regard to criminal justice responses to terrorism, including … the use of the Internet for terrorist purposes,"[1] the Terrorism Prevention Branch of UNODC, in collaboration with

[1] General Assembly resolution 66/178.

the Organized Crime and Illicit Trafficking Branch of UNODC and with the support of the Government of the United Kingdom of Great Britain and Northern Ireland, undertook to contribute to the Working Group project through the development of the current technical assistance tool on the use of the Internet for terrorist purposes. The current UNODC publication builds upon the conclusions of the Working Group conferences, and in particular the conference held in Berlin in January 2010, relating to Internet-specific legal aspects of terrorism.

In connection with the development of the present publication, UNODC convened two expert group meetings in Vienna, in October 2011 and February 2012, to provide a forum for counter-terrorism practitioners, from a geographically diverse group of Member States, to share their experiences relating to the use of the Internet for terrorist purposes. Experts from a total of 25 Member States participated in these meetings, including senior prosecutors, law enforcement officers and academics, as well as representatives from several intergovernmental organizations. The present publication draws heavily on the discussions and expertise shared during those meetings, and is intended to provide practical guidance to Member States to facilitate the more effective investigation and prosecution of terrorist cases involving the use of the Internet.

I. Use of the Internet for terrorist purposes

A. Introduction

1. Since the late 1980s, the Internet has proven to be a highly dynamic means of communication, reaching an ever-growing audience worldwide. The development of increasingly sophisticated technologies has created a network with a truly global reach, and relatively low barriers to entry. Internet technology makes it easy for an individual to communicate with relative anonymity, quickly and effectively across borders, to an almost limitless audience. The benefits of Internet technology are numerous, starting with its unique suitability for sharing information and ideas, which is recognized as a fundamental human right.[2] It must also be recognized, however, that the same technology that facilitates such communication can also be exploited for the purposes of terrorism. The use of the Internet for terrorist purposes creates both challenges and opportunities in the fight against terrorism.

B. Means by which the Internet is utilized for terrorist purposes

2. For the purposes of the present publication, a functional approach has been adopted regarding the classification of the means by which the Internet is often utilized to promote and support acts of terrorism. This approach has resulted in the identification of six sometimes overlapping categories: propaganda (including recruitment, radicalization and incitement to terrorism); financing; training; planning (including through secret communication and open-source information); execution; and cyberattacks. Each of these categories is addressed in greater detail below.

1. Propaganda

3. One of the primary uses of the Internet by terrorists is for the dissemination of propaganda. Propaganda generally takes the form of multimedia communications providing ideological or practical instruction, explanations, justifications or promotion of terrorist activities. These may include virtual messages, presentations, magazines, treatises, audio and video files and video games developed by terrorist organizations or sympathizers. Nevertheless, what constitutes terrorist propaganda, as opposed to legitimate advocacy of a viewpoint, is often a subjective assessment. Further, the dissemination of propaganda is generally not, in and of itself, a prohibited activity. One of the

[2] See, for example, International Covenant on Civil and Political Rights (General Assembly resolution 2200 A (XXI), annex), art. 19, para. 2.

basic tenets of international law is the protection of fundamental human rights, which include the right to freedom of expression (see discussion in section I.D below). This guarantees an individual the right to share an opinion or distribute content which may be considered objectionable by others, subject to certain limited exceptions. One commonly accepted exclusion with respect to that right is the prohibition against the distribution of certain categories of sexually explicit content, the prohibition of which is deemed to be in the public interest in order to protect certain vulnerable groups. Other exclusions, all of which must be provided for by law and shown to be necessary, may include communications that are clearly detrimental to the protection of national security and communications that are both intended and likely to incite acts of violence against individuals or specific groups of individuals.[3]

4. The promotion of violence is a common theme in terrorism-related propaganda. The broad reach of content distributed via the Internet exponentially increases the audience that may be affected. Further, the ability to directly distribute content via the Internet diminishes the reliance on traditional channels of communication, such as news services, which may take steps to independently evaluate the credibility of the information provided or to edit or omit aspects deemed to be unduly provocative. Internet propaganda may also include content such as video footage of violent acts of terrorism or video games developed by terrorist organizations that simulate acts of terrorism and encourage the user to engage in role-play, by acting the part of a virtual terrorist.

5. The promotion of extremist rhetoric encouraging violent acts is also a common trend across the growing range of Internet-based platforms that host user-generated content. Content that might formerly have been distributed to a relatively limited audience, in person or via physical media such as compact discs (CDs) and digital video discs (DVDs), has increasingly migrated to the Internet. Such content may be distributed using a broad range of tools, such as dedicated websites, targeted virtual chat rooms and forums, online magazines, social networking platforms such as Twitter and Facebook, and popular video and file-sharing websites, such as YouTube and Rapidshare, respectively. The use of indexing services such as Internet search engines also makes it easier to identify and retrieve terrorism-related content.

6. The fundamental threat posed by terrorist propaganda relates to the manner in which it is used and the intent with which it is disseminated. Terrorist propaganda distributed via the Internet covers a range of objectives and audiences. It may be tailored, inter alia, to potential or actual supporters or opponents of an organization or shared extremist belief, to direct or indirect victims of acts of terrorism or to the international community or a subset thereof. Propaganda aimed at potential or actual supporters may be focused on recruitment, radicalization and incitement to terrorism, through messages conveying pride, accomplishment and dedication to an extremist goal. It may also be used to demonstrate the effective execution of terrorist attacks to those who have provided financial support. Other objectives of terrorist propaganda may include the use of psychological manipulation to undermine an individual's belief in certain collective social

[3] Ibid., art. 19, para. 3.

values, or to propagate a sense of heightened anxiety, fear or panic in a population or subset of the population. This may be achieved through the dissemination of disinformation, rumours, threats of violence or images relating to provocative acts of violence. The intended audience may include direct viewers of content, as well as those affected by potential publicity generated by such material. With respect to the wider international community, the goal is often to convey a desire to achieve noble political ends.[4]

(a) Recruitment

7. The Internet may be used not only as a means to publish extremist rhetoric and videos, but also a way to develop relationships with, and solicit support from, those most responsive to targeted propaganda. Terrorist organizations increasingly use propaganda distributed via platforms such as password-protected websites and restricted-access Internet chat groups as a means of clandestine recruitment.[5] The reach of the Internet provides terrorist organizations and sympathizers with a global pool of potential recruits. Restricted access cyberforums offer a venue for recruits to learn about, and provide support to, terrorist organizations and to engage in direct actions in the furtherance of terrorist objectives.[6] The use of technological barriers to entry to recruitment platforms also increases the complexity of tracking terrorism-related activity by intelligence and law enforcement personnel.

8. Terrorist propaganda is often tailored to appeal to vulnerable and marginalized groups in society. The process of recruitment and radicalization commonly capitalizes on an individual's sentiments of injustice, exclusion or humiliation.[7] Propaganda may be adapted to account for demographic factors, such as age or gender, as well as social or economic circumstances.

9. The Internet may be a particularly effective medium for the recruitment of minors, who comprise a high proportion of users. Propaganda disseminated via the Internet with the aim of recruiting minors may take the form of cartoons, popular music videos or computer games. Tactics employed by websites maintained by terrorist organizations or their affiliates to target minors have included mixing cartoons and children's stories with messages promoting and glorifying acts of terrorism, such as suicide attacks. Similarly, some terrorist organizations have designed online video games intended to be used as recruitment and training tools. Such games may promote the use of violence against a State or prominent political figure, rewarding virtual successes, and may be offered in multiple languages to appeal to a broad audience.[8]

[4]Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, D.C., United States Institute of Peace Press, 2006), pp. 37-38.

[5]Scott Gerwehr and Sarah Daly, "Al-Qaida: terrorist selection and recruitment", in *The McGraw-Hill Homeland Security Handbook*, David Kamien, ed. (New York, McGraw-Hill, 2006), p. 83.

[6]Dorothy E. Denning, "Terror's web: how the Internet is transforming terrorism", in *Handbook of Internet Crime*, Yvonne Jewkes and Majid Yar, eds. (Cullompton, United Kingdom, Willan Publishing, (2010)), pp. 194-213.

[7]European Commission, Expert Group on Violent Radicalisation, "Radicalisation processes leading to acts of terrorism" (2008). Available from www.clingendael.nl/publications/2008/20080500_cscp_report_vries.pdf.

[8]Gabriel Weimann, "Online terrorists prey on the vulnerable", *YaleGlobal Online*, 5 March 2008. Available from http://yaleglobal.yale.edu/content/online-terrorists-prey-vulnerable.

(b) Incitement

10. While propaganda per se is not generally prohibited, the use of propaganda by terrorists to incite acts of terrorism is considered unlawful by many Member States. The Internet provides an abundance of material and opportunities to download, edit and distribute content that may be considered unlawful glorification of, or provocation to, acts of terrorism. It should be noted, however, that some intergovernmental and human rights mechanisms have expressed doubt that the concept of "glorification" of terrorism is sufficiently narrow and precise to serve as a basis for criminal sanctions compliant with the requirements of the principle of legality and the permissible limitations of the right to freedom of expression, as enshrined in articles 15 and 19 of the International Covenant on Civil and Political Rights.[9,10]

11. It is important to emphasize the distinction between mere propaganda and material intended to incite acts of terrorism. In several Member States, in order to be held liable for incitement to terrorism, a showing of the requisite intent and a direct causal link between alleged propaganda and an actual plot or execution of a terrorist act is required. For example, in a contribution to the expert group meetings, a French expert indicated that the dissemination of instructive materials on explosives would not be considered a violation of French law unless the communication contained information specifying that the material was shared in furtherance of a terrorist purpose.

12. Preventing and deterring incitement to terrorism in the interest of protecting national security and public order are legitimate grounds for limiting freedom of expression, as provided under article 19, paragraph 3, of the International Covenant on Civil and Political Rights. These grounds are also consistent with article 20, paragraph 2, of that Covenant, which requires States to prohibit any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. In the light of the fundamental nature of the right to freedom of expression, however, any restrictions on the exercise of this right must be both necessary and proportional to the threat posed. The right to freedom of expression is also linked to other important rights, including the rights to freedom of thought, conscience and religion, belief and opinion.[11]

(c) Radicalization

13. Recruitment, radicalization and incitement to terrorism may be viewed as points along a continuum. Radicalization refers primarily to the process of indoctrination that often accompanies the transformation of recruits into individuals determined to act with violence based on extremist ideologies. The process of radicalization often involves

[9] General Assembly resolution 2200 A (XXI), annex.

[10] See the following reports of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: A/65/258 (para. 46) and A/61/267 (para. 7); see also the report of the Special Rapporteur on the promotion and protection of the rights to freedom of opinion and expression, addendum on the tenth anniversary joint declaration: ten key challenges to freedom of expression in the next decade (A/HRC/14/23/Add.2).

[11] Office of the United Nations High Commissioner for Human Rights, "Human rights, terrorism and counter-terrorism", Fact Sheet No. 32 (Geneva, 2008), Chap. III, sect. H.

the use of propaganda, whether communicated in person or via the Internet, over time. The length of time and the effectiveness of the propaganda and other persuasive means employed vary depending on individual circumstances and relationships.

2. *Financing*

14. Terrorist organizations and supporters may also use the Internet to finance acts of terrorism. The manner in which terrorists use the Internet to raise and collect funds and resources may be classified into four general categories: direct solicitation, e-commerce, the exploitation of online payment tools and through charitable organizations. Direct solicitation refers to the use of websites, chat groups, mass mailings and targeted communications to request donations from supporters. Websites may also be used as online stores, offering books, audio and video recordings and other items to supporters. Online payment facilities offered through dedicated websites or communications platforms make it easy to transfer funds electronically between parties. Funds transfers are often made by electronic wire transfer, credit card or alternate payment facilities available via services such as PayPal or Skype.

15. Online payment facilities may also be exploited through fraudulent means such as identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes and auction fraud. An example of the use of illicit gains to finance acts of terrorism can be seen in the United Kingdom case against Younis Tsouli (see para. 114 below). Profits from stolen credit cards were laundered by several means, including transfer through e-gold online payment accounts, which were used to route the funds through several countries before they reached their intended destination. The laundered money was used both to fund the registration by Tsouli of 180 websites hosting Al-Qaida propaganda videos and to provide equipment for terrorist activities in several countries. Approximately 1,400 credit cards were used to generate approximately £1.6 million of illicit funds to finance terrorist activity.[12]

16. Financial support provided to seemingly legitimate organizations, such as charities, may also be diverted for illicit purposes. Some terrorist organizations have been known to establish shell corporations, disguised as philanthropic undertakings, to solicit online donations. These organizations may claim to support humanitarian goals while in fact donations are used to fund acts of terrorism. Examples of overtly charitable organizations used for terrorist ends include the innocuously named Benevolence International Foundation, Global Relief Foundation and the Holy Land Foundation for Relief and Development, all of which used fraudulent means to finance terrorist organizations in the Middle East. Terrorists may also infiltrate branches of charitable organizations, which they use as a cover to promote the ideologies of terrorist organizations or to provide material support to militant groups.[13]

[12] Written submission of expert from the United Kingdom.

[13] Maura Conway, "Terrorist 'use' of the Internet and fighting back", *Information & Security*, vol. 19 (2006), pp. 12-14.

3. Training

17. In recent years, terrorist organizations have increasingly turned to the Internet as an alternative training ground for terrorists. There is a growing range of media that provide platforms for the dissemination of practical guides in the form of online manuals, audio and video clips, information and advice. These Internet platforms also provide detailed instructions, often in easily accessible multimedia format and multiple languages, on topics such as how to join terrorist organizations; how to construct explosives, firearms or other weapons or hazardous materials; and how to plan and execute terrorist attacks. The platforms act as a virtual training camp. They are also used to share, inter alia, specific methods, techniques or operational knowledge for the purpose of committing an act of terrorism.

18. For example, *Inspire* is an online magazine allegedly published by Al-Qaida in the Arabian Peninsula with the stated objective of enabling Muslims to train for jihad at home. It contains a large amount of ideological material aimed at encouraging terrorism, including statements attributed to Osama Bin Laden, Sheikh Ayman al-Zawahiri and other well-known Al-Qaida figures. The fall 2010 edition included practical instructional material on how to adapt a four-wheel-drive vehicle to carry out an attack on members of the public and how a lone individual could launch an indiscriminate attack by shooting a gun from a tower. The publication even suggested a target city for such an attack, in order to increase the chances of killing a member of the Government.[14]

19. Instructional material available online includes tools to facilitate counter-intelligence and hacking activities and to improve the security of illicit communications and online activity through the use of available encryption tools and anonymizing techniques. The interactive nature of Internet platforms helps build a sense of community among individuals from different geographical locations and backgrounds, encouraging the creation of networks for the exchange of instructional and tactical material.

4. Planning

20. Many criminal justice practitioners have indicated that almost every case of terrorism prosecuted involved the use of Internet technology. In particular, planning an act of terrorism typically involves remote communication among several parties. A recent case from France, *Public Prosecutor v. Hicheur*,[15] illustrates how different forms of Internet technology may be used to facilitate the preparation of acts of terrorism, including via thorough communications within and between organizations promoting violent extremism, as well as across borders.

[14] Written submission of expert from the United Kingdom.

[15] Judgement of 4 May 2012, Case No. 0926639036 of the Tribunal de Grande Instance de Paris (14th Chamber/2), Paris.

Public Prosecutor v. Hicheur

In May 2012, a French court sentenced Adlène Hicheur, an Algerian-born French national, to five years of imprisonment for participation in a criminal conspiracy for the preparation of a terrorist act (under Article 421-1 et. seq. of the French Criminal Code), relating to acts that took place in France in 2008 and 2009.

The investigation implicating Hicheur, a nuclear physicist, was launched in early 2008 in connection with an e-mail communication containing jihadist content, which was sent to the website of the President of the French Republic and traced back to a member of Al-Qaida in the Islamic Maghreb (AQIM).

A preservation order issued in January 2009 enabled the authorities to identify e-mail exchanges between the AQIM member and, inter alia, the Global Islamic Media Front (GIMF) and the Rafidayin Center, a website with the stated goal of hosting and disseminating Al-Qaida documents, audio and video recordings, statements from warlords and suicide attackers and the materials of other extremist Islamic groups. The e-mail exchanges were encrypted using the dedicated software "Asrar el Mojahedeen" or "Mujahedeen Secrets", which includes 256-bit encryption, variable stealth cipher encryption keys, RSA 2,048-bit encryption keys and encrypted chat-forum-supported instant messaging.

Dozens of decrypted e-mail communications were presented at trial. The prosecution claimed that the content of those e-mails indicated that Hicheur actively performed, inter alia, the following acts in support of the jihadist network, notably on behalf of the Rafidayin Center:

- Translated, encrypted, compressed and password-protected pro-jihadist materials, including documents and videos, which he then uploaded and circulated via the Internet
- Distributed the encryption software "Mujahedeen Secrets" to facilitate covert Internet communications
- Conspired with an AQIM member to organize and coordinate pro-jihadist activities, including but not limited to providing financial support to the jihadist cause, disseminating pro-jihadist information and supporting the creation of an operational unit in Europe, and in particular in France, to potentially prepare terrorist attacks
- Acted as moderator on the pro-jihadist Ribaat website
- Took concrete steps to provide financial support to AQIM, including through the attempted use of PayPal and other virtual payment systems.

At trial, the prosecution claimed that those communications proved Hicheur had been fully aware that he was engaging with a member of AQIM, and that he had acted knowingly and willingly as an intermediary between jihadist fighters and GIMF. At the conclusion of the trial, the Court held that; "Hicheur became … a logistical and media support for this terrorist structure for which the 'media jihad' is crucial".

The Court further held that "Adlène Hicheur, by giving his agreement to the establishment of an operational unit linked to AQIM in Europe, or even in France, and determining targets or categories of targets to be struck, participated in a group [AQIM] specifically created to prepare acts of terrorism."

The court therefore found sufficient evidence to demonstrate, as required under the French Criminal Code, that Hicheur had provided not merely intellectual support but also direct logistical support to a clearly identified terrorist plan. The decision of the court is appealable.

Sources: Judgement of 4 May 2012 of the Tribunal de Grande Instance de Paris; and Tung, Liam, *Jihadists get world-class encryption kit* (29 January 2008), available from www.zdnet.com.au/jihadists-get-world-class-encryption-kit-339285480.htm.

21. Steps may also be taken via the Internet to identify a potential target of an attack and the most effective means of achieving the terrorist purpose. These preparatory steps may range from obtaining instructions on recommended methods of attack to collecting open-source and other information regarding a proposed target. The ability of the Internet to bridge distances and borders, and the vast amount of information publicly available in cyberspace, make the Internet a key tool in the planning of terrorist acts.

(a) Preparatory secret communication

22. The most basic function of the Internet is to facilitate communication. Terrorists have become increasingly sophisticated at exploiting communications technologies for anonymous communication related to the planning of terrorist acts. A simple online e-mail account may be used by terrorists for electronic, or virtual, "dead dropping" of communications. This refers to the creation of a draft message, which remains unsent, and therefore leaves minimal electronic traces, but which may be accessed from any Internet terminal worldwide by multiple individuals with the relevant password.

23. There is also an abundance of more sophisticated technologies that increase the difficulty of identifying the originator, recipient or content of Internet communications. Encryption tools and anonymizing software are readily available online for download. These tools may, inter alia, mask the unique Internet Protocol (IP) address that identifies each device used to access the Internet and its location, reroute Internet communications via one or more servers to jurisdictions with lower levels of enforcement against terrorist activity and/or encrypt traffic data relating to websites accessed. Steganography, the hiding of messages in images, may also be used.

(b) Publicly available information

24. Organizations and individuals often publish extensive amounts of information on the Internet. In the case of organizations, this may be a result in part of a desire to promote their activities and streamline their interaction with the public. Some sensitive information that may be used by terrorists for illicit purposes is also made available through Internet search engines, which may catalogue and retrieve inadequately protected information from millions of websites. Further, online access to detailed logistical information, such as real-time closed-circuit television footage, and applications such as Google Earth, which is intended for and primarily used by individuals for legitimate ends, may be misused by those intent on benefiting from the free access to

high-resolution satellite imagery, maps and information on terrain and buildings for the reconnaissance of potential targets from a remote computer terminal.

25. Particularly in the age of popular social networking media, such as Facebook, Twitter, YouTube, Flickr and blogging platforms, individuals also publish, voluntarily or inadvertently, an unprecedented amount of sensitive information on the Internet. While the intent of those distributing the information may be to provide news or other updates to their audience for informational or social purposes, some of this information may be misappropriated and used for the benefit of criminal activity.

5. Execution

26. Elements of the categories described above may be employed in the use of the Internet for the execution of terrorist acts. For example, explicit threats of violence, including in relation to the use of weapons, may be disseminated via the Internet to induce anxiety, fear or panic in a population or subset of the population. In many Member States, the act of issuing such threats, even if unfulfilled, may be deemed an offence. For example, in China, the fabrication of a threat and/or the circulation of a threat that is known to be fabricated in relation to the use of bombs or biological, chemical, or radioactive materials or other weapons, when committed with the intent "to seriously disrupt public order", is criminalized under domestic legislation.[16] Internet communications may also be used as a means to communicate with potential victims or to coordinate the execution of physical acts of terrorism. For example, the Internet was used extensively in the coordination of participants in the attacks of 11 September 2001 in the United States.

27. The use of the Internet in furtherance of the execution of acts of terrorism may, inter alia, offer logistical advantages, reduce the likelihood of detection or obscure the identity of responsible parties. Internet activity may also facilitate the acquisition of items necessary for the execution of the attack. Terrorists may purchase individual components or services required to perpetrate violent acts of terrorism by means of electronic commerce. Misappropriated credit cards or other forms of compromised electronic payment may be used to finance such purchases.

6. Cyberattacks

28. A cyberattack generally refers to the deliberate exploitation of computer networks as a means to launch an attack. Such attacks are typically intended to disrupt the proper functioning of targets, such as computer systems, servers or underlying infrastructure, through the use of hacking, advanced persistent threat techniques, computer viruses, malware,[17] phlooding[18] or other means of unauthorized or malicious access. Cyberattacks

[16] Written submission of expert from China.

[17] Pursuant to the International Telecommunication Union Toolkit for Cybercrime Legislation, section 1 *(n)*, malware may be defined as a program that is inserted into a computer program or system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the computer program, data or system.

[18] "Phlooding" refers to the targeting of the central authentication servers of an organization with multiple simultaneous authentication requests, with the aim of overloading the servers, resulting in a distributed denial of service.

may bear the characteristics of an act of terrorism, including the fundamental desire to instil fear in furtherance of political or social objectives. An example of a cyberattack was seen in Israel in January 2012, involving the targeting of multiple symbolic Israeli websites, such as the websites of the Tel Aviv Stock Exchange and the national airline, and the unauthorized disclosure of the credit card and account details of thousands of Israeli nationals.[19] While a considerable amount of attention has focused in recent years on the threat of cyberattacks by terrorists, that topic is beyond the scope of the present publication and, as such, will not be a subject of analysis.

C. Uses of the Internet for countering terrorist activity

29. While terrorists have developed many ways to use the Internet in furtherance of illicit purposes, their use of the Internet also provides opportunities for the gathering of intelligence and other activities to prevent and counter acts of terrorism, as well as for the gathering of evidence for the prosecution of such acts. A significant amount of knowledge about the functioning, activities and sometimes the targets of terrorist organizations is derived from website, chat room and other Internet communications. Further, increased Internet use for terrorist purposes provides a corresponding increase in the availability of electronic data which may be compiled and analysed for counter-terrorism purposes. Law enforcement, intelligence and other authorities are developing increasingly sophisticated tools to proactively prevent, detect and deter terrorist activity involving use of the Internet. The use of traditional investigative means, such as dedicated translation resources for the timely identification of potential terrorist threats, is also expanding.

30. Online discussions provide an opportunity to present opposing viewpoints or to engage in constructive debate, which may have the effect of discouraging potential supporters. Counter-narratives with a strong factual foundation may be conveyed through online discussion forums, images and videos. Successful messages may also demonstrate empathy with the underlying issues that contribute to radicalization, such as political and social conditions, and highlight alternatives to violent means of achieving the desired outcomes.[20] Strategic communications that provide counter-narratives to terrorist propaganda may also be disseminated via the Internet, in multiple languages, to reach a broad, geographically diverse audience.

31. The Center for Strategic Counterterrorism Communications, based in the United States, offers an example of a recently launched inter-agency initiative which is aimed at reducing radicalization and extremist violence by identifying in a timely manner extremist propaganda, inter alia, on the Internet and responding swiftly with targeted

[19] See Isabel Kershner, "Cyberattack exposes 20,000 Israeli credit card numbers and details about users", *New York Times*, 6 January 2012; and "2 Israeli web sites crippled as cyberwar escalates", *New York Times*, 16 January 2012.

[20] Counter-Terrorism Implementation Task Force Working Group on Use of the Internet for Terrorist Purposes, "Conference summary and follow-up/recommendations" of the Conference on the Use of the Internet to Counter the Appeal of Extremist Violence, held in Riyadh from 24 to 26 January 2011. Available from www.un.org/en/terrorism/ctitf/pdfs/ctitf_riyadh_conference_summary_recommendations.pdf.

counter-narratives via a wide range of communications technologies, including digital tools.[21] For instance, in May 2012, the Center was cited as having responded, within 48 hours, to banner advertisements promoting extremist violence posted on various websites by Al-Qaida in the Arabian Peninsula, with counter-advertisements on the same websites featuring an altered version of that same message that was intended to convey that the victims of the terrorist organization's activities were Yemeni nationals. The counter-narrative campaign involved cooperation among the United States Department of State, the intelligence community and the military. The Center also uses media platforms such as Facebook and YouTube for counter-narrative communications.[22,23]

D. Rule-of-law considerations

32. Respect for human rights and the rule of law is an integral part of the fight against terrorism. Due care must be taken to respect international human rights standards in all phases of counter-terrorism initiatives, from preventive intelligence gathering to ensuring due process in the prosecution of suspects. This requires the development of national counter-terrorism legislation and practices that promote and protect fundamental human rights and the rule of law.[24]

33. States have both a right and a duty to take effective measures to counter the destructive impact of terrorism on human rights, in particular the rights to life, liberty and physical integrity of individuals and the territorial integrity and security of States. Effective counter-terrorism measures and the protection of human rights are complementary and mutually reinforcing objectives which must be pursued together.[25] Counter-terrorism initiatives relating to Internet use may have an impact on the enjoyment of a range of human rights, including the rights to freedom of speech, freedom of association, privacy and a fair trial. While a comprehensive analysis of human rights issues is beyond the scope of the present publication, it is important to highlight key areas for consideration.

34. As noted in subsection B.1*(b)* above, the proscription of incitement to terrorism may involve restrictions on freedom of expression. Freedom of expression is not an absolute right. It may be restricted, subject to satisfaction of strictly construed tests of legality, necessity, proportionality and non-discrimination, when that freedom is used to incite discrimination, hostility or violence. A key difficulty in cases of glorification or incitement to terrorism is identifying where the line of acceptability lies, as

[21] Executive Order 13584 of 9 September 2011, "Developing an Integrated Strategic Counterterrorism Communications Initiative and Establishing a Temporary Organization to Support Certain Government-wide Communications Activities Directed Abroad", *Federal Register*, vol. 76, No. 179, 15 September 2011.

[22] "United States State Department fights al-Qaeda in cyberspace", *Al Jazeera* (25 May 2012). Available from http://blogs.aljazeera.com/americas/2012/05/25/us-state-department-fights-al-qaeda-cyberspace.

[23] "U.S. uses Yemeni web sites to counter al-Qaeda propaganda", *The Washington Post* (24 May 2012). Available from www.washingtonpost.com/world/national-security/us-hacks-web-sites-of-al-qaeda-affiliate-in-yemen/2012/05/23/gJQAGnOxlU_story.html.

[24] Office of the United Nations High Commissioner for Human Rights, Fact Sheet No. 32, chap. III, sect. H.

[25] Ibid., chap. I, sect. C.

this varies greatly from country to country depending on differing cultural and legal histories.[26] The right to freedom of association is similarly a qualified right, which may be subject to narrowly construed limitations and derogations.

35. Countering terrorist use of the Internet may involve the surveillance and collection of information relating to suspects. Due regard should be given to protecting persons against arbitrary or unlawful interference with the right to privacy,[27] which includes the right to privacy of information about an individual's identity as well as his or her private life. Domestic laws must be sufficiently detailed regarding, inter alia, the specific circumstances in which such interference may be permitted. Appropriate safeguards must also be in place to prevent abuse of secret surveillance tools. Further, any personal data collected must be adequately protected to ensure against unlawful or arbitrary access, disclosure or use.[28]

36. Guaranteeing due process rights is critical for ensuring that counter-terrorism measures are effective and respect the rule of law. Human rights protections for all persons charged with criminal offences, including terrorism-related crimes, include the right to be presumed innocent, the right to a hearing with due guarantees and within a reasonable time by a competent, independent and impartial tribunal and the right to have a conviction and sentence reviewed by a higher tribunal that meets the same standards.[29]

37. For a more detailed analysis of the issues highlighted in the present section and other relevant considerations, please see, for example, Fact Sheet No. 32 of the Office of the United Nations High Commissioner for Human Rights on "Human rights, terrorism and counter-terrorism", the report of the United Nations High Commissioner for Human Rights on the protection of human rights and fundamental freedoms while countering terrorism (A/HRC/16/50) and the following reports of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: ten areas of best practices in countering terrorism (A/HRC/16/51); and compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight (A/HRC/14/46).

[26] Organization for Security and Co-operation in Europe, Office for Democratic Institutions and Human Rights, "Human rights considerations in combating incitement to terrorism and related offences", background paper prepared for the expert workshop on "Preventing terrorism: fighting incitement and related terrorist activities", held in Vienna on 19 and 20 October 2006, sects. 3 and 4.

[27] See International Covenant on Civil and Political Rights, art. 17.

[28] "Human rights, terrorism and counter-terrorism", chap. III, sect. J.

[29] Ibid., chap. III, sect. F.

II. The international context

A. Introduction

38. Terrorist use of the Internet is a transnational problem, requiring an integrated response across borders and among national criminal justice systems. The United Nations plays a pivotal role in this regard, facilitating discussion and the sharing of good practices among Member States, as well as the building of consensus on common approaches to combating the use of the Internet for terrorist purposes.

39. The applicable international legal framework related to counter-terrorism is contained in a range of sources, including resolutions of the General Assembly and the Security Council, treaties, jurisprudence and customary international law. Security Council resolutions may impose legally binding obligations on Member States or provide "soft law" sources of political commitments or emerging norms of international law. Council resolutions adopted under Chapter VII of the Charter of the United Nations are binding on all Member States. The General Assembly has also adopted a number of resolutions relating to terrorism which provide useful sources of soft law and have high political importance, even though they are not legally binding.[30]

40. Legal obligations are also imposed upon States pursuant to bilateral and multilateral instruments addressing terrorism. "Universal" legal instruments are agreements that are open for ratification or accession by all Member States of the United Nations. By contrast, agreements promulgated by regional or other inter-State groupings may be open to only a limited group of potential signatories; such treaty-based obligations are binding only upon those States which choose to become a party to the agreements.

41. The duty to bring perpetrators of acts of terrorism to justice rests primarily with domestic authorities, as international tribunals do not generally have jurisdiction over such acts.[31] United Nations resolutions, universal legal instruments, regional agreements and model laws against terrorism play a key role in establishing common standards accepted across multiple jurisdictions.

[30] See United Nations Office on Drugs and Crime, Frequently Asked Questions on International Law Aspects of Countering Terrorism (2009). Available from www.unodc.org/documents/terrorism/Publications/FAQ/English.pdf.

[31] The Special Tribunal for Lebanon, established pursuant to Security Council resolution 1757 (2007), is currently the only international court with limited jurisdiction over the crime of terrorism.

B. United Nations counter-terrorism resolutions

42. The United Nations Global Counter-Terrorism Strategy[32] was unanimously adopted by the General Assembly in 2006, representing a milestone in the domain of multilateral counter-terrorism initiatives. Pursuant to the Strategy, Member States resolved, inter alia:

(a) To consistently, unequivocally and strongly condemn terrorism in all its forms and manifestations, committed by whomever, wherever and for whatever purposes, as it constitutes one of the most serious threats to international peace and security;

(b) To take urgent action to prevent and combat terrorism in all its forms and manifestations;

(c) To recognize that international cooperation and any measures that [they] undertake to prevent and combat terrorism must comply with [their] obligations under international law, including the Charter of the United Nations and relevant international conventions and protocols, in particular human rights law, refugee law and international humanitarian law;

(d) To work with the United Nations with due regard to confidentiality, respecting human rights and in compliance with other obligations under international law, to explore ways and means to "*(a) Coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet; (b) Use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard*" [emphasis added].

43. Several Security Council resolutions adopted in recent years require States to cooperate fully in the fight against terrorism, in all its forms. In particular, resolutions 1373 (2001) and 1566 (2004), adopted under Chapter VII of the Charter of the United Nations, require legislative and other action to be taken by all Member States to combat terrorism, including through increased cooperation with other Governments in the investigation, detection, arrest, extradition and prosecution of those involved in terrorist acts; and call upon States to implement the international conventions and protocols relating to terrorism.

44. Another key Security Council resolution relating to terrorist activity that may be conducted by means of the Internet is resolution 1624 (2005), which addresses the incitement and glorification of terrorist acts. In its fourth preambular paragraph, the Council condemns "in the strongest terms the incitement of terrorist acts "and repudiates" attempts at the justification or glorification (*apologie*) of terrorist acts that may incite further terrorist acts". In paragraph 1, it calls upon all States to adopt such measures as may be necessary and appropriate, and in accordance with their obligations under international law, to prohibit by law and prevent incitement to commit a terrorist act or acts.

[32] General Assembly resolution 60/288.

45. Recent United Nations reports and resolutions have specifically acknowledged the importance of countering terrorist use of the Internet as a key part of a comprehensive counter-terrorism strategy. In his 2006 report to the General Assembly entitled "Uniting against terrorism: recommendations for a global counter-terrorism strategy",[33] the Secretary-General explicitly stated: "The ability to generate and move finances, to acquire weapons, to recruit and train cadres, and to communicate, particularly through use of the Internet, are all essential to terrorists."[34] The Secretary-General went on to assert that the Internet was a rapidly growing vehicle for terrorist recruitment and dissemination of information and propaganda, which must be countered through coordinated action by Member States, while respecting human rights and other obligations under international law.[35]

46. In its resolution 1963 (2010), the Security Council expressed "concern at the increased use, in a globalized society, by terrorists of new information and communications technologies, in particular the Internet, for the purposes of the recruitment and incitement as well as for the financing, planning and preparation of their activities." The Council also recognized the importance of cooperation among Member States to prevent terrorists from exploiting technology, communications and resources.

C. Universal counter-terrorism legal instruments

47. Since 1963, the international community has been developing universal legal instruments to prevent terrorist acts under the auspices of the United Nations and its specialized agencies, in particular the International Civil Aviation Organization and the International Maritime Organization, and the International Atomic Energy Agency. The universal counter-terrorism instruments represent a major element of the global regime against terrorism and an important framework for international cooperation in countering terrorism. These universal legal instruments cover acts ranging from the hijacking of aircraft to nuclear terrorism by individuals and groups[36] and require the States that adopt them to criminalize the most foreseeable terrorist acts in the areas covered by the conventions. Nevertheless, these universal legal instruments are legally binding only on the signatories thereto,[37] which are also responsible for enforcing the provisions through the domestic criminal justice systems.

48. As a result of the attention focused on countering terrorism following the adoption of Security Council resolution 1373 (2001), in which the Council called on

[33] A/60/825.

[34] Ibid., para. 38.

[35] Ibid., paras. 58 and 60.

[36] Other covered terrorist acts include acts of aviation sabotage, acts of violence at airports, acts against the safety of maritime navigation, acts against the safety of fixed platforms located on the continental shelf, crimes against internationally protected persons (such as the kidnapping of diplomats), acts of unlawful taking and possession of nuclear material, acts of hostage-taking, acts of terrorist bombings and acts of funding of the commission of terrorist acts and terrorist organizations.

[37] For a list of the current ratification status of these universal legal instruments, please see www.unodc.org/tldb/universal_instruments_NEW.html.

Member States to become parties to the universal counter-terrorism legal instruments, the rate of adherence to these instruments has increased significantly. As at June 2011, two thirds of Member States had either ratified or acceded to at least 10 of the 16 universal counter-terrorism instruments.[38]

49. There is currently no comprehensive United Nations treaty on terrorism that is applicable to an exhaustive list of the manifestations of terrorism. Similarly, the international community has yet to agree on an internationally binding definition of the term "terrorism",[39] owing largely to the difficulty of devising a universally acceptable legal categorization for acts of violence committed by States, by armed groups such as liberation or self-determination movements or by individuals.

50. Member States have been engaged since 2000 in negotiations relating to a comprehensive counter-terrorism convention, which will ultimately include a definition of terrorism. Faced, however, with the difficulty of reaching consensus on a single, globally accepted definition of what constitutes terrorism, progress has instead been made through the existing universal legal instruments, which have developed along sectoral lines. These instruments focus on criminalizing specific "terrorist acts" without defining the broader concept of terrorism.

51. The universal instruments do not define terrorist offences as crimes under international law. Rather, they create an obligation for States parties to the agreements to criminalize the specified unlawful conduct under their domestic law, exercise jurisdiction over offenders under prescribed conditions and provide for international cooperation mechanisms that enable States parties to either prosecute or extradite the alleged offenders. Until the successful conclusion of ongoing negotiations on a universal definition or comprehensive convention relating to terrorism, bilateral and multilateral agreements should provide the basis for the development of common standards to counter the use of the Internet for terrorist purposes, in the interest of promoting international cooperation.

52. No universal convention has been adopted specifically relating to the prevention and suppression of terrorist use of the Internet. In December 2010, the General Assembly adopted resolution 65/230, in which it, inter alia, endorsed the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World[40] and requested the Commission on Crime Prevention and Criminal Justice to establish, in line with the Salvador Declaration, an open-ended intergovernmental expert group to conduct a

[38] See www.un.org/en/sc/ctc/laws.html.

[39] It is worth noting, however, that a recent decision by the Special Tribunal for Lebanon held that there was sufficient evidence to support the existence of a definition of the crime of terrorism under customary international law. See Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, Case No. STL-11-01/I, Special Tribunal for Lebanon (16 February 2011); available from www.stl-tsl.org/en/the-cases/stl-11-01/rule-176bis/filings/orders-and-decisions/appeals-chamber/interlocutory-decision-on-the-applicable-law-terrorism-conspiracy-homicide-perpetration-cumulative-charging.

[40] Adopted by the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Salvador, Brazil, from 12 to 19 April 2010, which addressed, inter alia, the need for Member States to consider ways of fighting new forms of crime, such as cybercrime.

comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation. The results of this study, which was launched by UNODC in February 2012, will facilitate an evaluation of the effects of the use of emergent information technologies in furtherance of criminal activities, including with respect to certain terrorist uses of the Internet, such as computer-related incitement to terrorism and terrorist financing offences.

D. International human rights law

53. Human rights obligations form an integral part of the international legal counter-terrorism framework, both through the obligation imposed on States to prevent terrorist attacks, which have the potential to significantly undermine human rights, and through the obligation to ensure that all counter-terrorism measures respect human rights. In the United Nations Global Counter-Terrorism Strategy, Member States reaffirmed those obligations, recognizing in particular that "effective counter-terrorism measures and the protection of human rights are not conflicting goals, but complementary and mutually reinforcing".

54. Key universal human rights instruments adopted under the auspices of the United Nations include the Universal Declaration of Human Rights,[41] the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights,[42] and applicable protocols.

55. Several regional organizations have also developed conventions guaranteeing human rights. Examples include the European Convention for the Protection of Human Rights and Fundamental Freedoms[43] (1950), the American Convention on Human Rights[44] (1969), the African Charter on Human and Peoples' Rights[45] (1981), and the Charter of Fundamental Rights of the European Union[46] (2000).

56. While a comprehensive analysis of issues relating to human rights law is beyond the scope of the present publication, rule-of-law considerations and the applicable legal instruments will be addressed with reference to specific counter-terrorism measures where the context so requires.[47]

[41] General Assembly resolution 217 A (III).

[42] General Assembly resolution 2200 A (XXI), annex.

[43] Council of Europe, *European Treaty Series*, No. 5.

[44] United Nations, *Treaty Series*, vol. 1144, No. 17955.

[45] Ibid., vol. 1520, No. 26363.

[46] *Official Journal of the European Communities*, C 364, 18 December 2000.

[47] See also United Nations Office on Drugs and Crime, Frequently Asked Questions on International Law Aspects of Countering Terrorism, sect. V.

E. Regional and subregional counter-terrorism legal instruments

57. In addition to the universal counter-terrorism instruments, several regional and subregional instruments offer valuable substantive and procedural standards for criminalizing acts of terrorism that may be perpetrated by means of the Internet. These instruments, which complement the universal counter-terrorism instruments, may vary in scope and in their degree of enforceability.

1. Council of Europe

58. In 2001, the Council of Europe elaborated the Council of Europe Convention on Cybercrime,[48] which is currently the only multilateral, legally binding instrument addressing criminal activity conducted via the Internet. The Council of Europe Convention on Cybercrime seeks to harmonize national laws relating to cybercrime, to improve domestic procedures for detecting, investigating, and prosecuting such crimes and to provide arrangements for fast and reliable international cooperation on these matters.[49] The Convention establishes a common minimum standard for domestic computer-related offences[50] and provides for the criminalization of nine such offences, including offences relating to unauthorized access to and illicit tampering with computer systems, programs or data; computer-related fraud and forgery; and attempting, aiding or abetting the commission of such acts.[51]

59. The Council of Europe Convention on Cybercrime also includes important procedural provisions which may facilitate investigations and evidence-gathering in connection with acts of terrorism involving use of the Internet. These provisions apply to any criminal offence committed by means of a computer and the collection of evidence in electronic form and are subject to applicable safeguards provided for under domestic law.[52]

60. For example, the Council of Europe Convention on Cybercrime requires parties to adopt legislation requiring Internet service providers (ISPs) to preserve specified data stored on their servers for up to 90 days[53] (renewable), if requested to do so by law enforcement officials during the course of a criminal investigation or proceeding, until the appropriate legal steps may be taken to compel disclosure of such data.[54] This expedited procedure for the preservation of stored data is crucial given the transient

[48] Council of Europe, *European Treaty Series*, No. 185 (also available from www.coe.int/cybercrime).

[49] Ibid., preamble.

[50] Explanatory report to the Council of Europe Convention on Cybercrime, para. 33. Available from http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[51] Ibid., arts. 2-8 and 11.

[52] Ibid., art. 14, para. 2 *(b)* and *(c)*, and art. 15. Such conditions shall include protection of human rights and liberties, including rights arising pursuant to obligations undertaken under the European Convention for the Protection of Human Rights and Fundamental Freedoms, the International Covenant on Civil and Political Rights, other applicable international human rights instruments, and judicial or other independent supervision.

[53] A minimum of 60 days is imposed with respect to preservation effected in response to a request for mutual legal assistance (Council of Europe Convention on Cybercrime, art. 29).

[54] Council of Europe Convention on Cybercrime, art. 16.

nature of electronic data and the often time-consuming traditional mutual legal assistance procedures in transnational cases.[55] The issuance of a preservation order, or similar measure, also has several benefits compared with traditional search and seizure procedures, as the ISP may be better placed to rapidly secure the evidence in question. Additionally, a preservation measure may be less disruptive to the legitimate business of the ISP, with lower potential for reputational harm to the business,[56] which may facilitate ongoing cooperation. The search and seizure procedure with respect to stored data, established pursuant to article 19 of the Council of Europe Convention on Cybercrime, provides protections regarding stored data that are similar to those generally afforded to tangible evidence[57] under the relevant domestic legislation.[58]

61. The Council of Europe Convention on Cybercrime also requires parties to implement legislation relating to the production of stored subscriber data.[59] Such information may be crucial during the investigative stage to establish the identity of a perpetrator of a terrorist act involving use of the Internet, and may include the physical location of such person, as well as other related communication services employed in the commission of the act. The Convention also requires signatory States to establish minimum standards to enable real-time collection of traffic data[60] associated with specified communications and the interception of content data in relation to specified serious offences under domestic law.[61]

62. The Council of Europe Convention on Cybercrime may be applied in conjunction with counter-terrorism instruments, such as the Council of Europe Convention on the Prevention of Terrorism,[62] to provide a legal basis for cooperation against the use of the Internet for terrorist purposes. The Council of Europe Convention on the Prevention of Terrorism requires parties to criminalize certain acts under domestic law that may lead to the commission of terrorist offences, such as public provocation, recruitment and training, all of which may be committed through the Internet. The Convention also mandates national and international cooperation measures aimed at preventing terrorism, including investigative measures. For example, article 22 of the Convention provides for the sharing with another party of unsolicited information relating to investigations or proceedings, within the limits imposed by domestic law, in the common interest of responding to criminal acts (spontaneous information).

[55] Explanatory report to the Council of Europe Convention on Cybercrime, para. 157.

[56] Ibid., para. 155.

[57] Such as the data medium upon which the data is stored.

[58] Explanatory report to the Council of Europe Convention on Cybercrime, para. 184.

[59] See Council of Europe Convention on Cybercrime, art. 18. "Subscriber data" is defined to include any information, other than traffic data or content data, relating to the user's identity, postal or geographic address, telephone and other access number, billing and payment information or any other information concerning the site or location where the communication equipment is installed that is available on the basis of the service agreement with the Internet service provider.

[60] Pursuant to article 1 *(d)* of the Council of Europe Convention on Cybercrime, "traffic data" includes information that indicates a communication's origin, destination, route, time, date, size, duration or type of underlying service.

[61] Pursuant to articles 20 and 21, respectively, of the Council of Europe Convention on Cybercrime.

[62] Council of Europe, Treaty Series, No. 196. Also available from http://conventions.coe.int/Treaty/en/treaties/html/196.htm.

63. The Council of Europe Convention on Cybercrime and the Council of Europe Convention on the Prevention of Terrorism are open to ratification or accession by all member States of the Council of Europe,[63] non-member States that participated in the elaboration of those Conventions and other non-member States by invitation, with agreement from all of the States then parties to the relevant Convention.[64] It is worth noting that several countries that have not formally acceded to the Council of Europe Convention on Cybercrime have nonetheless used its provisions as guidelines in the drafting of their own national cybercrime legislation. (See also section ⇑F below on model legislation.)

64. The Council of Europe has also elaborated the Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems.[65] This Additional Protocol may also facilitate the prosecution of terrorist acts committed via the Internet with the intention of inciting violence on the basis of race, colour, descent, national or ethnic origin, or religion.[66] The Additional Protocol is open to all contracting States of the Council of Europe Convention on Cybercrime.[67]

2. European Union

65. In 2002, the Council of the European Union adopted framework decision 2002/475/JHA of 13 June 2002 on combating terrorism, which harmonizes the definition of terrorist offences in all European Union member States[68] by introducing a specific and common definition of the concept of "terrorism", setting forth jurisdictional rules to guarantee that terrorist offences may be effectively prosecuted, and outlining specific measures with regard to victims of terrorist offences. In response to the growing terrorist threat, including the use of new technologies such as the Internet, framework decision 2002/475/JHA was amended in 2008[69] to specifically include provisions on public provocation to commit a terrorist offence, recruitment for terrorism and training for terrorism. In that decision, the Council of the European Union also took note of Security Council resolution 1624 (2005), in which the Council called upon States to take measures to prohibit by law incitement to commit a terrorist act or acts and to prevent such conduct.

[63] As at the date of the present publication, the 47 member States of the Council of Europe are the following: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Republic of Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, the former Yugoslav Republic of Macedonia, Turkey, Ukraine and United Kingdom.

[64] See Council of Europe Convention on Cybercrime, art. 36, and Council of Europe Convention on the Prevention of Terrorism, arts. 23-24.

[65] Council of Europe, *European Treaty Series*, No. 189.

[66] Ibid., art. 2.

[67] Ibid., art. 11.

[68] As at the date of the present publication, the 27 member States of the European Union are: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom.

[69] Council of the European Union Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

66. Framework decision 2008/919/JHA provides a basis for prosecuting the dissemination of terrorist propaganda and bomb-making expertise also through the Internet, to the extent that such dissemination is committed intentionally and meets the requirements of the named offences. The amendments to framework decision 2002/475/JHA relating to the offences of public provocation, recruitment and training were based on similar provisions of the Council of Europe Convention on the Prevention of Terrorism.[70] Framework decision 2008/919/JHA introduced new offences regarding conduct that may lead to acts of terrorism, irrespective of the means or technological tools through which these offences are committed. As with the Council of Europe Convention on the Prevention of Terrorism, while the provisions of framework decision 2008/919/JHA are not Internet-specific, they also cover activities conducted by means of the Internet.

3. Additional legal instruments

67. Additional binding legal instruments adopted by regional or subregional organizations which may contain provisions relevant to countering terrorist use of the Internet include the following:

- South Asian Association for Regional Cooperation Regional Convention on Suppression of Terrorism (1987)
- Arab Convention on the Suppression of Terrorism (1998)
- Treaty on Cooperation among States Members of the Commonwealth of Independent States in Combating Terrorism (1999)
- Convention of the Organization of the Islamic Conference on Combating International Terrorism (1999)
- Organization of African Unity Convention on the Prevention and Combating of Terrorism (1999)
- Inter-American Convention against Terrorism (2002)
- Association of Southeast Asian Nations Convention on Counter Terrorism (2007)
- Economic Community of West African States directive on fighting cybercrime (2009).

F. Model legislation

68. While model legislation provides advisory guidelines, rather than legally binding obligations, it plays an important role in harmonizing legal standards among States. Unlike international conventions, which may be subject to extensive negotiations to reflect the needs of a diverse range of potential signatories, the provisions of model

[70] Council of Ministers, "Amendment of the Framework Decision on combating terrorism", press release of 18 April 2008.

laws provide States with the benefit of strong foundational legal provisions as a point of departure for the development of domestic legislation. A key benefit of the use of model provisions as a basis for national legislation is the facilitation of international cooperation, including through the mitigation of conflicts arising out of misinterpretation of provisions in different legal systems (for example, between common-law and civil-law jurisdictions) and with respect to dual criminality requirements.[71] (See discussion in section V.F.5 below.)

1. Commonwealth

69. The Commonwealth Model Law on Computer and Computer Related Crime (2002) was drafted on the basis of the Council of Europe Convention on Cybercrime.[72] The Model Law is aimed at leveraging the similarities in the legal traditions of Commonwealth member States[73] to promote the harmonization of both substantive and procedural aspects of combating cybercrime and to promote international cooperation. The Commonwealth Model Law is consistent with the standards defined by the Council of Europe Convention on Cybercrime.

2. Commonwealth of Independent States

70. Member States of the Commonwealth of Independent States (CIS) have also adopted model legislative acts and guidelines, aimed at harmonizing the national legislative systems, taking into account international experiences in the fight against terrorism. These model provisions reflect international legal standards, adapted to the needs of CIS member States.[74] For example, article 13 of the Model Law on the regulatory framework of the Internet[75] provides model provisions with respect to countering the use of the Internet for illegal purposes.

3. International Telecommunication Union

71. The International Telecommunication Union (ITU) is a specialized agency of the United Nations that plays a leading role in cybercrime issues. ITU has developed the Toolkit for Cybercrime Legislation (2010) to promote harmonized national cybercrime

[71] Pursuant to the principle of dual criminality, extradition may be possible only in cases in which the act on the basis of which extradition has been requested is punishable in both the requesting and the requested State.

[72] For more information, see www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

[73] As at the date of the present publication, the 53 member States of the Commonwealth were: Antigua and Barbuda, Australia, Bahamas, Bangladesh, Barbados, Belize, Botswana, Brunei Darussalam, Cameroon, Canada, Cyprus, Dominica, Gambia, Ghana, Grenada, Guyana, India, Jamaica, Kenya, Kiribati, Lesotho, Malawi, Malaysia, Maldives, Malta, Mauritius, Mozambique, Namibia, Nauru, New Zealand, Nigeria, Pakistan, Papua New Guinea, Rwanda, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Samoa, Seychelles, Sierra Leone, Singapore, Solomon Islands, South Africa, Sri Lanka, Swaziland, Tonga, Trinidad and Tobago, Tuvalu, Uganda, United Kingdom, United Republic of Tanzania, Vanuatu and Zambia.

[74] As at the date of the present publication, the 11 member States of the Commonwealth of Independent States were: Azerbaijan, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Republic of Moldova, Russian Federation, Tajikistan, Turkmenistan, Ukraine and Uzbekistan.

[75] Annex to resolution 36-9 of the Inter-Parliamentary Assembly of the members of the Commonwealth of Independent States, adopted on 16 May 2011.

legislation and procedural rules, including with respect to acts of terrorism committed by using the Internet. The Toolkit was developed on the basis of a comprehensive analysis of the Council of Europe Convention on Cybercrime and the cybercrime legislation of developed countries.[76] While the ITU Toolkit primarily addresses cybersecurity issues, it provides model provisions for the criminalization of certain acts of terrorism involving use of the Internet, such as unauthorized access to computer programs or data for purposes of terrorism or the transmission of malware with the intent of furthering terrorism.[77]

[76] International Telecommunication Union, Toolkit for Cybercrime Legislation (2010), para. 2.2.

[77] Ibid., sects. 3 *(f)* and 6 *(h)*.

III. Policy and legislative frameworks

A. Introduction

72. In addition to using the Internet to plan and finance terrorist acts, terrorists also use it to recruit and train new members; communicate, research or reconnoitre potential targets; disseminate propaganda; and incite others to carry out acts of terrorism.

73. In the present chapter, issues related to the development of criminal justice policies and legislation aimed at countering these threats are considered, with the aim of identifying, by reference to examples and national experiences offered by some States represented at the expert group meetings, common challenges and approaches that can either impede or strengthen the effective investigation and prosecution of terrorism cases involving some aspect of Internet use.

B. Policy

74. In order to provide effective criminal justice responses to threats presented by terrorists using the Internet, States require clear national policies and legislative frameworks. Broadly speaking, such policies and laws will focus on:

(a) Criminalization of unlawful acts carried out by terrorists over the Internet or related services;

(b) Provision of investigative powers for law enforcement agencies engaged in terrorism-related investigations;

(c) Regulation of Internet-related services (e.g. ISPs) and content control;

(d) Facilitation of international cooperation;

(e) Development of specialized judicial or evidential procedures;

(f) Maintenance of international human rights standards.

Policy approaches

75. In its 2011 publication, *Countering the Use of the Internet for Terrorist Purposes: Legal and Technical Aspects*,[78] the Working Group on Countering the Use of Internet for

[78] See United Nations, Counter-Terrorism Implementation Task Force, Working Group on Countering the Use of Internet for Terrorist Purposes, *Countering the Use of the Internet for Terrorist Purposes: Legal and Technical Aspects* (New York, 2011).

Terrorist Purposes of the Counter-Terrorism Implementation Task Force identified three broad strategic approaches by which States might counter terrorist activities over the Internet; involving the use of:

(a) General cybercrime legislation;

(b) General (non-Internet-specific) counter-terrorism legislation;

(c) Internet-specific counter-terrorism legislation.

76. It is noted that in approach *(a)*, in addition to the use of general cybercrime legislation, other inchoate criminal offences such as solicitation and criminal association might also be used when dealing with terrorism cases involving some aspect of Internet use, particularly when dealing with alleged acts aimed at inciting acts of terrorism.

77. The Working Group's broad classification system is a useful conceptual framework to guide the work of policymakers and legislators when considering appropriate policy and legislative approaches for their particular States.

78. Another useful resource for policymakers and legislators, referred to in *Countering the Use of the Internet for Terrorist Purposes*[79] is the *Toolkit for Cybercrime Legislation*, developed under the auspices of ITU. In addition to other model criminal provisions, the Toolkit contains several specific terrorist-related offences, including section 3 *(f)*, which deals with unauthorized access to, or acquiring computer programs for, the purpose of developing, formulating, planning, facilitating, assisting in the commission of, conspiring to commit or committing acts of terrorism.

79. Within the broad framework provided by universal counter-terrorism instruments and relevant international human rights standards, Governments have considerable flexibility in their preferred approach; inevitably, these vary between States. The present chapter merely highlights examples of approaches adopted by some States that might be helpful to policymakers and legislators.

80. Currently, few States have developed counter-terrorism legislation specifically targeting the use of the Internet itself by terrorists, but there are some, including the United Kingdom, where, after the 2005 bombings in London the Government enacted the Terrorism Act 2006, Part 1 of which includes provisions specifically dealing with Internet-based activity that is likely to encourage or assist in the commission of acts of terrorism. The Act supplements the Computer Misuse Act 1990, which addresses computer-based crime and cybercrime more generally.

81. In 2007, the United Arab Emirates passed federal cyberlaws that, in addition to criminalizing hacking and other Internet-related activity, criminalized the establishment of a website or the publication of information for terrorist groups under false names with intent to facilitate contact with their leadership or promote their ideologies, finance

[79] Ibid., para. 20.

their activities or publish information on how to make explosives or other substances for use in terrorist attacks.[80]

82. In 2008, the Government of Saudi Arabia implemented new technology-related laws, including one that established as a criminal offence, punishable by fines and up to 10 years of imprisonment, owning a website that advocates or supports terrorism.[81]

83. Also in 2008, the Government of Pakistan enacted the Prevention of Electronic Crimes Ordinance, 2008, which made specific provision for offences connected to cyber-terrorism. The law is no longer in force, however.[82]

84. Finally, the same year saw the Government of India amend the Information Technology Act, 2000, to provide for the offence of "cyber terrorism" (section 66F) and other Internet-related issues.

85. Nevertheless, internationally, with some exceptions, in the absence of any universal instrument imposing an express obligation to enact legislation specifically targeting terrorist activity over the Internet, most Governments have elected to deal with such threats by using a mixed approach, utilizing a combination of general criminal laws, as well as cybercrime and counter-terrorism legislation. In some States, for example, criminal laws focus on substantive criminal acts without differentiating among the specific means by which they are committed. Under this approach, the Internet is regarded as merely a tool by which terrorists commit a substantive crime, often contained within the provisions of the national penal code.

86. This is the approach in China, where the Criminal Law of the People's Republic of China contains an article dealing with the criminalization of all illegal activities involving the use of the Internet. Article 287 of the Criminal Law makes it an offence to use a computer in the commission of an offence, which will be prosecuted and sentenced in accordance with the relevant criminalization and sentencing provisions in that law. In this way, under Chinese criminal law, the use of Internet is regarded as a medium or tool through which a criminal act may be committed, rather than an independent constituent element of the crime, and is therefore criminalized within the substantive provisions of the criminal law.

87. In the terrorism context, in China there are provisions criminalizing different forms of terrorist activities, including article 120 of the Criminal Law, which criminalizes activities related to organizing, leading and participating in terrorist organizations. This broad criminalization provision covers a wide range of terrorism-related activities, including those carried out over the Internet.

[80] Federal Law No. (2) of 2006 on the Prevention of Information Technology Crimes, *Official Gazette of the United Arab Emirates*, vol. 442, 36th year, Muharam 1427 H/January 2006 (unofficial English translation available from www.aecert.ae/pdfs/Prevention_of_Information_Technology_Crimes_English.pdf).

[81] David Westley, "Saudi tightens grip on Internet use", *Arabian Business*, 26 January 2008.

[82] "Pakistan lacks laws to combat cyber terrorism", *The New New Internet*, available from www.thenewnewInternet.com/2010/09/01/pakistan-lacks-laws-to-combat-cyber-terrorism.

88. In the Republic of Korea, two types of criminal law can be applied to terrorist acts involving some use of the Internet. One is the general criminal code and the other is a special criminal code, established in 1986, relating to criminal acts involving information/communication. Article 90 of the Criminal Code deals with the preparation of such acts, as well as conspiracy, incitement or propaganda and provides that any person who prepares or plots for the purpose of committing crimes under article 87 of the Criminal Code (public riots, revolts or disturbances) or article 88 (homicides committed for the purpose of acts under article 87) is liable to imprisonment of three years or more. Under article 101 of the Criminal Code, any person who prepares or conspires to commit offences under articles 92 to 99 of the Criminal Code is guilty of a crime and liable to two years or more imprisonment. Article 114 of the Criminal Code relates to organizing a criminal group. Also under the special criminal code, the Government established a range of criminal offences specifically criminalizing unlawful acts targeting information-communication networks and personal information.

89. In practice, regardless of the policy approach taken, experience shows that most States adopt a multifaceted approach when dealing with the investigation and prosecution of terrorist acts, including those involving some use of the Internet. Law enforcement and prosecution agencies use whatever legislative provisions best suit the particular circumstances of the case.

90. The powers required by law enforcement agencies to effectively investigate terrorism cases are broadly similar regardless of the particular jurisdiction involved, with differences in national policies and legislation reflecting the diversity in legal systems, constitutional arrangements and other factors (e.g. cultures).

91. The area of Internet regulation and content control leaves considerable room for variations in national approaches. While the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights provide international standards pertaining to the regulation of the expression and communication of ideas, there is no comprehensive internationally binding instrument setting definitive, binding norms on what is considered appropriate Internet content or how each State should regulate Internet-related activity within its own territory. Currently, child pornography is the one area where, even in the absence of a universally binding instrument or definition, States invariably prohibit such activities.[83] In the terrorism context, however, the absence of a universally agreed definition of terrorism presents an ongoing obstacle to any internationally agreed approach to the appropriate regulation of terrorism-related activity and content over the Internet.

92. In terms of specialized judicial or evidential procedures in the terrorism field, some States have adopted specific judicial and case management procedures for terrorism cases that might apply to cases involving the use of the Internet by terrorists. When this approach is adopted, it is important that any specialized mechanisms conform fully with relevant international human rights obligations, including those related to the right to liberty and a fair trial.

[83] Maura Conway, "Terrorism and Internet governance: core issues", *Disarmament Forum*, vol. 3 (2007), p. 27.

C. Legislation

1. Criminalization

93. As stated above, none of the universal instruments against terrorism impose an obligation on States to enact legislation specifically targeting the use of the Internet by terrorists. Accordingly, while it is therefore highly likely that most terrorism cases will involve some use of the Internet by perpetrators, it is likely that in many States, in addition to using offence provisions related to unlawful conduct specified in universal instruments, authorities will also be reliant on other criminal offence provisions under their penal codes, including inchoate offences such as conspiracy, solicitation and criminal association, in order to prosecute offenders.

94. In the present section, examples of different legislative provisions from some States are considered, with a view to identifying approaches that might provide the basis for effective criminal justice responses to different types of conduct.

(a) Internet-based acts or statements supporting terrorism

95. In addition to acts associated with the commission of substantive terrorist acts (e.g. terrorist bombings), there is clear evidence that the Internet is increasingly being used by terrorists to carry out support actions such as recruiting and training members, sharing useful information, disseminating propaganda and inciting the commission of acts of terrorism. Owing to the configuration and global reach of the Internet, it is increasingly likely that these types of activities may involve different actors being physically present in different legal jurisdictions.

96. In the United Kingdom, part VI of the Terrorism Act 2000 contains several offences that can provide the basis for charging individuals who have used the Internet to support terrorist activities.

97. Section 54 of the Act makes it an offence to provide, receive or invite others to receive instruction or training in the making or use of firearms, radioactive material or related weapons, explosives or chemical, biological or nuclear weapons.

98. Section 57 makes it an offence to possess articles in circumstances that give rise to a reasonable suspicion that a person has such articles in connection with the preparation, instigation or commission of an act of terrorism. In recent years, this offence has been used to successfully prosecute several individuals who have been found in possession of items as diverse as hard drives, DVDs and instructional documents on how to make or operate items such as mortars, suicide vests and napalm.[84] For there to have been a commission of this offence, the prosecution must prove a connection between the article in question and a specific act of terrorism. There have been several

[84] Susan Hemming, "The practical application of counter-terrorism legislation in England and Wales: a prosecutor's perspective", *International Affairs*, vol. 86, No. 4 (July 2010), p. 963.

successful prosecutions for offences under section 57; however, the Courts have adopted a more restrictive approach in interpreting the scope of application of the section, as demonstrated by the case of *R. v. Zafar, Butt, Iqbal, Raja and Malik* [2008] EWCA Crim 184.

R. v. Zafar, Butt, Iqbal, Raja and Malik

This 2007 case from the United Kingdom involved successful appeals by the defendants Zafar, Butt, Iqbal, Raja and Malik against convictions imposed for possession of articles for a purpose connected with the commission, preparation or instigation of an act of terrorism, contrary to section 57 of the Terrorism Act 2000.

Four of the five defendants in the case were students at Bradford University. The fifth, Raja, was a schoolboy in Ilford and established contact with Iqbal through the Internet messaging service MSN.

Raja visited Bradford for a few days, staying at the house in which Iqbal and Zafar lived, and brought with him three CDs he had made that contained selected material from the computer and were labelled as "philosophy discs". Raja was arrested by police upon his return home after the visit.

Subsequent police enquiries led them to arrest and search the places of residence of the other accused, which revealed that they too were in possession of radical jihadist material and other material such as a United States military manual downloaded from the Internet. Evidence of communications via online messenger were found, including a discussion between all four of the Bradford appellants and a cousin of Malik—Imran—who lived in Pakistan.

The defendants originally faced charges under section 58 of the 2000 Act; however, at the committal stage, the prosecution added counts under section 57 reflecting the same particulars as those under section 58. Following various pretrial rulings on the issue of whether electronically stored information could be considered an article for the purposes of section 57, the prosecution elected to proceed to trial on the basis of the section 57 charges only.

At trial, Zafar and Iqbal were acquitted on one count, which charged them with possession of three "philosophy discs" containing material emanating from Raja; however, they, together with the other defendants, were found guilty in respect of all other charges. Malik was sentenced to three years of imprisonment, Zafar and Iqbal to three years of detention in a young offenders' institution, Butt to 27 months of detention and Raja to two years of detention.

The defendants appealed these convictions. At the appeal, the Court considered the critical issue to be whether, based on the facts of the case, there existed between the articles and the acts of terrorism a connection that satisfied the requirements of section 57.

The articles that the Crown alleged that the appellants possessed in breach of section 57 were, for the most part, CDs and hard drives containing electronically stored material. This material included ideological propaganda and communications between the defendants, which the prosecution alleged showed a settled plan involving the defendants travelling to Pakistan to receive training and participate in fighting in Afghanistan, which the Crown alleged amounted to acts of terrorism. The Court of Appeal held that it was necessary for the prosecution to prove first the purpose for which each appellant held the stored material and then to prove that this purpose was "connected with the commission, preparation or instigation" of the prospective acts of terrorism relied on by the prosecution, namely fighting against the Government in Afghanistan.

On the facts of the case, noting that it raised difficult questions of interpretation about the scope of application of section 57, the Court held that the necessary connection was not present, and therefore the resulting convictions were unsound, and allowed the appeals.

99. Section 58 of the Act has proven particularly useful in several cases in which authorities have needed to intervene when there was no evidence that the individual was engaged in activity associated with terrorism. The section makes it an offence to collect, make or have in one's possession, without a reasonable excuse, any record of information of a kind likely to be useful to a person committing or preparing an act of terrorism or to have possession of any document or record containing such information.

100. In *R v. K* [2008] 3 All E.R. 526, the Court held that a document falls within the scope of section 58 only if it is of a kind that is likely to provide practical assistance to a person committing or preparing to commit an act of terrorism. This approach was reaffirmed in *R v. G and J* [2009] UKHL 13, in which the Court reaffirmed this "practical use test", under which possession of a document or record is a crime only if it is of practical use and was possessed by a person without a reasonable excuse.[85] There is no restriction on what might constitute a reasonable excuse for this purpose, provided that it is capable in law of amounting to a defence.

101. Under section 58, the prosecution is not required to prove that the accused is a terrorist or that any items are possessed for a terrorist purpose; however, the prosecution may only in very limited circumstances call extrinsic evidence to prove the practical utility of any item. For example, evidence of cipher may be called in order to decipher a document written in code, but no evidence may be called to explain the significance of locations circled on a map. The information must "speak for itself" and not be of a type in general circulation.

102. In *R v. Sultan Mohammed* [2010] EWCA Crim 227, the court held that "[p]rovided that the document containing the information is not one in every day use by ordinary members of the public (e.g. published timetables and maps) and provided that a reasonable jury could properly conclude that the document contains information of a kind likely to be useful to a person committing or preparing an act of terrorism, then it will be a matter for the jury whether they are sure that it contains such information. If so, and provided the defendant has the necessary mens rea, then the only issue will be whether the defendant has a reasonable excuse."[86] The jury must accordingly decide whether the explanation given for possessing the document is in fact reasonable given the particular facts and circumstances of the case.[87]

[85] Ibid., p. 962.

[86] Quotation from "R. v. Muhammed [2010] EWCA Crim 227: terrorism—preparing an act of terrorism", *Criminal Law and Justice Weekly* (20 March 2010).

[87] Hemming, "The practical application of counter-terrorism legislation in England and Wales", p. 963.

103. The Terrorism Act 2006 established (in its section 5) the offence of "committing acts in preparation for terrorism". This section was designed to deal with cases in which individuals actively planning acts of terrorism were stopped before they completed or attempted a substantive terrorist act.[88]

104. Section 5 has been particularly useful in "lone wolf" cases, in which an offender is acting alone, there is insufficient evidence to establish the basis of a conspiracy charge because it cannot be proven that more than one person was involved, or authorities do not know in detail the offence that was being planned. The offence does not require proof of an identifiable final act or acts of terrorism, but the prosecution must prove a specific intent to commit a terrorist act or to assist another to do so. Several individuals have been convicted of the offence in the United Kingdom and sentenced to varying terms of imprisonment, including life imprisonment.[89]

105. The case of *R v. Terence Roy Brown* [2011] EWCA Crim 2751, is an example of the utility of provisions such as section 58.

R v. Terence Roy Brown

Terence Roy Brown, a citizen of the United Kingdom, ran an online business, in which he advertised and sold an annual edition of a CD-ROM that he called the "Anarchist's Cookbook" (the title is nearly identical to that of a well-known book called *The Anarchist Cookbook*). Rather than a single publication, however, these discs contained 10,322 files, some of which were complete publications in their own right. These included terrorist manuals such as the Al-Qaida Manual and instructions for the manufacture of different forms of explosives and the construction of bombs. Other files consisted of instructions for making poisons, how to avoid attracting the attention of authorities when travelling and weapons-handling techniques. In an apparent effort to circumvent the law, Mr. Brown posted disclaimers on the website advertising the publication, stating that the instructions they contained might be illegal or dangerous to perform and were intended for "reading pleasure and historical value only". It was clear on investigation that Mr. Brown was motivated purely by commercial incentives. It was also apparent that he deliberately had expanded his collection in the immediate aftermath of the July 2005 London bombs and had significantly increased his profit as a result.

In March 2011, Mr. Brown was convicted of seven counts under the Terrorism Act 2000 (section 58) relating to the collection of information that could have been used to prepare or commit acts of terrorism, two counts under the Terrorism Act 2006 (section 2) relating to the dissemination of terrorist publications and an offence under the Proceeds of Crime Act 2002 relating to the transfer of criminal property (his use of the profits from his business).[a]

[88] Ibid., p. 964.

[89] Ibid.

The excuse raised by Mr. Brown at trial was that his activities amounted to no more than the lawful exercise of his right to freedom of expression in relation to material that was freely available on the Internet and that was similar in type, if not volume, to that sold by other online booksellers. The same points were raised during an unsuccessful application to appeal conviction, during which the court ruled that the restriction of Brown's article 10 rights in relation to material that was likely to assist terrorists was justified and proportionate. The court also affirmed the discretion of the prosecuting authorities not to charge every individual who might have committed an offence, but to consider instead each case on its own merits.

[a] "Businessman who published bomb-makers' handbook 'facing lengthy spell in jail'", *Daily Mail*, 9 March 2011. Available from www.dailymail.co.uk/news/article-1364621/Businessman-published-bomb-makers-handbook-facing-lengthy-spell-jail.html#ixzz1j4gXbMLu.

106. The case is one of several, including *R v. K* [2008] QB 827 and *R v. G* [2010] 1 AC 43, in which the courts in the United Kingdom have clarified the jurisprudence surrounding the scope and application of section 58 of the Act, in the light of relevant human rights safeguards.

107. In addition to criminal offences under anti-terrorism legislation, authorities in the United Kingdom have, when circumstances require, used the offence of solicitation to successfully prosecute persons carrying out activities linked to terrorism. An example of this approach is the case of *R v. Bilal Zaheer Ahmad*,[90] in which the defendant was convicted of solicitation of murder.

R v. Bilal Zaheer Ahmad

This United Kingdom case is linked to, and followed, the 2010 case involving Roshanara Choudhry, who was sentenced to life imprisonment on 2 November 2010 for the attempted murder of Stephen Timms, a Member of Parliament.

In a statement, Choudhry said she had decided to commit the offence approximately four weeks prior to the assault in May 2010 and had purchased two knives in preparation, one as a spare in case the first broke while she stabbed the victim. She told police that she had been watching Anwar al-Awalaki videos and Abdullah Azzam videos and had visited the website www.revolutionmuslim.com during her period of radicalization. This well-known site, which was hosted in the United States, contained material promoting violent jihad, including videos and speeches encouraging terrorism and weblinks to terrorist publications.

On 1 November 2010, the defendant posted a link on his Facebook page to a news article about the Timms/Choudhry case, to which he added the following comment:

[90] Nottingham Crown Court, 13 May 2011.

This sister has put us men to shame. WE SHOULD BE DOING THIS.

On 4 November 2010, the defendant posted an article entitled "MPs that voted for War on Iraq" on the Revolution Muslim website under the name of "BILAL". The article was headed with the symbol of the Islamic State of Iraq (an Al-Qaida affiliate). The opening text was a quotation from the Koran stating that those who died without participating in jihad were hypocrites.

The article advised readers that they could "track" British Members of Parliament through a link it provided to an official parliamentary website. This would enable them to find out details regarding the location of surgeries to be performed on Members of Parliament, where they could be "encountered in person".

This was followed by 29 religious quotations, all translated into English and all relating to the obligation for Muslims to participate in jihad or to "martyrdom". Immediately under the quotations was a link to a web page advertising a knife for sale. A copy of this article was captured evidentially by British counter-terrorism officers. A further copy of the web page was obtained from Google Inc. in response to a letter of request.

On 10 November 2010, the defendant was arrested by the Counter Terrorism Unit of the West Midlands Police near his home in Wolverhampton. He was found in possession of a laptop, which he told the arresting officers he had used to post the article on members of parliament on the Revolution Muslim website. Forensic examination of the laptop revealed that he appeared to have attempted to delete traces of his online activities prior to his arrest.

On 16 November, the defendant was charged with soliciting murder in relation to the article and with three offences of possession of material likely to be of use to a terrorist under section 58 of the Terrorism Act 2000. He later pleaded guilty to these charges, as well as to an offence of inciting religious hatred, arising from comments posted on an Internet forum, and was sentenced to 12 years of imprisonment, with an additional five years extended period on licence.

108. In the United States, Title 18 of the United States Code, section 842 *(p)*, entitled "Distribution of information relating to explosives, destructive devices, and weapons of mass destruction" makes it illegal for a person to distribute by any means information regarding the manufacture or use of explosives, destructive devices or weapons of mass destruction with the intent that the information be used in furtherance of a crime of violence or with the knowledge that the person to whom the information is distributed intends to use the information in furtherance of a crime of violence. This statute has been used in the United States to prosecute individuals who have distributed such information over the Internet.

(b) Incitement

109. The crime of inciting terrorist acts is the subject of Security Council resolution 1624 (2005). In that resolution, the Council called upon all States to, inter alia, adopt such measures as may be necessary and appropriate and in accordance with their obligations under international law to prohibit by law incitement to commit a terrorist act or acts, and to prevent such conduct.

110. The development and enforcement of laws criminalizing the incitement of acts of terrorism while fully protecting human rights such as the rights to freedom of expression and association presents an ongoing challenge for policymakers, legislators, law enforcement agencies and prosecutors. Cases involving statements by persons made over the Internet, especially when the alleged offender, the Internet services they use and their intended audience are located in different jurisdictions, are regulated by different national laws and constitutional safeguards and therefore present additional challenges for investigators and prosecutors from an international cooperation perspective.

111. International experience relating to the enforcement of criminal offences dealing with incitement to commit terrorist acts highlights two issues: first, how important (and sometimes difficult) it is in practice to differentiate between terrorist propaganda (statements advocating particular ideological, religious or political views) from material or statements that amount to incitement to commit violent terrorist acts; and second, how the enforcement of laws dealing with alleged acts of incitement requires a careful case-by-case assessment of the circumstances and context to determine whether the institution of a prosecution for an incitement offence is appropriate in a particular case.

112. Those experts at the expert group meeting who had been involved in cases related to the investigation and prosecution of crimes of inciting terrorist acts agreed and highlighted the importance, in practice, of fully assessing the context in which alleged statements of incitement were made, including not only the words but also the forum in which they were made, and that the characteristics of likely recipients might be highly relevant factors in determining whether criminal proceedings for the crime of incitement were instituted or likely to be successful in a particular case.

113. In the United Kingdom, section 59 of the Terrorism Act 2000 makes it an offence to incite another person to commit an act of terrorism wholly or partly outside the United Kingdom, when the act would, if committed in England and Wales, constitute an offence specified in the section (e.g. murder, wounding with intent, explosions or endangering life by damaging property).

114. In the well-known case of *R v. Tsouli and others*,[91] Younes Tsouli, Waseem Mughal and Tariq al-Daour pleaded guilty to charges under the Terrorism Act 2000 of inciting murder for terrorist purposes by establishing and maintaining large numbers of websites and chat forums used to publish materials inciting acts of terrorist murder, primarily in Iraq.

[91] *R v. Tsouli* [2007] EWCA (Crim) 3300.

R v. Tsouli and others

This well-known case from the United Kingdom involved three defendants—Younes Tsouli, Waseem Mughal and Tariq al-Daour—who were initially indicted on 15 counts. Prior to trial, Tsouli and Mughal pleaded guilty to a charge of conspiracy to defraud. During the trial, having heard the prosecution evidence, all three pleaded guilty to a charge of inciting terrorism overseas, and Al-Daour pleaded guilty to a charge of conspiracy to defraud.

Between June 2005 and their arrest in October 2005, the defendants were involved in the purchase, construction and maintenance of a large number of websites and Internet chat forums on which material was published that incited acts of terrorist murder, primarily in Iraq. The cost of purchasing and maintaining the websites was met from the proceeds of credit card fraud. The material on the websites included statements that it was the duty of Muslims to wage armed jihad against Jews, crusaders, apostates and their supporters in all Muslim countries and that it was the duty of every Muslim to fight and kill them wherever they were, civilian or military.

In the Internet chat forums, individuals disposed to join the insurgency were provided with routes by which to travel into Iraq and manuals on weapons and explosives recipes. Extreme ideological material demonstrating adherence to the espoused justification for the acts of murder that the websites and chat forums incited was recovered from the home of each defendant.

Al-Daour organized the obtaining of stolen credit cards, both for his own purposes and for providing Mughal with funds for the setting up and running of the websites. Al-Daour had also been involved in further credit card fraud; the proceeds of which were not applied to the support of the websites. The loss to the credit card companies from this aspect of the defendants' fraudulent activity was £1.8 million.

Among the evidence was a list made by Tsouli in his handwriting and found in his desk on which he had written the details of a number of websites and of stolen credit cards. This revealed 32 separate websites provided by a number of different web-hosting companies that Tsouli had set up or attempted to set up, mostly in the last week of June 2005 but continuing into July and into August. The creation and administration of these websites were funded by the fraudulent use of credit card details that had been stolen from account holders, either by direct theft of computer records, by hacking or by some fraudulent diversion within the financial institutions. These credit card details had been passed on to Tsouli by the other two defendants.

The websites created by Tsouli were used as a vehicle for uploading jihadist materials, which incited acts of violence outside the United Kingdom in Iraq. Access to the sites was restricted to those who had been issued with usernames and passwords. This was done, the trial judge found, to make it more difficult for the web-hosting companies and the law enforcement agencies to know what was being posted on the sites.

On 5 July 2007, Tsouli was sentenced to 10 years of imprisonment and 3½ years (concurrently) on two counts. Mughal to 7½ years of imprisonment and 3½ years (concurrently) on two counts and al-Daour, to 6½ years of imprisonment and 3½ years (concurrently).

115. Part 1 of the Terrorism Act 2006 established a number of new offences aimed at enhancing the ability of authorities to take action in cases involving statements by persons inciting or glorifying acts of terrorism or otherwise intended to support the commission of such acts.

116. Part 1 of the Act makes it an offence for a person to publish a statement intended to directly or indirectly encourage members of the public to prepare, instigate or commit acts of terrorism, including (but not limited to) encouragement that "glorifies" terrorist acts, or for a person to be reckless as whether such conduct has such an effect. In practice, how a statement is likely to be understood is determined by reference to the content as a whole and the context in which it is made available.

117. Section 2 of the Act makes it an offence to (intentionally or recklessly) disseminate terrorist publications. These are defined as publications that are likely to encourage acts of terrorism or are likely to be useful to someone planning or committing such an act. This second category covers the same types of documents or publications to which section 58 of the Terrorism Act 2000 applies. As with section 1 of the Terrorism Act 2006, the question of whether the material in question comes within the definition of a "terrorist publication" must be determined by reference to its content as a whole and the context in which it is made available.[92]

118. In the United Kingdom, when making decisions as to whether to initiate prosecutions for incitement, prosecutors exercise wide discretion, taking into account the right to freedom of speech and the overall context in which the statements or publications are made or distributed, including how they are likely to be understood, both by the general public and the intended recipients.

119. In the United States, a different legal approach has been taken to the criminalization and prosecution of acts of incitement of terrorism owing to constitutional safeguards attaching to the right to freedom of speech under the First Amendment to the Constitution. Under the principles set out in the landmark case of *Brandenburg v. Ohio*, 395 US. 444 (1969), in order to successfully prosecute an individual for incitement of criminal acts (including terrorism), the prosecution is required to prove both an intent to incite or produce unlawful action and the likelihood that the speech will actually incite imminent unlawful action.[93]

120. In prosecuting statements inciting acts of terrorism, authorities in the United States are reliant upon inchoate offences such as solicitation and conspiracy, together with the "material support" provisions of the United States Criminal Code, which in certain circumstances permit the prosecution of conduct that supports violent acts of terrorism.[94]

121. The material support provisions of the United States Criminal Code, Title 18, section 2339A and 2339B, prohibit persons from knowingly or intentionally providing, attempting to provide or conspiring to provide material support or resources to a terrorist organization. The Uniting and Strengthening America by Providing Appropriate

[92] Hemming, "The practical application of counter-terrorism legislation in England and Wales", p. 963.

[93] Elizabeth M. Renieris, "Combating incitement to terrorism on the Internet: comparative approaches in the United States and the United Kingdom and the need for an international solution", *Vanderbilt Journal of Entertainment and Technology Law*, vol. 11, No. 3 (2009), pp. 681-682.

[94] United States Criminal Code, title 18, sections 2339A and 2339B.

Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001 broadened the definition of material support to include "any property, tangible or intangible, or service, including … training, expert advice or assistance … or communications equipment".[95]

122. The criminal offences of solicitation or conspiracy, found in United States Criminal Code, title 18, section 373 *(a)* provides that any person can be charged with solicitation who "solicits, commands, induces or otherwise endeavours to persuade another person to engage in a felonious conduct with intent that another person engage in the conduct".

123. In the United States, there have been several cases in which this approach has been used to successfully prosecute the words or actions of terrorists communicated via the Internet. These include *United States of America v. Emerson Winfield Begolly*.

United States of America v. Emerson Winfield Begolly

A 22-year-old student (a United States national), Emerson Winfield Begolly was indicted for his involvement in the distribution over the Internet of information relating to bomb-making and solicitation to commit violence on American soil. Additional charges against him included assaulting and threatening Federal Bureau of Investigation (FBI) agents with a loaded firearm.

Formally known under the alias of "Asadullah Alshishani", Begolly took an active part in an internationally known jihadist forum called the Ansar al-Mujahideen English Forum and eventually became an active moderator. The forum provided an opportunity for Begolly to express his affinity for radical views while concurrently encouraging other members of his faith to engage in terrorist acts within the United States. His propaganda also included dissemination of videos with instructions for making explosive devices to perform acts of terrorism. The intended targets included synagogues, military facilities, train lines, police stations, bridges, cell phone towers and water plants.

Over a period of nine months, Begolly posted several lengthy messages in which he extensively discussed the need for violence. An indictment issued on 14 July 2011, by the U.S. District Court of the Eastern District of Virginia, included as a key evidence part of the propaganda that Begolly had posted on an Internet forum:

> Peaceful protests do not work. The Kuffar[a] see war as solution to their problems, so we must see war as the solution to ours. No peace. But bullets, bombs and martyrdom operations.

He also posted links to an online document entitled "The explosives course", made available for download. The 101-page document authored by "The Martyred Sheik Professor Abu Khabbab al Misri" (as referred to by Begolly) contains detailed instructions on setting up a laboratory with basic chemistry components for the manufacture of explosives. A note was added that those downloading the content should be careful to use anonymity software for their own protection.

[95] Renieris, "Combating incitement to terrorism on the Internet", pp. 682-683.

During this time, Begolly had been under the constant surveillance of federal authorities. An FBI agent downloaded the document from one of the uploaded links, which eventually led to Begolly being arrested. On 14 April 2011, he was charged with unlawful and purposeful distribution of information over the Internet related to the manufacture and distribution of explosive materials, use of weapons of mass destruction and solicitation to commit bombings of places for public use, government buildings and public transportation systems. On 9 August 2011, Begolly pleaded guilty to solicitation to commit terrorist acts. He is currently awaiting sentencing.

[a] A term extensively used by Begolly during his online forum discussions in reference to the "non-believers" or infidels.

(c) Review of legal approach to incitement

124. In Europe, article 3 of the Council of the European Union framework decision 2008/919/JHA of 28 November 2008 amending framework decision 2002/475/JHA on combating terrorism, and article 5 of the Council of Europe Convention on the Prevention of Terrorism oblige the respective member States of each instrument to criminalize acts or statements constituting incitement to commit acts of terrorism. The Council of Europe Convention on the Prevention of Terrorism imposes an obligation on member States to criminalize '"public provocation to commit a terrorist offence", as well as both recruitment and training for terrorism.

125. The implementation of the Convention, which is partly based on article 3 of the Additional Protocol to the Council of Europe Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, obliges States to strike a sensible balance between the requirements of law enforcement and the protection of human rights and liberties. It has therefore given rise to fundamental concerns and debates. Nevertheless, article 5 (like articles 6 and 7 on recruitment and training for terrorist purposes) must be applied in conjunction with the basic provision of article 12, which provides that implementation of that criminalization must be carried out in a manner that respects human rights, in particular the rights to freedom of expression, freedom of association and freedom of religion, as set out in human rights instruments, including article 10, paragraph 1, of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

126. The European Court of Human Rights, in assessing the protections afforded by article 10, paragraph 1, of the European Convention for the Protection of Human Rights and Fundamental Freedoms, has already dealt with article 5 of the Council of Europe Convention on the Prevention of Terrorism. In the well-known case of *Leroy v. France*,[96] a French Court did not find a violation of article 10 in the case of a journalist who had been convicted and fined for having published a certain cartoon in a Basque weekly newspaper. On 11 September 2001, the cartoonist submitted to the magazine's

[96] Judgement by the European Court of Human Rights (Fifth Section), case of *Leroy v. France*, Application no. 36109/03 of 2 October 2008.

editorial team a drawing representing the attack on the twin towers of the World Trade Centre, with a caption which parodied the advertising slogan of a famous brand: "We have all dreamt of it ... Hamas did it" (cf. "Sony did it"). The drawing was then published in the magazine on 13 September 2001.

127. In its reasoning, the European Court of Human Rights, inter alia, referred to article 5 of the Council of Europe Convention on the Prevention of Terrorism, the first time that the Court took that Convention into consideration in a judgement. It held that the drawing went further than merely criticizing the United States but rather supported and glorified its violent destruction. The Court noted the caption that accompanied the drawing, indicating the applicants' moral support for the suspected perpetrators of the attacks of 11 September 2001. Other factors taken into account by the Court were the applicant's choice of language, the date of publication of the drawings (which the Court considered increased the cartoonist's responsibility) and the politically sensitive region in which it was distributed (the Basque region). According to the Court, the cartoon had provoked a certain public reaction, capable of stirring up violence and demonstrating a plausible impact on public order in the region. The principles developed in this landmark case will apply equally to cases in which the alleged incitement to terrorism has occurred via the Internet.

128. There have been successful prosecutions for acts of incitement in Europe. For example, in Germany in 2008, Ibrahim Rashid, an Iraqi Kurdish immigrant was convicted of incitement after being charged with waging a "virtual jihad" on the Internet. Prosecutors claimed that, by posting Al-Qaida propaganda on Internet chat rooms, Rashid was trying to recruit individuals to join Al-Qaida and participate in jihad.

129. The UNODC *Digest of Terrorist Cases*[97] contains a useful summary of approaches taken to the criminalization of acts of incitement in Algeria, Egypt, Japan and Spain. In Algeria, article 87 bis 1 of the Penal Code makes acts of violent terrorism punishable by death, life imprisonment or other lengthy sentences. Article 87 bis 4 provides that whoever justifies, encourages or finances the listed terrorist acts is subject to imprisonment for from 5 to 10 years, as well as a fine.[98]

130. In Egypt, in article 86 bis of the Penal Code establishes as offences acts amounting to executive and support responsibility, the planning and preparation of terrorist acts, membership in or support of an illegal organization, providing financing and material support of terrorist organizations, and incitement offences. Moreover, the article provides aggravated penalties for, inter alia, intentionally promoting (by any means) the purposes of terrorist organizations or for obtaining or producing (directly or indirectly) articles, publications or recordings of any kind intended to promote or encourage such purposes.[99]

[97] United Nations Office on Drugs and Crime, *Digest of Terrorist Cases* (2010).

[98] Ibid., para. 100.

[99] Ibid., para. 111.

131. In Japan any person who induces a crime, directly or through an intermediary, is subject to sentencing as though the inducer had been one of the material executors of the offence (article 61 of the Penal Code).[100] Other statutory provisions in Japan, such as articles 38 to 40 of the Subversive Activities Prevention Act, criminalize incitement of insurrection or arson, with the intent to promote, support or oppose any political doctrine or policy.

132. In Spain, articles 18 and 579 of the Spanish Penal Code make public incitement to commit a crime of terrorism a preparatory act of the crime of provocation. Article 578 punishes the crime of praising terrorism, an offence that was incorporated in the Penal Code by Organic Law 7/2000 of 22 December 2000. As informally translated, this article provides that "The praising or the justification by any means of public expression or dissemination of the offences included in articles 571 to 577 of this Code (Crimes of Terrorism) or of anyone who has participated in their execution, or commission of acts that involve discredit, contempt or humiliation of the victims of a terrorist offence or of their family will be punished with imprisonment from one to two years." The Organic Law also provided a penalty of a period of civil disability upon conviction.[101]

133. In Indonesia there is no regulation specifically addressing activities undertaken by terrorists via the Internet, including incitement to commit acts of terrorism. Article 14 of Law No. 15/2003 on the elimination of acts of terrorism deals with incitement to conduct terrorist acts without reference to the particular mode of communication used by the perpetrator, as does the Indonesian Penal Code, which addresses incitement to commit other criminal acts. Indonesian authorities have successfully prosecuted persons for terrorism-related activity over the Internet. In 2007, 24-year-old Agung Prabowo, also known as Max Fiderman, was sentenced to three years of imprisonment (pursuant to section 13 *(c)* of Government Regulation in Lieu of Law No. 1/2002 and Law No. 15/2003 on the elimination of acts of terrorism) for registering and hosting a website, www.anshar.net, at the request of Noordin M. Top, leader of the Jemaah Islamiyah terrorist group, through an intermediary, Abdul Aziz. Aziz is reported to have designed www.anshar.net in mid-2005 at Top's request, with the aim of spreading jihadist propaganda. While it contained general information about Islam and jihad, it also contained specific "tips and advice" on how and where to carry out terrorist attacks, suggesting roads leading into shopping centres and offices, traffic jams and specific named locations where members of the public could be found.[102] In another case, Muhammad Jibril Abdul Rahman, also known as Muhammad Ricky Ardan (the "Prince of Jihad"), was sentenced to five years of imprisonment for having been an accomplice in an act of terrorism.

134. In Singapore, in the Internet context, section 4 2 *(g)* of Singapore's Internet Code of Practice prohibits material that "glorifies, incites or endorses ethnic, racial or religious hatred, strife or intolerance".

[100] Ibid., para. 100.

[101] Ibid., para. 115.

[102] See www.indonesiamatters.com/624/wwwansharnet-chatroom-jihad.

2. Rule-of-law considerations related to criminalization of incitement

135. When calling upon States to criminalize the incitement of terrorist acts, Security Council resolution 1624 (2005) expressly provides that States must ensure that any measures adopted to implement their obligations comply with all their obligations under international law, in particular human rights law, refugee law and humanitarian law.

136. This principle, which is also reflected in the universal counter-terrorism instruments, has been reaffirmed many times at the international level (including within the framework of the United Nations), is a fundamental element of the UNODC "rule of law" approach to strengthening criminal justice responses to terrorism under the universal legal regime against terrorism and is supported by many regional counter-terrorism and human rights instruments, most notably those elaborated by the Council of Europe, which have been referred to earlier (see section ↑II.D above).[103]

137. It is not possible within the confines of the present publication to fully analyse, in the context of respect for guaranteed human rights to freedom of expression, all the commentaries and judicial authority available on the proper scope and application of offence provisions enacted by countries to criminalize the incitement of terrorist acts.

138. Nevertheless, while the available jurisprudence on the precise scope of international human rights instruments such as article 10, paragraph 1, of the European Convention for the Protection of Human Rights and Fundamental Freedoms and article 19 of the International Covenant on Civil and Political Rights leaves room for ongoing debate, what is clear is that, in practice, striking the right balance between preserving the right to freedom of expression and enforcing criminal legislation targeting the incitement of terrorist acts continues to be a challenge for Governments.

3. Law enforcement powers

139. The investigation of terrorism cases involving the use of the Internet or other related services by suspected terrorists will often necessitate some type of intrusive or coercive search, surveillance or monitoring activity by intelligence or law enforcement agencies. It is therefore important, for the success of any prosecution, that these investigative techniques be properly authorized under national laws and, as always, that supporting legislation uphold fundamental human rights protected under international human rights law.

[103] See the reports of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism to the Human Rights Council and the General Assembly, in which the Special Rapporteur expressed concerns about the possible effect that legislation targeting incitement might have on freedom of speech and expression by promoting the criminalization of free speech falling short of incitement of terrorism. These views and concerns were highlighted in a written submission made to the expert group meeting by the Office of the United Nations High Commissioner for Human Rights; see also the joint Declaration on Freedom of Expression and the Internet, issued on 1 June 2011 by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the Representative on Freedom of the Media of the Organization for Security and Co-operation in Europe, the Special Rapporteur for Freedom of Expression of the Organization of American States and the Special Rapporteur on Freedom of Expression and Access to Information in Africa of the African Commission on Human and Peoples' Rights, in which they reaffirmed fundamental importance of the right to freedom of expression.

(a) Search, surveillance and interception powers

140. In Israel investigative powers for the collection of digital evidence on the Internet, in both general criminal and terrorism-related cases, are dealt with under the Computers Act of 1995, which defines a few specific powers for gathering digital evidence. The Computers Act amended the Wiretap Act, deeming the acquisition of communications between computers to be a "wiretap", and therefore, making it possible for investigative authorities to obtain judicial permission, or administrative permission in urgent and exceptional cases, to acquire data transferred on communication between computers.

141. In 2007, the Communication Data Act was enacted. The purpose of that statute was to arrange, in a more structured and progressive manner, the accepted practice regarding obtaining non-content data from landline and cellular phone companies, as well as from Internet-access providers. The Act does not apply to Internet-service providers that provide other services, such as information storage, information-sharing, e-mail, social services and so forth. Currently, in cases in which authorities wish to obtain information from Internet-service providers, an old section of the law applies that enables them, in general, to issue a subpoena and obtain information from anyone who has information that might advance the investigation.

142. In 2010, the Government of Israel promoted a bill aimed at codifying investigative powers relating to both physical and digital data. The bill is designed to arrange, in an advanced manner, the gathering of digital evidence. It contains an orderly arrangement of powers that are not currently set forth in Israeli legislation, such as secret searches of computers (in the case of especially serious crimes), obtaining information that is to be stored (in the future) on a certain computer, the manner in which stored e-mails in the possession of the service provider are to be obtained, a search of computer material by administrative authorization under certain circumstances. If passed, these measures would apply to terrorism cases involving use of the Internet.

143. In 2006, the Government of France passed new counter-terrorism legislation facilitating, for the purpose of terrorism-related investigations, the surveillance of communications and police access to communication data from telephone operators, Internet-service providers and Internet cafes.

144. The Law of Combating Terrorism and on Various Provisions Concerning Security and Borders Controls (2006-64 of 23 January 2006) provided that Internet-service providers, Internet cafes, hosting providers and operators must communicate traffic data, called numbers and IP addresses to specialist government agencies in cases related to the investigation of suspected terrorist activities.

145. Under article 6, mobile phone operators and Internet cafes are required to keep records of client connections for 12 months and make these available to police. The law also authorizes the use of surveillance cameras in public spaces such as train stations, churches and mosques, shops, factories and nuclear plants. Article 8 allows police

to automatically monitor vehicles and occupants on French roads and highways (including by taking pictures of vehicle licence plates and occupants) and to monitor people at large public gatherings.[104]

146. More recently, on 14 March 2011, the French Code of Criminal Procedure was amended to provide authorities with additional powers in terrorism investigations. These amendments include the power to requisition documents relevant to an investigation (including the conversion and transfer of computer data), the decryption of protected computer data, numeric infiltration, the capture of computer data (including images), wiretapping and the interception of other communications. Moreover, the law establishes the legal basis for the activities of law enforcement officers engaged in, inter alia, online chat room discussions as part of investigations into crimes related to the incitement of terrorism. This is an important legal issue to which Governments might wish to give consideration. These articles provide French law enforcement authorities with, inter alia, the ability to obtain evidence related to the connection data of e-mails, telephone activity and IP addresses.

147. The expert from China referred to regulations in that country under which the police, when undertaking a criminal investigation involving the use of the Internet, may order the submission by the Internet-service provider and Internet-communication provider of relevant records and data, which they are required to retain by law for 60 days.

148. In the United Kingdom, the Regulation of Investigatory Powers Act 2000 sets out a legal framework regulating the following five types of surveillance activities undertaken by Government agencies:

- Interception of communications (e.g. intercepting telephone calls or accessing the contents of e-mails)
- Intrusive surveillance (e.g. covert surveillance in private premises or vehicles)
- Directed surveillance (e.g. covert surveillance against an identified target in a public place)
- Covert human intelligence sources (e.g. undercover agents)
- Communications data (e.g. records related to communications but not the content of such communications).[105]

149. In addition to setting out the purposes for and procedures by which such activities must be authorized, the Act obliges surveillance authorities to consider whether the exercise of these powers and the interference with the rights of the individuals under surveillance are proportionate and to take steps to avoid what is known as "collateral intrusion", whereby the rights of parties other than those being targeted are affected.

[104] www.edri.org/edrigram/number4.2/frenchlaw.

[105] "Summary of surveillance powers under the Regulation of Investigatory Powers Act", National Council for Civil Liberties.

The Act also makes it an offence for parties holding encryption keys for targeted communications to withhold such keys from authorized agencies.[106]

150. In 2000, the Government of India passed the Information Technology Act 2000, which it amended in 2008, to provide for the offence of "cyber-terrorism" (section 66F) and other Internet-related issues. Section 67C (1) of the Act deals with the issue of data retention, stipulating that regulated providers "shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe" and making it an offence (punishable by up to three years of imprisonment and fines) to knowingly contravene this obligation.

151. Section 69 (1) of the Act provides Government authorities with the power to issue directions for the "interception, monitoring, and decryption of any information generated, transmitted, received or stored in any computer resource" and sets out the legal obligations and safeguards attaching to such State actions, while Section 69A (1) provides State agencies with the power to issue directions for blocking public access to any information through computer resources if they consider it necessary or expedient to do so, in the interests of India's sovereignty, integrity, security and international relations, or to prevent the incitement of related "cognizable" offences, including terrorism. Finally, Section 69B provides designated State agencies with the power to monitor, collect and store data traffic or information generated, transmitted or received via any computer resource.

152. In New Zealand, the Search and Surveillance Act 2012 updates, consolidates and harmonizes the powers of law enforcement agencies relating to search, surveillance and interception of communications to address new forms of technology. The Act creates a new definition of the term "computer system searches", extending it to include the search of computers that are not internally connected to, but are able to access, a network remotely.

153. In order to strengthen legal safeguards, the Act makes it clear that remote-access searching of computers is permitted in only two situations: when a computer had the capability to lawfully access a computer system which is the subject of the search and is therefore considered part of that system; and when there was no physical location to search (e.g. in the case of web-based e-mail that the user accesses from various locations, such as Internet cafes). The Act also provides that, when police undertake authorized remote access searches of Internet data facilities, they must provide electronic notification of the search via e-mail, sent to the e-mail address of the facility being searched.

(b) Issues associated with the provision of interception capability

154. When undertaking electronic monitoring, surveillance or interception activities, authorities will require the cooperation of operators that provide public telecommunications or related services. While in many cases private sector operators are willing to

[106] Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007), p. 216.

provide assistance to law enforcement agencies undertaking their lawful functions, clearly there are limits to the time and resources they are willing to expend on an entirely gratis basis. It is therefore desirable that Governments provide a clear legal basis for the obligations placed on private sector parties, including the technical specifications required of their networks and how the cost of providing such capabilities is to be met.

155. In Israel, section 13 of the Communication Law, 1982, states that the Prime Minister may direct Internet-access providers, within Israel, to carry out technological modifications as required by security forces (defined as including police, security and other special services) for the purpose of counter-terrorism activities. The law applies only to Internet-access providers, who under Israeli law receive their licences from the Ministry of Communications. It does not apply to data storage service providers or content management providers operating within Israel, as these operators do not require a licence from the Ministry.

156. In New Zealand, the Telecommunications (Interception Capability) Act 2004 clarifies the obligations of network operators to assist authorized government agencies in undertaking interception operations or providing authorized call-associated data. The Act obliges network operators to ensure that every public telecommunications network or service that it owns, controls or operates has interception capability. Networks or services are deemed to have this capability when authorized government agencies are able to intercept telecommunications or services in a manner that identifies and intercepts only targeted telecommunications, provides call-associated data and content (in a usable form) and enables unobtrusive, timely and efficient interception in a manner that protects the privacy of, and avoids undue interference with, other telecommunications users. The Act also obliges network operators to provide the means of decrypting any telecommunication carried over their network if the content is encrypted and the network operator has provided that encryption facility.

157. Recognizing the time and expense involved for some network operators to comply with these requirements, the Act provided affected operators with periods of 18 months to five years (depending on the status of the network) within which to incorporate this capability. Moreover, the Government agreed to meet the costs of incorporating interception capability into those networks already in operation at the date of commencement that lacked the necessary interception capability.

158. In Brazil, Federal Law No. 9.296 of 1996, together with article 5 (XII) of the Federal Constitution of 1988, regulates official wiretapping undertaken by authorized government agencies. While recognizing the inviolable nature of telecommunications, the laws provide, subject to judicial authorization, specific derogations for the purpose of criminal investigations or penal processes. The law sets out the procedures to be followed in wiretap cases, which take place under supervision of a judge. Once executed, the results of the wiretap are transcribed and provided to the judge, along with a summary of all actions taken pursuant to the authority (article 6).

159. In order to meet their legal obligations, telecommunications companies have been required to establish and train specialized units and invest in necessary technology. With regard to the costs of providing interception capability, it falls to the

telecommunications companies to provide the necessary technical resources and staff to support authorized interception activities. This approach reflects the fact that under Brazil's Constitution telecommunications companies operate under a government concession and provision of telecommunications services is considered a public service.

160. In Indonesia, following the Bali bombings in 2002, the Government passed anti-terrorism legislation which permits law enforcement and security agencies, for the purpose of terrorism-related investigations, to intercept and examine information that is expressed, sent, received or stored electronically or with an optical device. In relation to the retention period of Internet or log files, this subject is regulated under Law No. 11 of 2008 on Electronic Information and Transactions, specifically article 6, paragraph 1, subparagraph a, which obliges every system operated by an electronic system provider to reproduce in complete form any electronic information and/or electronic document for the duration of the retention period stipulated under the law.

161. In Algeria, in 2006, the Government adopted a law permitting microphone and video surveillance and the interception of correspondence, if authorized and executed under the direct control of the prosecutor. The same law authorizes the technique of infiltration for the purpose of investigating terrorism or organized crime and permits the agent to commit specified minor infractions in the course of the infiltration. The secrecy of the agent's identity is carefully protected by law, but the infiltration must be conducted under the authority of the prosecutor or investigating magistrate.[107]

162. In Malaysia, the Communications and Multimedia Act 1998 contains several provisions pertaining to the regulation of the Internet and related criminal investigations. For example, section 249 of the Act dealing with the issue of access to computer data during searches provides that access includes obtaining "passwords, encryption or decryption codes, software or hardware and any other means required to enable comprehension of computerized data".

163. In addition, chapter 4 of the Act, relating to national interest matters, imposes a general obligation on Internet service operators to use "best endeavours" to ensure that the network facilities they provide are not used for the commission of any offence under the law of Malaysia (Section 263) and provides that the responsible minister may determine, specifying related technical requirements, that a licensee or class of licensees shall implement the capability to allow authorized interception of communications (Section 265).

164. Chapter 2 of the Act relates to the issue of offensive content, and prohibits content application service providers and any persons using such services from providing content that is "indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person" (Section 211). Persons contravening these obligations commit an offence and are liable to a fine not exceeding 50,000 ringgit (approximately US$16,200) or to imprisonment for a term not exceeding one year, or both, and shall also be liable to an ongoing fine of 1,000 ringgit (approximately

[107] United Nations Office on Drugs and Crime, *Digest of Terrorist Cases*, para. 215.

US $325) for every day or part of a day during which the offence is continued after conviction. Section 212 of the Act provides for the designation of an industry body to be a forum for the development of an industry code relating to content.

165. In the United States, telecommunications operators are currently obliged, under the Communications Assistance to Law Enforcement Act 1994, to provide interception capability for telephone and broadband networks.

(c) Regulation of Internet cafes

166. There is evidence that terrorists have in some cases used Internet cafes to carry out actions associated with terrorism; however, there is no data available on the proportion this type of activity in relation to legitimate Internet activity conducted through these services.

167. The issue of the extent to which Governments should, for counter-terrorism purposes, regulate Internet or cybercafes is a complex issue, closely linked to human rights issues. Internationally, there is a divergence of approaches. In some States, including Egypt, India, Jordan and Pakistan, Governments apply specific legislative or regulatory measures, which oblige operators of Internet cafes to obtain, retain and, upon request, produce photo identification, addresses and usage/connection data of customers to law enforcement agencies.

168. While Governments can impose obligations on operators of Internet cafes aimed at restricting misuse of those services by terrorists, the utility of such measures is open to debate, especially when facilities such as other publicly available Internet services (e.g. computers at public libraries or public wireless fidelity (Wi-Fi) zones) that offer similar opportunities for the anonymous use of the Internet by terrorists. It is noted that in 2005, the Government of Italy imposed regulatory obligations on operators of Internet cafes relating to the identification of customers; however, these regulations were abolished in late 2010, owing in part to concerns about the effect that this form of regulation might have on the development of Internet services and their uptake by legitimate users.

(d) Content control

169. The issue of the extent to which Governments should regulate terrorism-related content on the Internet is highly contentious. Approaches vary considerably, with some States applying strict regulatory controls on Internet and other related service providers, including in some cases the use of technology to filter or block access to some content. Others adopt a lighter regulatory approach, relying to a greater extent on self-regulation by the information sector.

170. In the article "Terrorism and the Internet: should web sites that promote terrorism be shut down?",[108] Barbara Mantel notes that "most Internet service providers, web

[108] Barbara Mantel, "Terrorism and the Internet: should web sites that promote terrorism be shut down?", *CQ Global Researcher*, vol. 3, No. 11 (November 2009).

hosting companies, file-sharing sites and social networking sites have terms-of-service agreements that prohibit certain content". For example, she notes, Yahoo's Small Business Web hosting service specifically forbids users from utilizing the service to provide material support or resources to any organization(s) designated by the United States Government as a foreign terrorist organization. To that extent, there is an element of self-regulation within the information society.

171. When assessing the approach and level of intervention in this area, Governments need to take a number of factors into account, including the location where content is hosted, constitutional or other safeguards relating to the right to freedom of expression, the content itself and the strategic implications from an intelligence or law enforcement perspective of monitoring or infiltrating certain sites or rendering them inaccessible.[109]

172. In the United Kingdom, an innovative tool, available to authorities in dealing with cases involving potential acts of incitement over the Internet, is contained in section 3 of the Terrorism Act 2006, which provides police with the power to issue a "take down" notice to persons associated with operating websites or other Internet content.

173. Section 3 of the Act applies to cases involving offences under sections 1 or 2 of that Act in which "*(a)* a statement is published or caused to be published in the course of, or in connection with, the provision or use of a service provided electronically; or *(b)* conduct falling within section 2(2) [dissemination of a terrorist publication] was in the course of, or in connection with, the provision or use of such a service".

174. Section 3(2) provides that, if the person upon whom the notice has been served fails to remove the terrorism-related content, and if he or she is subsequently charged with offences under sections 1 or 2 of the Terrorism Act 2006 in relation to it, then a rebuttable assumption may be made at trial that the content in question had his or her endorsement.

175. Despite the availability of these "take down" notices as a preventive measure, in practice this power has not yet been used. In most cases, especially when the offending content was hosted on the websites of third parties, it tended to breach the terms and conditions of the service provider, and authorities were able to successfully negotiate the removal of the offending content. In fact, in the United Kingdom the specialized Counter Terrorism Internet Referral Unit coordinates national responses to referrals from the public, as well as from Government and industry, on terrorism-related Internet content and acts as a central, dedicated source of advice for the police service.

[109] Catherine A. Theohary and John Rollins, "Terrorist use of the Internet: information operations in cyberspace", Congressional Research Service report (8 March 2011), p. 8.

4. International cooperation

176. States are obliged, under many different international, regional, multilateral and bilateral instruments related to terrorism and transnational organized crime, to establish policies and legislative frameworks to facilitate effective international cooperation in the investigation and prosecution of these types of cases.

177. In addition to having policies and legislation that establish criminal offences necessary to satisfy dual criminality requirements, States should enact comprehensive legislation that provides their authorities with a legal basis for international cooperation with foreign counterparts in transnational terrorism-related investigations. In cases involving the use of Internet, it is highly likely that effective international cooperation, including the ability to share information, including Internet-related data, will be a key factor in the success of any criminal prosecution.

178. Issues related to international cooperation in terrorism cases are dealt with in closer detail in chapter V below.

IV. Investigations and intelligence-gathering

A. Tools in the commission of terrorist offences involving the Internet

179. Technological advancements have provided many sophisticated means by which terrorists may misuse the Internet for illicit purposes. Effective investigations relating to Internet activity rely on a combination of traditional investigative methods, knowledge of the tools available to conduct illicit activity via the Internet and the development of practices targeted to identify, apprehend and prosecute the perpetrators of such acts.

180. A case from France illustrates how different types of investigative techniques, both traditional and specifically relating to digital evidence, are employed in unison to compile the necessary evidence to successfully prosecute terrorist use of the Internet.

Public Prosecutor v. Arnaud, Badache, Guihal and others

This French case involves several defendants: Rany Arnaud, Nadir Zahir Badache, Adrien Luciano Guihal and Youssef Laabar, who were convicted on 26 January 2012 by the Tribunal Correctionnel de Paris and sentenced to terms of imprisonment ranging from 18 months to 6 years for, inter alia, disseminating terrorist-related material.

Arnaud, Badache and Guihal were arrested in France in December 2008 after Arnaud, who operated under the username of "Abdallah", posted messages calling for jihad against France on a propaganda website, minbar-sos.com:

> "Do not forget that France keeps on fighting our brothers in Afghanistan and that you are in a land of war, rush up to martyr as soon as you can, boycott their economy, squander their wealth, do not support their economy and do not participate in the financing of their armies."

As a result of the posting, authorities had intercepted Arnaud's Internet account, put him under physical surveillance and tapped his phone line. After arresting Mr. Arnaud, investigators forensically examined the content of the computers used by him and found that he had conducted research on matters relating to the commission of terrorist acts, for example products capable of being used to make explosives and incendiary devices, identifying possible targets and tracking the activities of a company which used ammonium nitrate. The enquiries revealed that Arnaud had recruited Guihal and Badache, taken part in meetings and discussions to prepare an attack, made contact with people involved in jihadist movements to seek help in carrying it out and received remittances to fund it. These acts constituted crimes pursuant to articles 421-2-1, 421-1, 421-5, 422-3, 422-6 and 422-7 of the French Criminal Code, and articles 203 and 706-16 et. seq. of the Code of Criminal Procedure.

The Court found that the plan in which Mr. Arnaud had allegedly taken part, in association with the other offenders, which consisted of placing explosives on a truck that would explode upon reaching the target, posed a particularly high threat to public policy. He was thus sentenced to six months imprisonment on charges relating to participating in a group committing criminal acts for the purpose of preparing a terrorist attack, possession of several fraudulent documents and fraudulent use of administrative documents evidencing a right, identity or quality or granting an authorization. On the same charge, Mr. Badache was sentenced to two years of imprisonment, with six months suspended, while Mr. Guihal was sentenced to four years, with one year suspended. Mr. Laabar, who faced trial for other related acts, was sentenced to 18 months incarceration.

181. The investigation and prosecution of cases involving digital evidence requires specialist criminal investigation skills, as well as the expertise, knowledge and experience to apply those skills in a virtual environment. While the admissibility of evidence is ultimately a question of law, and therefore within the remit of the prosecutors, investigators should be familiar with the legal and procedural requirements to establish admissibility for the purposes of both domestic and international investigations. A sound working knowledge of the requirements of applicable rules of evidence, and in particular with respect to digital evidence, promotes the collection of sufficient admissible evidence by investigators to support the successful prosecution of a case. For example, the procedures used in gathering, preserving and analysing digital evidence must ensure that a clear "chain of custody" has been maintained from the time it was first secured, so that it could not have been tampered with from the moment of its seizure until its final production in court.[110]

1. Internet-based communication

(a) Voice-over-Internet protocol

182. Over the past decade, applications that allow users to communicate in real time using voice-over-Internet protocol (VoIP), video chat or text chat have grown in popularity and sophistication. Some of these applications offer advanced information-sharing functions, for example allowing users to share files or giving them the ability to remotely view another user's onscreen activity in real time. VoIP in particular has become increasingly used as an effective means to communicate via the Internet. Well-known VoIP service providers include Skype and Vonage, which operate by converting analogue sound into a compressed, digital format, enabling transfer of the digital packets of information via the Internet, using relatively low bandwidth connections.

183. As VoIP telephony involves the transmission of digital data packets, rather than analogue signals, and service providers typically generate subscriber invoices related to Internet usage based on aggregate data volume, computer-to-computer VoIP calls are not invoiced on a per-call basis, as is the practice with traditional mobile and fixed-line

[110] See, for example, Association of Chief Police Officers (United Kingdom), *Good Practice Guide for Computer-Based Electronic Evidence*. Available from www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

telephone calls. This difference in billing practices may have a significant impact on investigations involving VoIP communications, as it makes it more difficult for law enforcement authorities to corroborate such communications with markers relating, for example, to the time of the call and the location of the participants. Other indicators, however, such as the timing and volume of Internet data traffic, may also provide a means to identity perpetrators of illicit Internet activity (see para. 205 below). Additionally, while the origin and destination of conventional telephone calls may be routed via fixed-line switches or cellular communication towers, which leave geolocational traces, wholly Internet-based VoIP communications, conducted for example via wireless networks, may pose challenges in the context of an investigation. Further complicating factors arising out of the use of VoIP technology may involve, inter alia, the routing of calls via peer-to-peer networks and the encryption of call data (discussed in greater detail in section IV.A.2 below).[111]

184. Duly submitted information requests to VoIP service providers may, however, still provide valuable identifying information such as a user's IP address, e-mail address or payment details.

(b) Electronic mail

185. Web-based e-mail services also provide terrorists with a covert means of communication, which can be misused for illicit purposes. E-mail messages sent between parties typically contain a number of elements which may be of investigative value. A typical e-mail may be comprised of the envelope header, the message header, the message body and any related attachments. While only an abbreviated version of the envelope header may be displayed, in accordance with the settings of the applicable software, the complete envelope header generally contains a record of each mail server through which the message transited on the way to the final recipient, as well as information regarding the IP address of the sender.[112] The information contained in the envelope header is less susceptible to tampering (although not impermeable) than that in the message header, which generally consists of user-provided information in fields such as "To", "From", "Return-Path", "Date" and "Time", as displayed on the device from which the message is being sent.[113]

186. One commonly used technique to reduce electronic traces between parties, and therefore the likelihood of detection, is communication through the use of saved, unsent messages in the draft folder of the e-mail account. This information is then available to multiple parties using a shared password to access the account. Additional steps may also be taken to avoid detection, for example use of a remote public access terminal, such as in an Internet cafe, to access the draft message. This method was used in connection with the Madrid terrorist bombings in 2004.

[111] Written submission of expert from the Raggruppamento Operativo Speciale of the Carabinieri of Italy.

[112] United States, Department of Justice, Office of Justice Programs, National Institute of Justice, *Investigations Involving the Internet and Computer Networks* (2007), p. 18 ff.

[113] Ibid., p. 20.

187. It is also possible to employ anonymizing techniques (discussed in greater detail in section ⇑IV.A.2 below) in connection with e-mail communications, for example by disguising the IP address associated with the sender of an e-mail. Anonymizing mail servers may also be used, which remove identifying information from the envelope header prior to forwarding it to the subsequent mail server.

The importance of international cooperation in investigating terrorism-related Internet activities

The expert from the Italian Raggruppamento Operativo Speciale (Special Operations Group) of the Carabinieri of Italy outlined the key role of international cooperation and specialized investigative techniques in the investigation of the use of the Internet for terrorist purposes by the Turkish-based extremist organization, The Revolutionary People's Liberation Party-Front (DHKP-C). Close collaboration between law enforcement officials in Turkey and Italy enabled the Italian investigators to identify the encryption techniques and other data security measures used by DHKP-C members to exchange information in furtherance of terrorist purposes, including via online mail services. In particular, DHKP-C members used the stenography software Camouflage to hide data within images in JPEG and GIF files, and WinZip software to encrypt files, which were included as attachments to e-mail communications (see section IV.A.2 below). Italian investigators intercepted or otherwise obtained encryption passwords and identified relevant programs to assist in deciphering communications. Additional information was obtained through forensic computer analysis, using EnCase software (See section IV.C below) and traditional investigative techniques, to enable investigators to obtain digital evidence from the computers of a suspect under investigation. The results of this investigation, together with extensive cross-border cooperation, led to the arrest, in April 2004, of 82 suspects in Turkey and an additional 59 suspects in Belgium, Germany, Greece, Italy and the Netherlands.

(c) Online messenger services and chat rooms

188. Online messenger services and chat rooms provide additional means of real-time communication, with varying degrees of potential anonymity. Online messenger services typically involve bilateral communications, while chat rooms offer open communication among a group of individuals. Registration for online messenger services is typically based on unverified, user-provided information; however, some Internet services also log the IP address in use at the time of registration, which may be requested by law enforcement authorities, subject to applicable legal safeguards. Communications are usually identified by a unique screen name, which may be assigned permanently upon registration or limited to a particular online session. Information shared during an online messenger session is not generally recorded by the service provider and therefore may not be available for retrieval after the online session is terminated, subject to recovery facilitated by forensic analysis of a participant's hard drive.

189. Password-protected online chat rooms may be used by terrorist organizations and sympathizers to promote a sense of community within a global environment. Chat room messages may be subject to more monitoring and recordkeeping by the service provider than bilateral messaging are, increasing the likelihood of potentially obtaining

documentary evidence in connection with investigations.[114] In some jurisdictions, law enforcement personnel may, subject to certain conditions, covertly register for, and participate in, chat room discussions under a pseudonym in connection with an investigation.

190. For example, in France, article 706 of the Code of Criminal Procedure provides for the authorization by the prosecutor or investigative judge of such infiltration operations in connection with offences committed through electronic communications (see discussion in section III.C.3*(a)*). The aim of such operations may be, inter alia, to gather intelligence or otherwise take proactive action in connection with a perceived terrorist threat. Due care should be taken, however, at the inception of the operation to ensure that any infiltration of online chat room or other Internet-based discussions is conducted in a manner that would not support a defence of entrapment, based on the assertion that a government authority induced a suspect to commit a crime that he or she was not predisposed to commit.

(d) File-sharing networks and cloud technology

191. File-sharing websites, such as Rapidshare, Dropbox or Fileshare, provide parties with the ability to easily upload, share, locate and access multimedia files via the Internet. Encryption and anonymizing techniques employed in connection with other forms of Internet communication are similarly applicable to files shared via, inter alia, peer-to-peer (P2P) and File Transfer Protocol (FTP) technology. For example, in the *Hicheur* case (see para. 20 above), evidence was presented that digital files in support of terrorist activities were shared via Rapidshare, after being encrypted and compressed for security. Some file-sharing networks may maintain transfer logs or payment information, which may be relevant in the context of an investigation.

192. Cloud computing is a service which provides users with remote access to programs and data stored or run on third-party data servers. As with file-sharing, cloud computing provides a convenient means to securely store, share and distribute material online. The use of cloud technology to access remotely stored information reduces the amount of data stored locally on individual devices, along with the corresponding ability to recover potential evidence in connection with an investigation of terrorist use of the Internet.

193. The data servers used to provide these services may also be physically located in a different jurisdiction from that of the registered user, with varying levels of regulation and enforcement capabilities. Close coordination with local law enforcement authorities may therefore be required to obtain key evidence for legal proceedings.

2. Data encryption and anonymizing techniques

194. Data encryption refers to the protection of digital information from disclosure by converting it into ciphertext, using a mathematical algorithm and an encryption key,

[114] Ibid., pp. 34 ff.

so that it is intelligible only to the intended recipient. Encryption tools may be hardware- or software-based, or a combination of both. Once encrypted, a password, a passphrase, a "software key" or a physical access device, or some combination thereof, may be required to access the information. Encryption may be employed in respect of both "at-rest" data, contained in storage devices such as computer hard drives, flash media and smart phones, and "in transit" data, transmitted over the Internet, for example by means of VoIP and e-mail communications. Some examples of common software-based encryption tools include those integrated into computer operating systems or applications, as well as stand-alone software such as Pretty Good Privacy and WinZip.[115] In a case in Brazil, an investigation was launched on the basis of international cooperation and information-sharing against a suspect alleged to be participating in, moderating and controlling the operations of a jihadist website affiliated with recognized terrorist organizations, notably Al-Qaida. This website hosted videos, text and messages from leadership-level extremist militants, which had been translated into English to reach a broader audience, and was also used to conduct fundraising activities and racially motivated propaganda campaigns. The police operation that led to the detention of the suspect was targeted to take the suspect by surprise, while he was connected to the Internet and actively engaged in activities relating to the website. By apprehending the suspect while his computer was on and the relevant files were open, investigators were able to bypass the cryptographic symmetric keys and other encryption and security features used by the suspect and his associates. Investigators were therefore able to access digital content that might have been otherwise unavailable or more difficult to obtain if the computer had been secured while it was shut off.

195. Internet activity, or the identity of the associated users, can also be disguised through advanced techniques, including masking the source IP address, impersonating another system's IP address or redirecting Internet traffic to an obscured IP address.[116] A proxy server enables users to make indirect network connections to other network services. Some proxy servers allow the configuration of a user's browser to automatically route browser traffic through a proxy server. The proxy server requests network services on behalf of the user and then routes the delivery of the results again through a proxy. Varying levels of anonymity may be facilitated by the use of proxy servers. A proxy may obscure the identity of a user by fulfilling requests for network services without revealing the IP address from which the request originates, or by intentionally providing a distorted source IP address. For example, applications such as The Onion Router may be used to protect the anonymity of users by automatically rerouting Internet activity via a network of proxy servers in order to mask its original source. Rerouting network traffic via multiple proxy servers, potentially located in different jurisdictions, increases the degree of difficulty of accurately identifying the originator of a transmission.

196. Alternatively, a suspect may hack into a legitimate organization's IP address and browse the Internet using the hacked address. Any traces of such activity would be

[115] United States, Department of Justice, Office of Justice Programs, National Institute of Justice, *Investigative Uses of Technology: Devices, Tools and Techniques* (2007), p. 50.

[116] National Institute of Justice, *Investigations Involving the Internet and Computer Networks*, p. 9.

linked to the IP address of the compromised organization. A suspect may also access a website through a compromised computer or store malware (used, for example, to obtain credit card or other personal financial information) on compromised websites in an effort to avoid being identified.

197. There is a variety of software programs that are available to disguise or encrypt data transmitted over the Internet for illicit purposes. These programs may include the use of software such as Camouflage to mask information through steganography or the encryption and password protection of files using software such as WinZip. Multiple layers of data protection may also be employed. For example, Camouflage allows one to hide files by scrambling them and then attaching them to the end of a cover file of one's choice. The cover file retains its original properties but is used as a carrier to store or transmit the hidden file. This software may be applied to a broad range of file types. The hidden file may, however, be detected by an examination of raw file data, which would show the existence of the appended hidden file.[117]

198. In the United Kingdom, it is a criminal offence under the Regulation of Investigatory Powers Act 2000 to refuse to hand over an encryption key when required. Care must be taken, however, to ensure that suspects do not seek to evade the provision by utilizing several layers of encryption and multiple keys to protect different data sets. For example, a setting of TruCrypt, a common free encryption tool, allows a suspect to encrypt a hard drive and create two passwords: one for the "clean" drive and the other containing the incriminating material. This can be circumvented by ensuring that the forensic examination of the hard drive takes into consideration whether there is any "missing volume" of data. Additionally, offences of this nature are usually summary offences, which carry maximum penalties of six months imprisonment. In the United Kingdom, however, when the case involves national security issues, the maximum penalty increases to two years of imprisonment.

3. Wireless technology

199. Wireless networking technology allows computers and other devices to access the Internet over a radio signal rather than via a hard-wired connection, such as a cable. To access a Wi-Fi network, a degree of proximity to the network resources must be maintained, which is dependent upon the strength of the wireless signal. Wireless networks may be configured to allow open access to the Internet, without registration, or may be secured with the use of a passphrase or varying levels of encryption. Wireless networks, registered to individuals, businesses or public entities, can often be accessed from public locations. Anonymous access to secured or unsecured Wi-Fi networks may allow perpetrators to mask links between Internet activity and identifying information.

200. In addition, service providers such as Fon have emerged in recent years, which enable registered users to share a portion of their residential Wi-Fi bandwidth with

[117] Written submission of expert from the Raggruppamento Operativo Speciale of the Carabinieri of Italy.

other subscribers, in exchange for reciprocal access to Wi-Fi networks of subscribers worldwide. Activity conducted over a shared Wi-Fi network significantly complicates the process of attribution of an act to a single, identifiable perpetrator in the course of an investigation.[118]

201. A novel technique relates to the use of software-defined high performance High-frequency (HF) radio receivers routed through a computer. In this way, no data is exchanged through a server and no logs are created. It is more difficult for law enforcement and intelligence agencies to intercept communications sent using this method, both in relation to finding the location of the transmitters and with respect to predicting in real time the frequency at which the communications are transmitted.

B. Investigations of terrorist cases involving the Internet

1. Systematic approach to investigations involving the Internet

202. There is a vast range of data and services available via the Internet which may be employed in an investigation to counter terrorist use of the Internet. A proactive approach to investigative strategies and supporting specialist tools, which capitalizes on evolving Internet resources, promotes the efficient identification of data and services likely to yield the maximum benefit to an investigation. In recognition of the need for a systematic approach to using technological developments relating to the Internet for investigative purposes, the Raggruppamento Operativo Speciale of the Carabinieri of Italy developed the following guidelines, which have been disseminated through the University College Dublin, master's programme in forensic computing and cybercrime (see section IV.G below) and implemented by domestic enforcement authorities of many member States of the International Criminal Police Organization (INTERPOL) and the European Police Office (Europol):

Protocol of a systematic approach

- *Data collection:* This phase involves the collection of data through traditional investigative methods, such as information relating to the suspect, any co-inhabitants, relevant co-workers or other associates and information compiled through conventional monitoring activities of channels of communication, including in relation to fixed-line and mobile telephone usage.
- *Research for additional information available via Internet-based services:* This phase involves requests to obtain information collected and stored in the databases of web-based e-commerce, communications and networking services, such as eBay, PayPal, Google and Facebook, as well as using dedicated search engines such as www.123people.com. Data collected by these services through commonly used Internet "cookies" also provide key information regarding multiple users of a single computer or mobile device.

[118] Ibid.

- The activities in phases *(a)* and *(b)* above provide information that may be combined and cross-referenced to build a profile of the individual or group under investigation and made available for analysis during later stages of the investigation.
- *VoIP server requests:* In this phase, law enforcement authorities request information from VoIP service providers relating to the persons under investigation and any known affiliates or users of the same networking devices. The information collected in this phase may also be used as a form of "smart filter" for the purposes of verifying the information obtained in the two prior phases.
- *Analysis:* The large volume of data obtained from VoIP servers and the providers of various Internet services are then analysed to identify information and trends useful for investigative purposes. This analysis may be facilitated by computer programs, which may filter information or provide graphic representations of the digital data collected to highlight, inter alia, trends, chronology, the existence of an organized group or hierarchy, the geolocation of members of such group, or factors common among multiple users, such as a common source of financing.
- *Identification of subjects of interest:* In this phase, following smart analysis of the data, it is common to identify subjects of interest based, for example, on subscriber information linked to a financial, VoIP or e-mail account.
- *Interception activity:* In this phase, law enforcement authorities employ interception tactics similar to those used for traditional communication channels, shifting them to a different platform: digital communication channels. Interception activity may be undertaken in connection with telecommunications services, such as fixed-line broadband, mobile broadband and wireless communications, as well as with regard to services provided by ISPs, such as e-mail, chat and forum communication services. In particular, in recent years experience has revealed vulnerabilities in new communications technologies which may be exploited for investigative or intelligence-gathering purposes. Due care should be taken with respect to ensuring the forensic integrity of the data being gathered and the corroboration, to the extent possible, of any intelligence gathered with objective identifiers such as GPS coordinates, time stamps or video surveillance.

Where permitted by domestic law, some law enforcement authorities may also employ digital monitoring techniques facilitated by the installation of computer hardware or applications such as a virus, a "Trojan Horse" or a keystroke logger on the computer of the person under investigation. This may be achieved through direct or remote access to the relevant computer, taking into consideration the technical profile of the hardware to be compromised (such as the presence of antivirus protections or firewalls) and the personal profile of all users of the device, targeting the least sophisticated user profile.

203. The Korean National Police Agency has responded to the need to standardize domestic law enforcement practices relating to digital forensics by developing and implementing two manuals: *the Standard Guidelines for Handling Digital Evidence and the Digital Forensics Technical Manual*. The *Standard Guidelines* detail seven steps in the proper handling of digital evidence: preparation; collection; examination; evidence request, receipt, and transport; analysis; reporting; and preservation and evidence management. The *Digital Forensics Technical Manual* outlines required procedures and the appropriate approach to the collection of digital evidence, including with reference to establishing the appropriate environment, forensic tools and equipment; preparatory steps such as the set-up of hardware and software, network connections and

time-accuracy; measures to secure the maximum amount of digital evidence; independent analysis of secured data; and the production of the final report.[119]

2. *Tracing an IP address*

204. The IP address associated with an Internet communication is an important identifier, and therefore key in investigations into terrorist use of the Internet. An IP address identifies the specific network and device being used to access the Internet. The IP addresses can be dynamic, temporarily assigned for the duration of an online session from a pool of addresses available to an ISP, or static (assigned on a fixed basis, as in the case of website addresses). Dynamic IP addresses are typically assigned to ISPs within region-based blocks. Therefore, in the absence of the intervening use of anonymizing or other techniques, a dynamic IP address can often be used to identify the region or State from which a computer is connecting to the Internet.

205. Further, in response to a duly made request, an ISP can often identify which of its subscriber accounts was associated with an IP address at a specific time. Traditional investigative methods may then be used to identify the person physically in control of the subscriber account at that time. In the *Hicheur* case (see para. 20 above), the defendant was identified by tracing a static IP address used to access an e-mail account under surveillance. A request made to the relevant ISP enabled authorities to link the IP address to a subscriber account used by multiple occupants of a household, including the defendant. By intercepting the data traffic for this subscriber account, investigators were also able to establish links between the IP address and activity on a pro-jihadist website which, inter alia, distributed materials for the purpose of physically and mentally training extremist combatants. In particular, investigators were able to correlate the times at which multiple connections were made to the website's discussion forum with concurrent increases in Internet data volume linked to the defendant's personal e-mail account.[120]

206. Given the time-sensitive nature of investigations involving the Internet and the risk of alteration or deletion of digital data owing to, inter alia, potential server capacity constraints of the relevant ISP or applicable data protection regulations, consideration should also be given to the appropriateness of a request to the ISP to preserve data relevant to the criminal investigation, pending fulfilment of the necessary steps to secure the data for evidentiary purposes.

207. In the case of an investigation relating to a website, the relevant domain name must first be resolved to an IP address. In order to identify the associated IP address, which is in turn registered with the Internet Corporation for Assigned Names and Numbers (ICANN), several dedicated utilities may be used. Common utilities, which

[119] Written submission of expert from the Republic of Korea.

[120] Judgement of 4 May 2012, Case No. 0926639036 of the Tribunal de Grande Instance de Paris (14th Chamber/2), p. 7 et. seq.

are available via the Internet, include "whois" and "nslookup".[121] For example, a whois query related to the domain name of the United Nations Office on Drugs and Crime (www.unodc.org) produces the following result:

Domain ID: D91116542-LROR

Domain Name: UNODC.ORG

Created On: 11-Oct-2002 09:23:23 UTC

Last Updated On: 19-Oct-2004 00:49:30 UTC

Expiration Date: 11-Oct-2012 09:23:23 UTC

Sponsoring Registrar: Network Solutions LLC (R63-LROR)

Status: CLIENT TRANSFER PROHIBITED

Registrant ID: 15108436-NSI

Registrant Name: Wiessner Alexander

Registrant Organization: United Nations Vienna

Registrant Street1: Vienna International Centre, P.O. Box 500

Registrant City: A-1400 Wien Vienna AT 1400

Registrant Postal Code: 99999

Registrant Country: AT

Registrant Phone: +43.1260604409

Registrant FAX: +43.1213464409

Registrant E-mail: noc@unvienna.org

These details are provided by the registrant, however. As a result, further steps may also be required to independently verify the accuracy of registrant details. Domains may also be leased or otherwise under the control of a party other than the registrant.

208. Persons investigating the use of the Internet for terrorist purposes should also be aware that online activity related to an investigation may be monitored, recorded and traced by third parties. Due care should therefore be taken to avoid making online enquiries from devices which can be traced back to the investigating organization.[122]

3. Specialized investigative utilities and hardware

209. Investigators with the appropriate technical background have available to them a range of specialized utilities and hardware. Some, such as "Ping", and "Traceroute",

[121] National Institute of Justice, *Investigations Involving the Internet and Computer Networks*, p. 10.

[122] Ibid.

may be integrated into the operating system of a device under investigation. Ping, for example, may be used to send a signal to a computer connected to the Internet to determine whether it is connected at a given time, subject to the interference of any firewalls or other network configuration. Similarly, Traceroute may show the path between two networked computers, which may assist in determining the physical location.

210. Other programs that may be used, subject to domestic laws and regulations regarding, inter alia, access to the device and interception of communications, include "trojan horses" or Remote Administration Trojans (RATs), which may be introduced covertly into a computer system to collect information or to enable remote control over the compromised machine. Keystroke monitoring tools may also be installed on a device and used to monitor and record keyboard activity. Keystroke loggers, in the form of hardware or software, assist in obtaining information relating to, inter alia, passwords, communications and website or localized activity undertaken using the device being monitored. In addition, data packet "sniffers" may be used to gather data relevant to an investigation. Sniffers, which may be a device or software, gather information directly from a network and may provide information relating to the source and content of communications, as well as the content communicated.

C. Forensic data preservation and recovery

211. An important part of the acquisition of evidence in connection with cases involving the use of the Internet for terrorist purposes concerns the recovery of stored digital data. The two primary goals in this data recovery exercise are the retrieval of relevant evidence for the purposes of effective investigation and prosecution and the preservation of the integrity of the data source and the chain of custody to ensure its admissibility in court proceedings. In order to identify the best method of evidence preservation, it is important to distinguish between volatile data, which stored on devices, such as the random access memory (RAM) of devices, and may be irretrievably lost if there is a disruption in the power supply, and non-volatile data, which is maintained independently of the power supply to the device. For example, the act of switching off a computer may alter the data contained on the storage discs and RAM, which may contain important evidence of computer programs used by the suspect or websites visited. Volatile data may provide information relating to current processes on an active computer which may be useful in an investigation, such as information relating to users, passwords, unencrypted data or instant messages. Examples of storage devices for non-volatile data include internal/external hard disks, portable disk drives, flash storage devices and zip disks.

212. The United States Department of Homeland Security has developed a valuable overview of this process in a guide entitled "Best practices for seizing electronic evidence: a pocket guide for first responders".[123] This guide outlines the following steps to preserve evidence in connection with criminal investigations involving computing devices:

[123] United States, Department of Homeland Security, "Best practices for seizing electronic evidence: a pocket guide for first responders", 3rd ed. (2007). Available from www.forwardedge2.com/pdf/bestPractices.pdf.

Best practices for data preservation

- Do not use the computer or attempt to search for evidence
- If the computer is connected to a network, unplug the power source to the router or modem
- Prior to moving any evidence, photograph the computer as found, including the front and back, as well as any cords or connected devices and the surrounding area
- If the computer is "off", do not turn it "on"
- If the computer is "on" and something is displayed on the monitor, photograph the screen
- If the computer is "on" and the screen is blank, move the mouse or press the space bar (this will display the active image on the screen); after the image appears, photograph the screen
- For desktop computers, unplug the power cord from back of the computer tower
- For laptop computers, unplug the power cord; if the laptop does not shut down, locate and remove the battery pack (the battery is commonly placed on the bottom, and there is usually a button or switch that allows for its removal); once the battery is removed, do not return it to or store it in the laptop (this will prevent the accidental start-up of the laptop)
- Diagram and label cords to later identify connected devices
- Disconnect all cords and devices from the tower or laptop
- Package and transport components (including the router and modem, if present) as fragile cargo
- Where permitted pursuant to the terms of any applicable search warrant, seize any additional storage media
- Keep all media, including the tower, away from magnets, radio transmitters and other potentially damaging elements
- Collect instruction manuals, documentation and notes, paying particular attention to any items that may identify computer-related passwords or passphrases
- Document all steps involved in the seizure of a computer and its components.

213. With regard to mobile devices such as smart phones and personal digital assistants, similar principles apply, except that it is recommended not to power down the device, as this may enable any password protection, thus preventing access to evidence. The device should therefore be kept charged, to the extent possible, or undergo specialist analysis as soon as possible before the battery is discharged to avoid data loss.

214. The case below from India illustrates the importance of forensic analysis in the identification and recovery of digital and other evidence of terrorist use of the Internet.

The Zia Ul Haq case

The defendant, Zia Ul Haq, who was arrested on 3 May 2010 and is currently awaiting trial, is allegedly a member of Lashker e Taiba, which is a Pakistan-based armed group fighting against Indian control in Kashmir. The prosecution case against Zia Ul Haq alleges, inter alia, that he was lured into jihad while working in Saudi Arabia between 1999 and 2001; received training outside India in the use of arms, ammunition and explosives and communicating through e-mails; collected a consignment of arms, ammunition and explosives in Delhi in 2005, after being requested to do so via e-mail; and subsequently used the Internet to coordinate with other members of Lashker e Taiba and conspired to commit terrorist acts using arms, ammunition and explosives.

The prosecution further alleges that, on 7 May 2006, Zia Ul Haq used hand grenades supplied in the weapons consignment from Lashker e Taiba in an attack against the Odeon cinema in Hyderabad.

E-mail communications between the defendant and his handler were obtained from the Internet-service providers and their content was examined. The cybercafe computers that were used by the offender were forensically analysed, the hotel where he stayed while he was in Delhi to collect the grenades was traced and his signature in the guests' register forensically matched. While the defendant was in jail awaiting trial, a letter rogatory was sent from India to the central authority in another country to initiate action against the alleged handler.

Zia Ul Haq was charged in India for various offences, including under sections 15, 16, 17 and 18 of the Unlawful Activities (Prevention) Act of 1967, as amended in 2004 and 2008, which provides for punishment for terrorist activities, training and recruitment for terrorist purposes, raising funds for terrorist activities and conspiracy to commit terrorist activities.

215. Owing to the fragile nature of digital evidence, its assessment, acquisition and examination is most effectively performed by specially trained forensic experts. In Israel, domestic legislation acknowledges the importance of specialist training, requiring that digital evidence be secured by trained computer investigators, who undergo a basic professional course and advanced professional in-service training to become acquainted with computer systems, diverse forensic software and the optimal way to use them. When the need for an especially complex investigation arises, such as recovery of deleted, defective or complexly coded or encrypted files, an external expert, who may later be called as an expert witness on behalf of the prosecution, may be retained.[124]

216. It is advisable to perform any examinations on a copy of the original evidence, in order to preserve the integrity of the original source data.[125] A duplicate copy of digital data may be created with the use of specific forensic tools, such as Guidance Software's EnCase or Forensic Tool Kit¸ or freeware alternatives. To the extent possible,

[124]Written submission of expert from Israel.

[125]United States, Department of Justice, Office of Justice Programs, National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (2004), p. 1. Available from www.ncjrs.gov/pdffiles1/nij/199408.pdf.

at least two different forensic tools should be used to create duplicate copies, in the event that one does not adequately collect all data.[126]

217. EnCase makes a duplicate image of the data on the device under examination, analysing all sectors of the hard disk, including unallocated sectors, to ensure the capture of any hidden or deleted files. The software may also be used, inter alia, to analyse the structure of the file system of digital media, organize the files under analysis and generate a graphic representation or other report relating to certain characteristics of the files. EnCase also generates and assigns a unique identifier, known as a "hash value", to the digital evidence.[127]

218. In order to support the authenticity of digital evidence in connection with legal proceedings (see section IV.D below), a hash value assigned to digital files, or portions thereof, is based on a mathematical algorithm applied to characteristics of the dataset. Any alteration of the dataset would result in the generation of a different hash value. Hash values are generated with respect to *(a)* the original hard drive prior to the creation of a duplicate image, *(b)* the duplicated copy or copies prior to forensic examination and *(c)* the duplicated copy or copies after examination. Matching hash values support a finding that digital evidence has not been tampered with and that the copy that has undergone forensic examination may be treated as the original source data for the purposes of the legal proceedings. Commonly used algorithms include MD5 and SHA.[128]

D. Supporting the authentication of digital evidence

219. An effective prosecution of suspected use of the Internet for terrorist purposes must be supported by evidence that has been properly collected and well documented (see section VI.G.2). This is necessary to establish the integrity of the digital evidence, for the purposes of both its admissibility in court and its persuasive value. The integrity of digital evidence may be established by a combination of traditional and specialized investigative techniques. Key issues include the chain of custody of both the physical device used to store or transmit electronic data and the actual data, as well as the procedures followed to secure such data and any deviations from established procedures. With regard to traditional investigative methods, law enforcement officers may make enquiries to establish, to the extent possible, who may have handled or had access to the evidence prior to it being taken into custody and when, how and from where the evidence was collected.

220. A prosecutor may also be required to show, inter alia, that the information obtained is a true and accurate representation of the data originally contained on the

[126] EC-Council Press, *Computer Forensics: Investigating Data and Image Files* (Clifton Park, New York, Course Technology Cengage Learning, 2010), p. 2-4.

[127] Written submission of expert from the Raggruppamento Operativo Speciale of the Carabinieri of Italy.

[128] Barbara J. Rothstein, Ronald J. Hedges and Elizabeth C. Wiggins, "Managing discovery of electronic information: a pocket guide for judges" (Federal Judicial Center, 2007). Available from www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf.

media and that it may be attributed to the accused. Hash values generated with respect to digital evidence provide strong support that such evidence remains uncompromised. Additional corroborating evidence and testimony may also be introduced to establish authenticity. An illustration of this practice can be found in the case of Adam Busby, who was convicted in Ireland in 2010 of sending a bomb threat via e-mail to Heathrow Airport in London. During the Busby trial, in addition to producing evidence that the e-mail was sent from a specific computer to which the accused had access, hard-copy computer logs and closed caption television footage were also introduced to establish the time at which the e-mail was transmitted and the fact that the accused was the person in control of the computer at that time.

E. Operational cybercrime units

1. National or regional cybercrime units

221. Increased dependency on computer technology has led to dramatic increases in the demand for dedicated cybercrime units to respond to requests for forensic retrieval of computer-based evidence, and not just in terrorist cases involving the use of the Internet. Organized crime such as drug trafficking, trafficking in persons and international paedophile groups offers examples of cases in which criminal use of the Internet has been particularly prevalent, but in recent years there has been an increase in the degree to which cases involve computer-based or electronic evidence in some form. The establishment of national cybercrime units with specialized skills relating to the investigation of cybercrime could significantly improve a State's operational capability to support such demands. Depending on geographical and resource requirements, such a national unit may also be supported by smaller regional units to respond to local needs. Additionally, it may be more efficient and cost-effective to have regional units under the command of local regional management.

222. The responsibilities of national or regional cybercrime units may include the following:

(a) Gathering open-source intelligence by using specialist online surveillance techniques from social networking sites, chat rooms, websites and Internet bulletin boards revealing the activities of terrorist groups (among many other criminal elements). Insofar as terrorist groups are concerned, this function could be placed within the remit of counter-terrorism units in which personnel have sufficient training and experience to conduct this task, but specialist training within a cybercrime environment is seen as essential training for this role. The intelligence-gathering function also requires evaluation and analysis to support the development of strategy in countering the threat posed by terrorists' use of the Internet. Conflicting responsibilities or objectives between national intelligence agencies may, however, hinder harmonization and the translation of intelligence leads into effective operational plans;

(b) Conducting specialist cybercrime investigations in national and international technology-related crime cases, such as those involving Internet fraud or theft

of data and other cases in which complex issues of technology, law and procedure arise and the management of the cybercrime unit assesses that the specialist investigation resources of that unit are necessary;

(c) Serving as an industry and international liaison for the development of partnerships with the principal stakeholders in the fight against cybercrime, such as the financial services industry, the telecommunications services industry, the computer industry, relevant government departments, academic institutions and intergovernmental or regional organizations;

(d) Maintaining an assessment unit to assess cybercrime cases nationally and internationally for prioritized investigation by national or regional cybercrime units. Such a unit may also be responsible for the maintenance of statistics on the incidence of cybercrime cases;

(e) Providing training, research and development, as the complex and evolving nature of cybercrime requires scientific support from specialist academic institutions to ensure that national and regional units are properly skilled and resourced with all the technological tools, training and education that is required to forensically examine computer media and investigate cybercrime.

2. Computer forensic triage units

223. Computer forensic triage units may be established to support national and regional cybercrime units. The personnel of such units would be trained to forensically view computer items using specially developed software tools at search sites. A triage team member can conduct an initial examination on site to either eliminate computers or other peripheral computer equipment from the investigation as having no evidential value or may seize the computer-based evidence in accordance with proper forensic techniques and support local investigation teams in the questioning of suspects as regards the computer-based evidence uncovered. When necessary, the items of computer media seized by triage units may also be submitted for full forensic examination to the relevant regional cybercrime unit or to the national cybercrime unit, as appropriate.

224. Researchers from University College Dublin are currently working on the development of a range of forensic software tools to support preliminary analysis, which will be available to law enforcement officials at no cost. The development of these tools is part of a broader strategic solution being explored by the University College Dublin Centre for Cybersecurity and Cybercrime Investigation and the Computer Crime Investigation Unit of An Garda Síochána (Ireland's national police service), aimed at assisting underresourced cybercrime units, with limited budgets and personnel, in the management of their caseloads. The objective of this initiative will be to create an entirely "open source" forensics lab. Participating investigators will receive instruction on building computer evidence storage and processing equipment, and will be trained on the use of free forensic tools.

F. Intelligence-gathering

225. Intelligence-gathering is a key component of counter-terrorism activities, as information obtained through such channels often triggers the investigations that lead to the prosecution of suspects, or is used as evidence at trial, to the extent permitted by domestic law and rules of procedure. The different purposes for which intelligence may be gathered, and the different agencies which may acquire or use this information, may require the careful balancing of competing interests, however. For example, the law enforcement or intelligence services involved in acquiring intelligence information may place significant emphasis on the protection of the confidentiality of the source of the information, while officials of the court would need to consider, inter alia, a defendant's right to a fair trial and equal access to the evidence presented against him or her. Due care should be taken to ensure that adequate checks and balances are in place with respect to the fundamental human rights outlined in the applicable international conventions.[129]

226. In some Member States, intelligence from anonymous sources is not admissible as evidence in court; however, intelligence information that is corroborated by authoritative sources or additional evidence may be considered. For example, in Ireland, intelligence gathered on terrorists can amount to prima facie evidence that a particular individual is a member of an unlawful organization when that evidence is given under oath by a police officer with a rank of at least chief superintendent. The Irish Supreme Court upheld the use of such intelligence as evidence, in the presence of corroborating evidence, when the fear of reprisals made direct evidence unavailable and given the senior rank of the officer giving evidence.[130]

227. Several experts have also highlighted the tension between the need to encourage the availability of information regarding potential terrorist activity conducted via the Internet and the need to apprehend and prosecute the perpetrators of such activity. For example, once potentially terrorism-related website activity is identified, national security agencies may consider the long-term and short-term implications of the operational response. Such response may include passively monitoring website activity for intelligence purposes, covertly engaging with other users to elicit further information for counter-terrorism purposes or shutting down the website. The varying objectives and strategies of different domestic and foreign agencies may guide the preferred counter-terrorism actions.[131]

228. The practical considerations when evaluating the intelligence value versus the threat level of an online resource were highlighted in a recent report of the United States Congressional Research Service:

[129] See, for example, the Universal Declaration of Human Rights, art. 10; International Covenant on Civil and Political Rights, art. 14; and European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 6.

[130] *People (DPP) v. Kelly*, [2006] 3 I.R. 115.

[131] Catherine Theohary and John Rollins, Congressional Research Service (United States), "Terrorist use of the Internet: information operations in cyberspace" (8 March 2011), p. 8.

> For example, a "honey pot" jihadist website reportedly was designed by the [Central Intelligence Agency] and Saudi Arabian Government to attract and monitor terrorist activities. The information collected from the site was used by intelligence analysts to track the operational plans of jihadists, leading to arrests before the planned attacks could be executed. However, the website also was reportedly being used to transmit operational plans for jihadists entering Iraq to conduct attacks on U.S. troops. Debates between representatives of the [National Security Agency, Central Intelligence Agency, Department of Defense, Office of the Director of National Intelligence and National Security Council] led to a determination that the threat to troops in theater was greater than the intelligence value gained from monitoring the website, and a computer network team from the [Joint Task Force-Global Network Operations] ultimately dismantled it.[132]

As illustrated in the above case, coordination between agencies is an important factor in successfully responding to identified threats.

229. Other Member States, such as the United Kingdom, have indicated that significant emphasis has been placed on developing working relationships and entering into memorandums of understanding between the prosecution and law enforcement or intelligence agencies, with positive results. Similarly, in Colombia, the Integrated Centre of Intelligence and Investigation (Centro Integrado de Inteligencia e Investigación, or CI3) is the domestic agency that coordinates investigations into suspected terrorist activities using a strategy based on six pillars. This approach involves a high-ranking official from the national police assuming overall command and control of different phases of the investigation, which include the gathering, verification and analysis of evidence and a judicial phase in which police collect information on parties and places associated with the commission of any crimes.[133]

230. The expert from France outlined the domestic approach to coordinating interagency responses to identified terrorist activity:

- Phase 1: Surveillance and intelligence services identify a threat by monitoring Internet activity
- Phase 2: The surveillance services notify the public prosecution services of the threat identified. The judge or prosecutor can then authorize law enforcement authorities to place the Internet activity of an identified suspect under surveillance. As of 2011, legislation permits the leading judge to authorize law enforcement to record the monitored person's computer data. Moreover, personal data (e.g. name, phone number, credit card number) can be requested from the relevant service providers
- Phase 3: The investigation is conducted based on the evidence gathered from the sources outlined under phases 1 and 2.

[132] Ibid, p. 13.

[133] United Nations Office on Drugs and Crime, *Digest of Terrorist Cases*, para. 191.

G. Training

231. Law enforcement officials involved in investigations of the use of the Internet for terrorist purposes require specialist training in the technical aspects of how terrorists and other criminals can use the Internet in furtherance of illicit purposes and how law enforcement can effectively use the Internet as a resource to monitor the activities of terrorist groups. Training may be provided through public or private sector initiatives, or a combination of both.

232. Courses on information technology forensics and cybercrime investigations may be provided at the regional or international level by organizations such as Europol and INTERPOL. In addition, a number of countries have developed their own law enforcement cybercrime training programmes, either alone or in conjunction with academic institutes. Training may also be provided through ad hoc training courses, seminars, conferences and hands-on training provided through the public sector or relevant industry stakeholders.

233. Specialized training may also be available through academic institutions, such as University College Dublin in Ireland, which in 2006 established the Centre for Cybersecurity and Cybercrime Investigation. Programmes offered by the university include the law-enforcement-only master's degree in forensic computing and cybercrime investigation. Further courses also provide first responders with training to support their operational role in connection with cybercrime cases.

234. The Cybercrime Centres of Excellence Network for Training, Research and Education (2CENTRE) is a project funded by the European Commission and launched in 2010, with the aim of creating a network of Cybercrime Centres of Excellence for Training, Research and Education in Europe. Centres are currently being developed in Belgium, Estonia, France and Ireland. Each national centre is founded on a partnership among representatives of law enforcement, industry and academia, collaborating to develop relevant training programmes and qualifications, as well as tools for use in the fight against cybercrime. The University College Dublin Centre for Cybersecurity and Cybercrime Investigation is the leader and coordinator of the project.[134]

235. Online counter-terrorism training is also available through the Counter-Terrorism Learning Platform of UNODC, which was launched in 2011.[135] The platform is an interactive tool specifically designed to train criminal justice practitioners in the fight against terrorism, while incorporating them into a single virtual community where they can share their experiences and perspectives to fight terrorism. In addition to allowing practitioners who have previously participated in training provided by UNODC to connect and create networks with their counterparts, the platform allows them to be kept abreast of legal developments in the field, to be informed about upcoming training opportunities and to engage in continuous learning activities.

[134] See www.2centre.eu.

[135] See www.unodc.org/unodc/en/terrorism/unodc-counter-terrorism-learning-platform.html.

V. International cooperation

A. Introduction

236. The speed, global reach and relative anonymity with which terrorists can use the Internet to promote their causes or facilitate terrorist acts, together with complexities related to the location, retention, seizure and production of Internet-related data, makes timely and effective international cooperation between law enforcement and intelligence agencies an increasingly critical factor in the successful investigation and prosecution of many terrorism cases.

B. Instruments and arrangements relating to international cooperation

1. The universal instruments against terrorism

237. The universal instruments against terrorism, comprised of international conventions and protocols and relevant resolutions of the Security Council, contain comprehensive mechanisms for international cooperation in criminal proceedings related to terrorism. These instruments make provision for extradition, mutual legal assistance, transfer of criminal proceedings and convicted persons, reciprocal enforcement of judgements, freezing and seizure of assets and exchange of information between law enforcement agencies.

238. Key elements of the instruments against terrorism relating to international cooperation include:

- The obligation to bring perpetrators of acts of terrorism to justice
- The obligation to extradite or prosecute (the *aut dedere aut judicare* principle)
- The obligation to establish legal jurisdiction in defined circumstances
- The obligation to exclude the political offence exception as a ground for refusing a request for cooperation
- Respect for the rule of law and human rights
- Respect for the principle of dual criminality
- Respect for the rule of speciality
- Respect for the *ne bis in idem* rule: precluding a second prosecution for the same offence.[136]

[136] United Nations Office on Drugs and Crime, *Manual on International Cooperation in Criminal Matters related to Terrorism* (2009), sect. 1.C.

239. The general principles applicable to extradition and mutual legal assistance in cases involving terrorism or transnational organized crime are part of comprehensive mechanisms set out in the universal counter-terrorism instruments and other instruments dealing with transnational organized crime (e.g. the United Nations Convention against Transnational Organized Crime).[137] It is not the intention of the present publication to provide a detailed restatement or analysis of how these principles should be implemented by States at the national level. Rather; its focus is on identifying, within the broad international cooperation framework established through these instruments, and with reference to established principles and mechanisms, issues specific to terrorism cases involving the use of the Internet, in order to provide guidance to policymakers and practitioners on approaches or strategies that reflect current good practice

(a) Absence of a universal instrument relating to cyberissues

240. While the international cooperation mechanisms in the universal instruments against terrorism, when fully implemented, are likely to provide a legal basis for cooperation in many cases involving Internet-related acts by persons involved in the commission of unlawful conduct specified in the instruments, none of them deals specifically with Internet-related acts per se. In the absence of a counter-terrorism instrument dealing specifically with Internet issues connected to terrorism, authorities, when investigating and prosecuting such cases, will continue to be reliant upon existing international or regional treaties or arrangements, established to facilitate international cooperation in the investigation and prosecution of terrorism or transnational organized crime offences generally.

241. It is clear that international cooperation in the investigation and prosecution of terrorism cases involving use of the Internet by terrorists is hindered, to some extent, by the absence of a universal instrument dealing specifically with cyberissues. It is not the aim of the present document, however, to assess the relative merits of arguments in favour or against the utility of the development of a comprehensive universal instrument dealing with, inter alia, international cooperation in criminal cases (including terrorism) involving cyberrelated issues. Rather, its focus is on identifying areas under the current international framework that operate as obstacles to such cooperation and how existing available instruments and arrangements might be used by national authorities to facilitate or strengthen international cooperation in terrorism cases involving some aspect of Internet use.

(b) Other instruments: the United Nations Convention against Transnational Organized Crime and the Council of Europe Convention on Cybercrime

242. The United Nations Convention against Transnational Organized Crime is the primary international instrument dealing with the international cooperation between States on serious transnational organized crime. Articles 16 (extradition), 18 (mutual legal assistance), 19 (joint investigations) and 27 (law enforcement cooperation) of the

[137] United Nations, *Treaty Series*, vol. 2225, No. 39574.

Organized Crime Convention deal with international cooperation. Although the unlawful conduct referred to in the Organized Crime Convention deals with transnational organized crime, not terrorism, the underlying principles and mechanisms in that Convention related to international cooperation are very similar to those set out in the universal counter-terrorism instruments. As such, those States parties which have implemented their international cooperation obligations under these instruments should have broadly compatible frameworks and mechanisms.

243. In addition to the Council of Europe Convention on Cybercrime, the Council of Europe Convention on the Prevention of Terrorism; the European Convention on Extradition,[138] with its three Additional Protocols;[139] the European Convention on Mutual Assistance in Criminal Matters,[140] with its two Additional Protocols;[141] and the Council of the European Union Act 2000/C 197/01 [of 29 May 2000] establishing, in accordance with article 34 of the Treaty on European Union, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union might afford a legal basis for international cooperation in terrorism cases involving some element of Internet use.

244. The Council of Europe Convention on Cybercrime contains provisions aimed at encouraging international cooperation via police and judicial cooperation mechanisms and provisional measures in urgent cases, for example, the informal provision of spontaneous information upon request (art. 26) and the establishment of 24/7 points of contact (art. 35). Such requests can be accompanied by a request for non-disclosure and provide a legal mechanism enabling the use of informal means of communication and information-sharing among the parties of the Convention, even if they do not have such a provision in their national legislation.

245. It is noted that the Council of Europe Convention on Cybercrime is open not only to members of the Council of Europe or non-member States that have participated in its elaboration, but may also be acceded to by other non-member States, in the latter case subject to unanimous agreement of the contracting States entitled to sit on the Committee of Ministers.

2. Other regional or multilateral arrangements

246. In addition to the international and regional instruments mentioned above, States may choose to enter into bilateral or multilateral treaties or arrangements that make specific provision for cooperation on cyberrelated activity connected to terrorism or transnational crime. Extradition and mutual legal assistance tend to be regulated either by treaties or through "soft law" agreed upon by blocs of countries. Nevertheless, regional and subregional organizations also play an important role in facilitating the

[138] Council of Europe, *European Treaty Series*, No. 24.

[139] Ibid., Nos. 86, 98 and 209.

[140] Ibid., No. 30.

[141] Ibid., Nos. 99 and 182.

exchange of information and the provision of cooperation under such mutually agreed arrangements.

(a) European arrest warrant: Schengen framework

247. The European arrest warrant under the Schengen framework is a cooperation tool applicable throughout all member States of the European Union; it has proven extremely useful in strengthening legal cooperation in the investigation and prosecution of criminal cases, including those related to terrorism in Europe. Once issued, it requires, on the basis of reciprocity, that the authorities of another member State arrest and transfer a criminal suspect or sentenced person to the issuing State so that the person can be put on trial or complete a detention period. In this context, it is noted that the European arrest warrant provides, inter alia, for the extradition of a member State's own nationals, a concept formerly alien to the legal (often constitutional) provisions of many States adhering to the so-called European continental system.

(b) European evidence warrant

248. Since it came into force in 2009, the European evidence warrant has, in a similar way to the European arrest warrant with respect to arrests, provided a streamlined procedure for procuring and transferring evidence, including objects, documents and data, between member States for use in criminal proceedings. For the purposes of the European evidence warrant, evidence gathered may include Internet-related customer data.[142]

249. Using these framework decisions and other international instruments, European States have, as a bloc, established a highly developed, broadly collective approach to the cross-border collection and transmission of evidence and extradition/surrender of offenders for the purposes of criminal proceedings. Other Governments might consider, at a political and operational level, the desirability of adopting and adapting a collective approach at the regional or subregional level to harmonizing their efforts to cooperate in the cross-border investigation and prosecution of terrorism-related offences.

(c) Commonwealth Schemes relating to extradition and mutual legal assistance

250. In a similar manner to the European arrest warrant under the Schengen framework, the Commonwealth Scheme for the Transfer of Convicted Offenders (London Scheme) provides a simplified mechanism for extradition between Commonwealth countries, providing for the provisional arrest of offenders on the basis of arrest warrants issued by other member countries, without the need for an assessment of the evidential sufficiency of the case against the suspect. The scheme defines offences as extraditable if they constitute offences in both countries and carry imprisonment for two years or more.

[142]Voislav Stojanovski, "The European evidence warrant", in *Dny práva—2009—Days of Law: the Conference Proceedings*, 1st. ed., David Sehnálek and others, eds. (Brno, Czech Republic, Masaryk University, 2009).

251. Likewise, the Commonwealth Scheme for Mutual Assistance in Criminal Matters (Harare Scheme) is aimed at increasing the level and scope of assistance rendered between Commonwealth countries in criminal matters by facilitating the identification and location of persons; the service of documents; the examination of witnesses; search and seizure of evidence; the appearance of witnesses; the temporary transfer of persons in custody for purpose of testimony; the production of judicial or official records; the tracing, seizure and confiscation of the proceeds or instrumentalities of crime; and the preservation of computer data.

252. While the Commonwealth Schemes are not treaties as such, they are examples of non-binding arrangements, or "soft law", under which certain countries have agreed to incorporate compatible legislation into their domestic laws, consistent with agreed principles, to simplify extradition and mutual legal assistance among themselves in criminal cases, including terrorism-related investigations and prosecutions

(d) Council of Europe

253. In addition to the elaboration of instruments aimed at promoting international cooperation in cyberrelated criminal cases, including terrorism, the Council of Europe has also established (under article 35 of the Council of Europe Convention on Cybercrime) the Council of Europe 24/7 Network of contact points available 24 hours a day, seven days a week, which is aimed at facilitating international cooperation in cybercrime cases. The Council of Europe and European Union regional projects CyberCrime@IPA and Cybercrime@EAP, among others, support the participation of 24/7 contact points in training events, which provides an opportunity for them to link up with each other as well as network with members of the Group of Eight (G-8) network.

254. Since 2006, the Council of Europe has, through its Global Project on Cybercrime, been supporting countries worldwide in the strengthening of legislation; the training of judges, prosecutors and law enforcement investigators in matters related to cybercrime and electronic evidence; and in law enforcement/service provider cooperation and international cooperation.[143] Since 2010, one focus area has been criminal money flows and financial investigations on the Internet, including Internet-based terrorist financing.[144]

(e) European Union action plan: cybercrime centre

255. On 26 April 2010, recognizing the integral role that information and communications technology plays in modern society and the increasing number, scope, sophistication and potential impact of threats for multiple jurisdictions reinforcing the need for strengthened cooperation between Member States and the private sector, the Council of the European Union adopted conclusions concerning a cybercrime action plan, to be included in the Stockholm Programme for 2010-2014 and the associated future Internal Security Strategy.

[143] See www.coe.int/lportal/web/coe-portal/what-we-do/rule-of-law/terrorism.

[144] Council of Europe, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, *Criminal Money Flows on the Internet: Methods, Trends and Multi-Stakeholder Counteraction* (2012).

256. Under the plan, members agreed, inter alia, to mandate the European Commission, in cooperation with Europol, to analyse and report back on the utility and feasibility of establishing a European cybercrime centre to strengthen knowledge, capacity and cooperation on cybercrime issues. This work has been completed and a proposal developed under which Europol would host a new facility for receiving and processing analytical work files related to serious organized crime and terrorism.

3. Role of other regional organizations and cooperation agreements

257. As stated earlier, formal cooperation agreements, at the regional or subregional level, between law enforcement or intelligence agencies play an integral role in efforts by the international community to strengthen and coordinate measures targeting terrorism and transnational organized crime. While cooperation under these arrangements is usually not based on legally binding treaties or other instruments, it can nevertheless provide highly effective mechanisms for cooperation between participating member countries.

258. Internationally, there are many examples of such arrangements, but three, operating in Europe, Africa and the Pacific, illustrate how groups of countries with compatible law enforcement and security interests and objectives can successfully work together to develop and harmonize close cooperation on criminal investigations.

259. The French-German Centre for Police and Customs Cooperation, also known as the Offenburg Centre, was established in 1998 to, inter alia, support the coordination of multi-agency operations (e.g. search and surveillance operations and exchanging information collected) across those countries' common border. It is staffed by police and customs and border agencies from both federal and state level and handles many thousands of requests each year, serving as a platform for mediating pragmatic solutions to issues between partner agencies and developing inter-agency trust and cooperation.

260. In Africa, members of the Southern African Regional Police Chiefs Cooperation Organization and the Eastern African Police Chiefs Cooperation Organization have agreed to specific areas in which police agencies will cooperate, including in the regular exchange of crime-related information; the planning, coordination and execution of joint operations, including undercover operations; border control and crime prevention in border areas, as well as follow-up operations; the controlled delivery of illegal substances or any other objects; and technical assistance and expertise, where required.[145]

261. In the Pacific region, the Pacific Transnational Crime Coordination Centre provides a hub for the collection, coordination, analysis and sharing of criminal intelligence data collected via a network of national transnational crime units located in member countries across the region. The Centre, which is operated by officers seconded from

[145] Charles Goredema, "Inter-State cooperation", in *African Commitments to Combating Organised Crime and Terrorism: A review of eight NEPAD countries* (African Human Security Initiative, 2004). Available from www.iss.co.za/pubs/Other/ahsi/Goredema_Botha/pt1chap5.pdf.

different law enforcement and border agencies in Pacific island countries, provides member countries with an access point to INTERPOL and other law enforcement agencies around the world, via the international network of the Australian Federal Police, which supports the initiative.

262. Similarly, countries that are not necessarily close geographically, but that have common interests in thematic areas related to law enforcement and security, might enter into collective arrangements that provide for information exchange and intelligence sharing.

(a) Egmont Group of Financial Intelligence Units

263. An example of such an arrangement with implications for investigations related to terrorist financing is the Egmont Group of Financial Intelligence Units. Investigations into suspected terrorist financing will invariably involve the collection, sharing and analysis of financial or banking records located in one or more jurisdictions. In these cases, the ability of financial intelligence units to cooperate and share financial intelligence is likely to be critical to a successful investigation and prosecution. The Egmont Group, an international body established in 1995, works to promote and improve cooperation between financial intelligence units in efforts to counter money-laundering and the financing of terrorism and to foster, among other things, the expansion and systematization of international cooperation in the reciprocal exchange of information. The Egmont Group recommends that its members enter into memorandums of understanding in which they agree to exchange financial intelligence relevant to the investigation and prosecution of terrorist financing, money-laundering and related criminal activity.

264. In order to ensure that their national financial intelligence units are able to cooperate effectively with foreign counterparts in such cases, authorities should consider the desirability of entering into appropriate information-sharing agreements or arrangements with foreign counterparts. The model memorandum of understanding suggested by the Egmont Group provides useful guidance on the types of issues that might need to be addressed.

(b) International Criminal Police Organization

265. Many international instruments, including the International Convention for the Suppression of the Financing of Terrorism[146] (art. 18, para. 4) and the United Nations Convention against Transnational Organized Crime (art. 18, para. 13) and various Security Council resolutions, including resolution 1617 (2005), specifically encourage countries to work within the INTERPOL framework for cooperation on the exchange of information.

266. One of the core functions of INTERPOL is to promote international cooperation between international law enforcement agencies and the fast and secure exchange and

[146] United Nations, *Treaty Series*, vol. 2178, No. 38349.

analysis of information related to criminal activities. It does this via its I-24/7 system, which is available to law enforcement officials in all member countries.

267. Using the I-24/7 system, national central bureaus can search and cross-check a wide range of data, including information on suspected terrorists and a variety of databases. The aim of the system is to facilitate more effective criminal investigations by providing a broader range of information for investigators.

268. In addition to the I-24/7 network, the cybercrime program of INTERPOL is aimed at promoting the exchange of information among member countries through regional working parties and conferences, delivering training courses to build and maintain professional standards, coordinating and assisting international operations, establishing a global list of contact officers for cybercrime investigations, assisting member countries in the event of cyberattacks or cybercrime investigations through investigative and database services, developing strategic partnerships with other international organizations and private sector bodies, identifying emerging threats and sharing this intelligence with member countries and providing a secure web portal for accessing operational information and documents.[147]

269. Since 2009, INTERPOL has worked closely with University College Dublin to provide specialist training and academic exchanges to promote law enforcement e-crime investigation expertise. In August 2011, cybercrime investigators and computer forensic specialists from 21 countries took part in the first INTERPOL/University College Dublin cybercrime summer school training course. The two-week programme, which was developed by the University, included case-simulation exercises and was delivered by professionals from law enforcement, University College Dublin and the private sector. The event was aimed at developing theoretical and practical knowledge and skills across a range of areas to assist investigators in conducting more effective cybercrime investigations and provided participants with skills in such areas as disk imaging, live data forensics, mobile phone forensics, money-laundering investigations, search and seizure techniques, VoIP and wireless investigations and malware detection and analysis.[148]

270. Finally, the High-Tech Crime Unit of INTERPOL facilitates operational cooperation among member countries through global and regional cybercrime expert group meetings and training workshops, as well as cooperation among law enforcement, industry and academia. It also assists member countries in the event of cyberattack and in cybercrime investigations, through investigative and database services.

(c) European Police Office

271. A major part of the mandate of Europol is to improve the effectiveness of and cooperation among law enforcement authorities of European Union member States in preventing and combating terrorism and other forms of transnational organized crime.

[147] See www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

[148] Ibid.

Europol plays a key role in the European Cybercrime Task Force, an expert group made up of representatives from Europol, Eurojust and the European Commission, working together with the heads of European Union cybercrime units to facilitate the cross-border fight against cybercrime. Europol offers the following support to European Union member States on cybercrime related issues:

- Cybercrime database: Europol provides European Union member States with investigative and analytical support on cybercrime and facilitates cross-border cooperation and information exchange
- The Threat Assessment on Internet Facilitated Organised Crime (iOCTA) assesses current and future trends in cybercrime, including terrorist activities, and attacks on electronic networks, which informs both operational activity and European Union policy
- The Internet Crime Reporting Online System (ICROS) and the Internet and Forensic Expert Forum (IFOREX) are currently in development. These will provide centralized coordination of reports of cybercrime from the authorities of European Union member States, and will host technical data and training for law enforcement.[149]

272. In addition to this support, at an operational level and in conjunction with Eurojust, Europol is heavily involved in the establishment and support of joint investigation teams and provides support to member States with respect to investigations through analytical work files and case-based coordination and tactical meetings. Under the analytical work file platform for analysis, nominative data (e.g. information on witnesses, victims, telephone numbers, locations, vehicles and events) is stored and subjected to a dynamic analytical process linking objects, entities and data between national inquiries and investigations. The data is tagged with a "handling code" that clearly indicates the conditions of use attached to that particular data component.

(d) Eurojust

273. As part of its mandate, the work of Eurojust in the counter terrorism field includes the facilitation of the exchange of information between the judicial authorities of the different member States involved in terrorism-related investigations and prosecutions;[150] supporting the judicial authorities of member States in the issuance and execution of European arrest warrants; and facilitating investigative and evidence-gathering measures necessary for member States to prosecute suspected terrorism offences (e.g. witness testimony, scientific evidence, searches and seizures, and the interception of communications). The 27 Eurojust national members (judges, prosecutors or police authorities with equivalent competences in their respective member States)

[149] See "Cybercrime presents a major challenge for law enforcement", European Police Office press release, 3 January 2011. Available from www.europol.europa.eu/content/press/cybercrime-presents-major-challenge-law-enforcement-523.

[150] Council of the European Union decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences obliges all member States to designate national correspondents for terrorism matters, who must inform Eurojust (the judicial cooperation unit of the European Union) of all terrorist activities in their country, from the first stages of interviewing suspects to the indictment stage and from European arrest warrants issued with regard to terrorism to mutual legal assistance requests and judgements.

are based in The Hague, the Netherlands, and are in permanent contact with the national authorities of their respective member States, which may request the support of Eurojust in the course of particular investigations or prosecutions against terrorism (e.g. in resolving conflicts of jurisdiction or facilitating the gathering of evidence).

274. Eurojust also encourages and supports the establishment and work of joint investigation teams by providing information and advice to practitioners. Joint investigation teams are increasingly recognized as an effective instrument in the judicial response to cross-border crime and an adequate forum in which to exchange operational information on particular terrorism cases. Eurojust national members can participate in joint investigation teams, acting either on behalf of Eurojust or in their capacity as national competent authorities for terrorism. For example, in a Danish case related to terrorist activities, in which a request for the establishment of a joint investigation team was forwarded to Belgian authorities, the Danish and Belgium desks at Eurojust were involved in setting up the team between the two competent national authorities. Eurojust also provides financial and logistical assistance to the operations of such teams and hosts the permanent secretariat for joint investigation teams.

275. The *Terrorism Convictions Monitor* of Eurojust is also intended to provide practitioners with examples of judgements in one country which might be useful in another, in particular with respect to interpreting European Union legislation on terrorism. In its September 2010 edition, the *Terrorism Convictions Monitor* provided in-depth analysis of two cases featuring common attributes, such as jihadist-related terrorism, radicalization and use of the Internet.[151] One of the cases, provided by Belgian authorities, was *Malika el Aroud and Others*, referred to below (see para. 377). The Counter-Terrorism Team of Eurojust regularly organizes tactical and strategic meetings on terrorism trends, in which leading magistrates and experts on terrorism law from European Union and non-European Union countries share their expertise on concrete matters. Examples of such meetings include the 2010 strategic meeting relating to the use of VoIP technology for terrorist purposes and the need for lawful interception, and a tactical meeting held in April 2011 on violent single issue extremism/terrorism. At these meetings, common issues are identified, and best practices and resulting knowledge are disseminated to European Union decision makers, identifying possible ways to make counter-terrorism coordination more effective.

C. National legislative frameworks

276. The existence, at the national level, of a legislative framework providing for international cooperation is a fundamental element of an effective framework for the facilitation of international cooperation in the investigation and prosecution of terrorism cases. Such legislation should incorporate into a country's domestic law the principles related to international cooperation espoused in the universal instruments against terrorism.

[151] The *Terrorism Convictions Monitor* is available upon request from the Eurojust Counter-Terrorism Team.

277. In addition to producing a number of publications aimed at assisting countries with the legislative incorporation of international cooperation mechanisms, the Terrorism Prevention Branch of UNODC includes advisory support, training and capacity-building on these issues as part of its menu of services available to countries on the implementation of their international counter-terrorism obligations.

D. Non-legislative measures

278. While accession to multilateral and bilateral instruments and adopting related legislation are fundamental components of any effective regime for international cooperation, they are not the entire answer. A key element in the successful provision of effective international cooperation is the presence of a properly resourced and proactive central authority which can, based on any available mechanisms (both formal and informal), facilitate cooperation in a timely and efficient manner.

279. An important precondition for successful international cooperation is the presence of effective inter-agency coordination between law enforcement, specialist intelligence agencies (e.g. financial intelligence units) and central authorities at the national level, supported by necessary legislation and clear, streamlined procedures for handling requests.

280. A good example of cooperation, at both the national and international level, is illustrated in the following case, prosecuted in Colombia, with extensive formal and informal cooperation between authorities.

Case involving the Revolutionary Armed Forces of Colombia (FARC)

On 1 March 2008, the Colombian armed forces carried out various operations against alleged members of the Revolutionary Armed Forces of Colombia (FARC). During these operations, an individual suspected of being one of the top leaders of FARC and several other members of the organization were killed, and evidence was retrieved, which included electronic devices such as computers, digital diaries and USB sticks. The objects containing digital evidence were passed to the Colombian judicial police for use in possible criminal investigations and prosecutions.

The data retrieved from the digital devices revealed information related to the organization's international network of support, including links to several countries in Central and South America and in Europe. The network's primary objective was fundraising for FARC activities, the recruitment of new members and the promotion of the organization's policies, including the removal of the organization's designation on various terrorism lists maintained by the European Union and some countries. Based on the evidence retrieved, the Public Prosecutor of Colombia initiated criminal investigations against the persons allegedly supporting and financing FARC.

The evidence, which was shared by Colombian authorities with counterparts in Spain, led to the identification of the leader of FARC in Spain, known by the alias "Leonardo". "Leonardo" entered Spain in 2000, and was granted political asylum.

The Public Prosecutor of Colombia obtained sufficient evidence to order the issuance of an arrest warrant for the purposes of extradition against "Leonardo" and used diplomatic and other legal international cooperation channels to request his extradition to Colombia for trial.

"Leonardo" was arrested in Spain, and searches of his residence and workplace revealed documents and electronic devices that contained evidence of his links to the crimes under investigation. He was subsequently released on bail; his refugee status prevented his immediate extradition.

Criminal proceedings were initiated in Colombia against "Leonardo" in absentia for his alleged involvement in the financing of terrorism. In a decision by the Supreme Court of Justice of Colombia, the information obtained during the 1 March 2008 operation and located on the seized electronic devices was deemed inadmissible. The Prosecutor subsequently, in conjunction with counterparts in several other countries where members of the FARC network of support were present, used all available channels of international cooperation to identify members of the network in Spain and other European countries and collect further evidence in support of the case.

Additionally, in responding to the letters rogatory issued by the Public Prosecutor of Colombia, the Spanish judicial authorities transmitted to their Colombian counterparts all the information collected during the raids and searches of "Leonardo's" house. According to the Spanish judicial police, this information established the culpability of "Leonardo" and other persons with respect to forming a FARC terrorist cell in Spain. It also helped establish "Leonardo's" culpability for the financing of terrorism and strengthened the assumption of possible links between "Leonardo" and persons being prosecuted for their links with the terrorist group Euskadi Ta Askatasuna (ETA) (Basque Homeland and Liberty). The searches conducted in Spain resulted in the seizure of further documentary and digital evidence, which was substantively similar to the evidence that had been declared inadmissible. Using this new evidence provided by Spanish authorities, the Colombian Prosecutor continued the proceedings against "Leonardo". Furthermore, the new evidence established efforts by FARC to provide its members with access to universities, non-governmental organizations and other State entities where funding opportunities could be sought and new members recruited.

The evidence also supported the existence of an "international commission" within FARC, which operated a security programme for communications, particularly those transmitted via the Internet or radio waves (permanent means of communications between the leaders of the organization and members of the international network of support), by encrypting the information transmitted, using steganography to conceal messages, sending spam e-mails and deleting browsing histories to ensure that information could not be retrieved by investigative or judicial authorities. In this regard, Spanish and Colombian authorities cooperated to "break" the keys and decipher the content of the messages that were transmitted from the alleged leaders of FARC in Colombia and Spain.

Before initiating the proceedings against "Leonardo", the Public Prosecutor of Colombia submitted a request to a judge that the new evidence be deemed "evidence subsequently received" and from an "independent source". The effect of these requests, which were granted, was to allow the inclusion of the evidence in the legal proceedings without triggering the grounds on which similar evidence would otherwise have been excluded.

The Prosecution of the defendant "Leonardo" in absentia on charges of financing of terrorism is currently ongoing in Colombia, pending the outcome of the extradition proceedings.

281. In the above case, the authorities benefited from both formal mutual legal assistance mechanisms and informal relationships. While there may be differences in the extent to which authorities in different countries can provide mutual assistance in the absence of a treaty or formal request, authorities in many countries do have some ability to provide assistance on the basis of informal requests from foreign counterparts in investigations related to terrorism. The expert group meeting highlighted several cases and circumstances in which such informal cooperation had been or could be used to successfully investigate cases involving the use of the Internet by terrorists.

1. The importance of relationships

282. At an operational level, it is also highly important that national law enforcement and prosecuting agencies promote, establish and maintain relationships of trust and confidence with foreign counterparts with which they might need to cooperate in cross-border criminal investigations.

283. Given the transnational nature of much terrorism and related criminal activity, the highly complex and sensitive nature of intelligence-based investigations and the need for urgency in rapidly-evolving events and investigations, trust between law enforcement and prosecution agencies at both the national and international level is often a critical factor in the successful investigation and prosecution of terrorism-related offences. This is particularly important in the Internet context, where the preservation of, for example, usage data and digital evidence held on computers and other portable devices, often in one or more different jurisdictions, is often critical evidence in a prosecution, and has to occur within tight time frames. Personal contacts with counterparts in other jurisdictions, familiarity with their procedures and trust are all factors that contribute to effective international cooperation.

284. While the means by which informal cooperation can be afforded by specific countries might differ, it is possible to identify some elements of good practice in the provision of informal assistance in terrorism-related investigations.

(a) Developing effective mechanisms for exchange of information: the use of liaison officers

285. Several experts at the expert group meeting noted that their national law enforcement agencies operate a network of international liaison posts which assist greatly with the facilitation of international cooperation requests. For example, the German Federal Criminal Police Office, the *Bundeskriminalamt* has a liaison officer and direct contacts in about 150 countries. Moreover, the European Expert Network on Terrorism Issues, established in 2007, brings together experts from academia, police and intelligence services and has proven to be a very effective channel for members to share information and expertise on a multidisciplinary basis.

286. The case of *R. v. Namouh* is an example of highly successful international cooperation, undertaken entirely on an informal basis, between law enforcement/prosecution authorities in Austria and Canada in the investigation and prosecution of persons located in those jurisdictions and using the Internet to engage in terrorism-related activity.

R. v. Said Namouh

Mr. Said Namouh was a Moroccan national living in a small town in Canada.

On 10 March 2007, a video in the form of an "open" letter read by Sheik Ayman al-Zawahiri was posted on an Internet website. In it, Al-Zawahiri warned the Governments of Austria and Germany to withdraw their troops from peace-support missions in Afghanistan or face consequences. At one point in the statement, Al-Zawahiri stated:

> Peace is a reciprocal matter. If we are safe, you will be safe. If we are at peace, you will be at peace and, if we are going to be killed, God willing, you will be beaten and killed. This is the exact equation. Try, then, to understand it, if you understand.

The video, with the accompanying statements by Al-Zawahiri, was set against a mosaic of images that included armoured cars with national flags and prominent Austrian and German national politicians. In some parts of the video, there were photos of Al-Zawahiri and other hooded figures.

Following the broadcast of the video, Austrian authorities initiated an investigation that included wiretaps on various communications from Mohammed Mahmoud, an Austrian national living in Vienna. These communications consisted of VoIP and Internet chat sessions, conducted in Arabic, which revealed that Mr. Mahmoud was engaged in communication about issues associated with jihad with a person in Canada, including plans for a terrorist attack, most likely in Europe. The participants discussed using explosives and other arrangements related to an attack.

As a result of interception activities, Said Namouh, living in Canada, was identified as one of the participants in the above communications. In July 2007, the Royal Canadian Mounted Police became involved in the investigation, which was coordinated between Austrian and Canadian authorities through Canada's law enforcement liaison officer based in Vienna. While a formal mutual legal assistance treaty existed between Austria and Canada, no formal mutual legal assistance request under the treaty was initiated; the cooperation took place entirely on an informal basis.

Investigations revealed that between November 2006 and September 2007 someone using Mr. Namouh's Internet connection was spending a considerable amount of time on the Internet and was in constant contact with jihadists around the world, including via the Global Islamic Media Front (GIMF), one of the oldest and most prominent virtual jihadist groups. Supported by Al-Fajr Center, GIMF acts as the media arm for the Army of Islam [Jaish al-Islam]. Among other things, GIMF disseminates propaganda and provides jihadists with the tools (e.g. bomb manuals, encryption software) needed to carry out jihad. Much of Mr. Namouh's Internet activity involved postings on various discussion forums frequented by jihadists.

In May 2007, BBC journalist Alan Johnston was kidnapped in Gaza by the "Army of Islam". GIMF published several videos related to this event, but of particular note was the video published on 9 May 2007, in which the Army of Islam claimed responsibility for the kidnapping, as well as videos published on 20 and 25 June, in which threats to execute him were made if certain demands were not met. Fortunately, Mr. Johnston was released unharmed on 3 July 2007.

On 7 and 8 May, communications by Mr. Namouh via an Internet chat forum, intercepted by authorities, revealed that Mr. Namouh was participating in discussions related to the Alan Johnson kidnapping, and specifically in discussions about the preparation of the GIMF message claiming responsibility, which was broadcast a short time later on 9 May. According to a transcript of the Internet chat on 8 May, produced in evidence at trial (and translated from Arabic to French), Mr. Namouh posted: "My beloved brother Abou Obayada, stay with us on the line, may Allah fulfil you with riches so that you may see what needs to be done; the statement will be made today, God willing."

In total, between 3 June and 9 September 2007, 31 conversations took place between Namouh and Mahmoud. These conversations revealed them to be planning to carry out a bombing at an undisclosed location in Europe and discussing how to obtain or make suicide explosive belts, financing issues and travel plans to meet other persons in the Maghreb and Egypt for final preparations. These conversations suggested that Mr. Namouh was the intended suicide bomber.

On 12 September 2007, fearing the plans were getting very close to fruition, authorities in Austria and Canada carried out the simultaneous arrests of Namouh and Mahmoud.

In Canada, Mr. Namouh was charged with conspiracy to use explosives (unknown location in Europe), participation in the activities of a terrorist group, facilitating terrorist activities and extortion of a foreign Government (threat video against Austria and Germany).

At trial, Mr. Namouh's defence challenged several aspects of the prosecution, including by raising constitutional arguments based on the right to freedom of expression (related to the issue of whether the GIMF was a terrorist organization). Objections were raised to the objectivity of the primary expert witness called by the prosecution to give testimony on the Al-Qaida movement, its offshoots, global jihadism (including virtual jihadism) and the methods and style of GIMF propaganda and the organization's use of the Internet. The defence also challenged whether activities undertaken by GIMF and associated groups amounted to terrorism, as well as the reliability of evidence related to the interception of Internet-based communications in Austria and Canada and the accuracy of translations of the records of these communications from Arabic into French. The defence asked the court to find that different messages circulated by Mr. Namouh on behalf of GIMF should be taken figuratively and not as acts counselling or encouraging acts of terrorism.

In considering the defence arguments in relation to the nature of the material posted or communicated on behalf of GIMF, the court concluded:

> The Court has no doubt on this subject. The context of these messages clearly refers to real actions encouraged by the GIMF. Death and destruction are everywhere. The jihad promoted by the GIMF is a violent one. This promotion clearly constitutes counselling ("encouragement") and sometimes a threat of terrorist activity. Therefore, this activity clearly falls within the definition of terrorist activity within the meaning of Section 83.01 of the Criminal Code.

In finding that Mr. Namouh was guilty of counselling or encouraging acts of terrorism, the court referred to intercepted communications containing statements which showed the zealous, active nature of his participation in the activities of GIMF. Also relevant in the court's view were several posts, including the one below from 12 December 2006, in which the defendant expressed his wish to conceal his activities, and those of GIMF, by removing incriminating computer data:

> [TRANSLATION]
> Urgent Urgent Urgent
> May the peace, mercy, and benedictions of Allah be with you
> I want to erase all the jihadist films and books that are on my computer without leaving any traces, may Allah bless you, because I suspect that someone has inspected my computer.
> May the peace, mercy, and benedictions of Allah be with you.
>
> In other communications, the defendant enquired about the use of anonymizing software and similar tools that could be used to conceal his activities. Following trial in October 2009, the defendant was found guilty of all charges; he was later sentenced to life imprisonment.

(b) Joint investigations

287. While the concept of "joint investigations" is mentioned in some international treaties (e.g. article 19 of the United Nations Convention against Transnational Organized Crime), there is no express reference to the strategy in the universal counter-terrorism instruments. Nevertheless, such an approach to investigations is entirely consistent with the underlying principles and spirit of the international cooperation elements of these instruments. Some countries, particularly in Europe, have successfully adopted this approach in a number of terrorism-related investigations, and the important role of Europol in establishing and supporting joint investigation teams is noted. The main purpose of these joint investigation teams, which comprise both national law enforcement officers and Europol officers, is to carry out investigations for a specific purpose and limited duration in one or more member States.[152]

288. Europol works with a system of national units, which are designated contact points within national police forces. It facilitates and encourages information exchange between member States through a secure digital network and provides a system of 17 analytical work files within the Europol legal framework, primarily aimed at enabling participating authorities to ensure full coordination and cooperation.

289. While it is difficult to assess, at the international level, the extent to which countries have collaborated in this manner, discussions at the expert group meeting highlighted the increasing awareness within the international law enforcement and security communities that the nature of modern terrorism and modi operandi of terrorists makes close cooperation in the investigation of terrorism an increasingly important component of successful efforts to disrupt, prevent and prosecute terrorist acts.

[152] Eveline R. Hertzberger, *Counter-Terrorism Intelligence Cooperation in the European Union* (Turin, Italy, United Nations Interregional Crime and Justice Research Institute, July 2007).

E. Formal versus informal cooperation

290. International cooperation in terrorism cases involving a cross-border element can take many forms, depending on the nature of the offence being investigated, the type of assistance sought, the applicable national legislation and the existence and status of any supporting treaty or arrangement.

291. Despite improvements in the overall level of their efficiency and effectiveness, formal mutual legal assistance procedures in criminal cases can still be lengthy processes, involving considerable amounts of bureaucracy for both requesting and requested countries. In many terrorism cases, particularly those involving Internet-related crimes, informal cooperation is increasingly proving to be as important as formal channels, avoiding considerable delays in situations in which time-critical actions (e.g. the preservation of Internet-usage data) are pivotal to a successful prosecution outcome. Participants at the expert group meeting highlighted the importance of the proactive development and utilization, wherever possible, by national intelligence, law enforcement authorities and prosecutors of mechanisms available for facilitating both informal and formal channels for international cooperation.

292. In many cases, for example when authorities in one country seek the preservation of Internet data held by an ISP in another country, it might be possible for authorities to cooperate informally to preserve such data for the purpose of the investigation or prosecution of a criminal offence.

293. The legal issues associated with the conduct of Internet-related criminal investigations, particularly issues related to jurisdiction, can be extremely complex. In cases in which investigators in one country need to access information held on computers located in another country, complex questions can arise about the legal authority and the basis for their actions. While it is possible for authorities in one country to deal directly with parties holding the information they seek in another, the responses to this approach may vary. As a general rule, it is desirable for authorities to work with their foreign counterparts, if possible on an informal basis, to obtain such information.

294. The form and method of cooperation will depend largely on the nature and intended purpose of the assistance requested. For example, while authorities in one country might be able to afford informal assistance to foreign counterparts by seeking the voluntary preservation of Internet-related data from ISPs, the search and seizure of such data will usually require judicial authorization, which can only be obtained by formal means.

295. Sometimes, the use of formal requests is the only method by which authorities can provide the required mutual cooperation. In such cases, it is important that countries have in place legislation and procedures that provide for timely and effective responses to requests, to maximize, to the extent possible, the likelihood of such assistance being successful.

Informal cooperation

296. Given the potential importance and urgency of locating and securing Internet-related data in terrorism investigations, and the probability that such data will be held in another country, investigators need to consider both formal and informal means of obtaining it. While formal mutual legal assistance channels might offer greater certainty with respect to associated legal issues, they also take longer and involve more bureaucracy than informal channels.

297. At the expert group meeting, the expert from Canada emphasized the critical role that the close informal cooperation between the Royal Canadian Mounted Police and Austria's Federal Agency for State Protection and Counter-Terrorism (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung), facilitated through Canada's liaison officer based in Vienna, played in the successful outcome of the prosecution. In addition to that case, other experts referred to other similar examples in which the use of liaison officers to facilitate informal cooperation had been instrumental in successful outcomes.

298. Internet-related data such as customer usage data held by ISPs is likely to be crucial evidence in terrorism cases involving the use of computers and the Internet. If investigators can secure physical possession of computers used by a suspect, as well as associated usage data held by ISPs, they are more likely to establish the link between the suspect and the commission of a crime.

299. With this is mind, it is important that investigators and prosecutors be fully cognizant of the potential importance of Internet-related data and the need to take the earliest possible steps to preserve it in a manner that ensures its admissibility as potential evidence in any later proceedings. To the extent possible, national law enforcement agencies should develop, either directly with ISPs or with counterpart agencies in other countries, clear procedures, involving both formal and informal elements, aimed at ensuring the earliest possible retention and production of Internet-usage data required for a criminal investigation.

300. In the United States, where many major ISPs are hosted, a "dual" approach is used by authorities to assist foreign counterparts with the retention and production of Internet-related data held by ISPs based in the United States, for possible evidential purposes. Under this approach, foreign requests for retention and production of user account information of Internet service providers could be handled in two ways:

(a) *Informal process.* There are two ways by which investigating authorities can secure the retention of Internet related data held in the United States by informal means: (i) foreign authorities can develop a direct relationship with ISPs and make a direct informal request that they retain and produce the required data; or (ii) if no direct relationship exists, they can make an informal request through the Federal Bureau of Investigation, which will make the request to the ISP;

(b) *Formal process.* Under the formal process, foreign authorities can make a formal mutual legal assistance request for data related to a specific user

account, which goes through the Office of International Affairs of the United States Department of Justice. Upon receipt, the request will be reviewed by the Department's Counterterrorism Section to identify whether it is connected to any investigation being led by the United States. If not, the request is submitted to a federal court for the necessary warrant authorizing the collection and transmittal of the required information to authorities in the requesting country.

301. The above approach for production of ISP-related data has been used successfully in several terrorism investigations by authorities in the United Kingdom and the United States. In one particular case, the procedures resulted in a United States-based ISP providing a substantial cache of Internet data which was crucial evidence in a prosecution in the United Kingdom.

F. Challenges and issues

302. By its very nature, the virtual geographical footprint, fragmented structure and rapidly evolving technology associated with the Internet presents ongoing challenges and issues for law enforcement and criminal justice authorities involved in the investigation and prosecution of terrorism cases. The discussion at the expert group meeting highlighted some areas that were currently problematic in relation to international cooperation. These included difficulties, in some cases, in satisfying the dual criminality requirements in extradition and mutual legal assistance requests. A number of experts had experienced cases in which mutual legal assistance or extradition requests had been delayed or refused because of problems satisfying dual criminality requirements. In some cases, that had been a result of the incompatibility of criminal offence provisions, but in others it was the result of an unduly restrictive approach to judicial interpretation of corresponding criminalization provisions by the judiciary. Several experts considered that this situation highlighted the need for training for members of the judiciary on international cooperation issues.

1. Protecting sensitive information

303. Experts from several countries at the expert group meeting referred to the ongoing challenges associated with the sharing of sensitive intelligence information by national law enforcement and intelligence agencies with foreign counterparts. Invariably, in terrorism cases criminal investigations and prosecutions are intelligence-based, at least in the early stages, and involve sensitive information that is closely held and protected. The disclosure of such information carries considerable risks, often not only for its originating source but also for the agency or agencies holding it, particularly if disclosure is likely to or might compromise an ongoing or future investigation or operation.

304. Assessments by national authorities on whether and in what circumstances to share such information, or under what conditions, can be complex, requiring them to balance a number of factors. Nevertheless, regardless of the specific criteria used for

assessing the possible sharing of information, in all cases, regardless of the circumstances, the agency making the disclosure will want to satisfy itself that the receiving agency will provide the agreed safeguards and protection to the information once in its possession.

2. Sovereignty

305. The concept of sovereignty, including the right of nations to determine their own political status and exercise permanent sovereignty within the limits of their territorial jurisdiction, is a widely recognized principle under international relations and law. Cases requiring the investigation or prosecution of cross-border activities of terrorists or other criminals might have sovereignty implications for those countries in which investigations need to be undertaken.

306. In some instances, concerns, valid or otherwise, held by national authorities about perceived intrusion into their State's sovereignty can impede effective international cooperation in criminal cases. It is therefore important, when considering investigative actions involving the collection of evidence related to computers or the Internet, for investigators and prosecutors to be mindful of the potential implications such investigative actions might have for the sovereignty of other States (e.g. authorities in one country remotely searching the computer being operated by a suspect located in another country).

307. Generally speaking, whenever possible, national authorities considering investigative steps relating to persons or objects located in another jurisdiction should notify and coordinate such actions with their foreign counterparts in relevant countries.

3. Retention and production of Internet-related data

308. As stated, in many terrorism cases an important part of the evidence against suspected offenders will relate to some aspect of Internet-related activity by the suspect (e.g. credit card billing information and customer usage data related to Internet-based communication such as e-mail, VoIP, Skype or related to social networking or other websites). In many cases, it will be necessary for investigating authorities to ensure that the relevant Internet-data is retained and preserved for later evidential use in proceedings. In this regard, it is important to note the distinction between "retention" of data and "preservation" of data. In many countries, ISPs are obliged by law to retain certain types of data for a specified time period. On the other hand, preservation refers to an obligation imposed on an ISP, pursuant to a judicial order, warrant or direction, to preserve data under specified terms and conditions for production as evidence in criminal proceedings.

309. One of the major problems confronting all law enforcement agencies is the lack of an internationally agreed framework for retention of data held by ISPs. While Governments in many countries have imposed legal obligations on locally based ISPs to retain Internet-related data for law enforcement purposes, internationally there is no single, universally agreed, standard time period for which every ISP is obliged to retain this information.

310. As a result, while investigators in countries that have imposed data-retention obligations on ISPs have some certainty, when engaged in purely domestic investigations, about the type of Internet data that will be retained by ISPs and for how long, the same cannot be said in those investigations in which they are required to collect data held by an ISP in another country.

311. In the United States, the current approach requires ISPs to retain usage data at the specific request of law enforcement agencies, with providers applying widely varying policies for storing data, ranging from days to months.

312. While there have been some efforts, most notably within the European Union, to achieve some consistency on this issue, this has proven, even at the European Union level, to be problematic. Under directive 2006/24/EC of the European Parliament and of the Council of the European Union of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending directive 2002/58/EC, in dealing with the retention of data held by providers of electronic communications services and public communications networks, European Union member States are obliged to ensure that regulated providers retain specified communications data for a period of between six months and two years. Nevertheless, despite the Directive, there remains no single consistent data-retention period for all ISPs hosted within the European Union, with periods ranging across the six-month to two-year time period set by the directive. Consequently, while there is a greater measure of certainty on these issues even within the European Union context, there are differences in the duration for which data is held by ISPs based there.

313. Several participants at the expert group meeting were of the view that the development of a universally accepted regulatory framework imposing consistent obligations on all ISPs regarding the type and duration of customer usage data to be retained would be of considerable benefit to law enforcement and intelligence agencies investigating terrorism cases.

314. With no universally agreed standards or obligations on ISPs and other communication providers relating to the retention of Internet-related data, it is important in criminal investigations that investigators and prosecutors identify at the earliest possible stage whether such data exists and for what time frame, whether it is likely to be of relevance to a prosecution and where it is located, along with the applicable time frame, if any, for which it must be retained by the party holding it. If in doubt, it would be prudent for authorities to contact their counterparts in the country in which the data is located and initiate steps (either formal and informal) that might be necessary to secure the preservation of the data for possible production. Depending on the circumstances, including their familiarity or relationship with the relevant ISP, authorities might consider contacting the ISP directly and seeking its informal assistance. Given sensitivities over compliance with customer confidentiality and national privacy laws, however, the level of responsiveness by ISPs to such direct, informal requests can be highly variable. It would always be prudent for investigators and prosecutors to communicate and coordinate their efforts with their foreign counterparts to secure the preservation and production of such information.

4. Evidential requirements

315. In order for testimony, exhibits or other information to be admissible as evidence in criminal proceedings, investigators and prosecutors need to exercise great care to ensure that the methods used in its collection, preservation, production or transmission are in full accordance with applicable laws, legal principles and rules of evidence. A failure to observe the requirements relating to the admissibility of evidence can weaken the prosecution case, to the point that authorities may even be obliged to discontinue or withdraw the prosecution case. In the *Namouh* case, Canadian prosecutors were able, through close collaboration with their Austrian counterparts, to ensure that vital evidence relating to the defendants' use of Internet chat rooms and websites was collected and transmitted to Canada for use in an admissible form even though there were differences between the two countries in the applicable rules of evidence.

316. In terrorism cases, there are a number of issues that can pose considerable challenges for authorities in ensuring the admissibility of certain types of information. Successfully overcoming them remains an ongoing challenge for all practitioners involved in the investigation and prosecution of terrorism-related cases, which often contain characteristics that could impede the admissibility of information. The transnational nature of terrorism cases, including the extensive use of intelligence (often provided by foreign partners under strict conditions) or highly specialized, often covert and intrusive, search, surveillance and interception methods as the basis for the collection of evidence, can present significant obstacles to authorities seeking to present admissible evidence to a court or tribunal.

317. In the terrorism context, with specific reference to evidential issues that might arise in relation to the Internet or computer technology, the general approach taken by investigators and prosecutors remains the same. Issues of particular importance are likely to be the need to secure, at the earliest possible opportunity, physical possession of computers or similar devices allegedly used by suspects; and the need to apply appropriate measures, in accordance with recognized good practice, to protect the integrity of these exhibits (i.e. the chain of custody/evidence) and undertake any digital forensics. A failure to follow these procedures could potentially affect the admissibility of this type of evidence. Other forms of evidence that might require particular care include material obtained as a result of search and/or surveillance activities, which must be carried out only within the terms of the appropriate judicial authorization.

318. When managing evidential issues, at the investigative stage, it is important that investigators have sufficient understanding of the legal rules/principles applicable to investigative actions they are undertaking as part of an investigation and/or to communicate closely with prosecutors, by both updating them and seeking legal advice. In cases in which evidence is being collected by authorities in one country for use in a prosecution taking place in another, close communication and coordination with foreign counterparts on the actions being taken to collect and preserve evidence is very important. As part of this coordination, it is important that authorities undertaking investigative actions clearly understand the evidential requirements/implications associated with their actions in the jurisdiction in which the evidence is ultimately to be used. Issues

associated with the admissibility of foreign evidence in terrorism-related cases are dealt with more broadly in the UNODC *Digest of Terrorist Cases*.[153]

5. Dual criminality

319. A requirement, commonly found in the universal counter-terrorism instruments and other international, regional and bilateral instruments relating to terrorism and transnational organized crime, is that only unlawful conduct that constitutes a criminal offence in both the requesting and requested States can form the basis for international cooperation. This requirement, known as "dual criminality", can present difficulties in all criminal investigations and prosecutions, not merely those relating to terrorism, involving some element of international cooperation. Several participants at the expert group meeting identified the dual criminality issue as an ongoing fundamental problem, which often led to mutual legal assistance or extradition requests being refused when authorities in requested countries considered dual criminality requirements not to have been satisfied.

320. In the terrorism context, in the absence of any universal obligation on States to criminalize specific unlawful conduct carried out over the Internet, central authorities are likely to be reliant, when making or receiving requests for international cooperation, on criminal offences established under terrorism-related legislation or their national penal codes. For example, in the case of alleged acts of incitement to terrorism that occur over the Internet, owing to differences in the legal approach taken by States with respect to such conduct, international cooperation requests might need to be based on inchoate offences such as solicitation.

321. In addressing this issue, it is desirable that Governments, when criminalizing the required unlawful conduct associated with terrorism, formulate offences in terms that are as close as possible to those contained in relevant instruments. Moreover, to the extent permitted under national legal systems, legislation should be drafted in a way that is not unduly restrictive with respect to the issue of dual criminality, providing central authorities and judges with sufficient scope to focus on and assess the substance of the unlawful conduct that is the subject of requests rather than adopting an unduly narrow approach. If this legislative approach is adopted uniformly by States, the full benefits of legislative harmonization intended by the instruments will be achieved and the potential for problems with respect to dual criminality reduced.

322. While issues related to dual criminality can create difficulties in criminal cases involving international cooperation generally, they can be particularly problematic in cases involving certain terrorism-related crimes committed by using the Internet (e.g. incitement) in which the risk of incompatibility between the national legislative and constitutional frameworks of corresponding States might be higher. An example, discussed at the expert group meeting, relates to the position regarding extradition from the United States of persons accused of the crime of incitement. In that country, there are strong constitutional safeguards relating to freedom of speech, enshrined in the First

[153] See United Nations Office on Drugs and Crime, *Digest of Terrorist Cases*, paras. 292-295.

Amendment to the United States Constitution. Under United States law, statements amounting to independent advocacy for any ideological, religious or political position are not considered criminal acts per se, although they might constitute acts amounting to the provision of information at the direction of or in order to control a terrorist organization, or fall within the scope of the offence of solicitation. Given this position, mutual legal assistance or extradition requests related to alleged acts of incitement involving some constituent element within the United States might be problematic from a dual criminality perspective, requiring authorities in both countries to take a flexible and pragmatic approach.

323. In addition to having compatible legislation and a flexible approach to applying such legislation, it is important that investigators, prosecutors and the judiciary be well trained and that they understand the way international cooperation mechanisms fit into the international community's response to terrorism and transnational organized crime.

6. Differences in the application of constitutional and human rights safeguards

324. Matters related to human rights and constitutional safeguards touch on many issues associated with the investigation and prosecution of terrorism, including those related to international cooperation. Again, using acts relating to the incitement of terrorism as an example, different national approaches to the application of constitutional rights and/or human rights can be reflected in different legal approaches. This can lead to difficulties in international cooperation cases in which States seek to request or provide assistance. For example, when authorities in one country make a request to their counterparts in another country for Internet-related data relating to statements made over the Internet amounting to incitement to commit terrorism in their jurisdiction, it will be of great relevance whether the alleged acts also constitute a crime in the requested country. In the broader context of Internet content control, when authorities in one country seek the removal of content that they consider incites terrorism, and which is hosted on a server located in another jurisdiction, applicable laws and constitutional safeguards for rights such as the freedom of expression may differ.

325. The situation involving some types of terrorist-related e-mail or Internet content being routed through, or stored on, ISPs based in the United States is particularly relevant. Depending on the nature and context of such content, these cases, which fall under United States jurisdiction, can be problematic given the strong protections afforded to freedom of speech by the First Amendment to the United States Constitution. In these cases, authorities in different countries need to communicate closely to determine what, if any, preventive or prosecution measures can be taken that are consistent with their respective national laws, legal and cultural norms and international counter-terrorism obligations.

7. Concurrent jurisdiction

326. Terrorism cases in which constituent elements of crimes are carried out over the Internet can raise complex jurisdictional issues, especially when a suspected offender is located in one country and uses Internet sites or services hosted by ISPs in another

to carry out constituent acts of a crime. There have been cases in which persons resident in one country have set up, administered and maintained websites used for promoting jihad and for other terrorism-related purposes in another.

327. The Belgian case of *Malaki el Aroud and Others* (see para. 377) is one such example. The defendant, who was living in Belgium, administered a website, hosted in Canada, which she used for promoting jihad and for other purposes aimed at supporting terrorist activities. The prosecution of terrorist-related activities in these situations relies heavily on effective international cooperation.

328. There are no binding rules under international law dealing with the issue of how States should deal with situations in which more than one State might assert jurisdiction to prosecute a crime involving the same suspect. Despite the fact that States have broad discretion with respect to the criteria applied, this typically involves balancing, or weighing up, different factors. These might include the relative "connectivity" between the alleged crime and particular States, including the suspect's nationality, the location where various constituent acts forming the crime took place, the location of relevant witnesses and evidence and the relative potential difficulties in collecting, transmitting or producing evidence in a particular jurisdiction. In some States, including Belgium, Canada and Spain, certain forms of jurisdiction are considered to be subsidiary to others. States with close connections to a crime (e.g. the crime is committed within their territory or by one of their nationals) are considered to have primary jurisdiction, with States holding jurisdiction on other bases acting only when the State with primary jurisdiction is either unwilling or unable to prosecute.[154]

329. Some countries, including Canada, apply a "real and substantial connection" test when determining whether criminal jurisdiction exists.[155] In Israel, when international cooperation requests are received from other countries, these are investigated domestically to determine if it can be proven that an offence under Israeli law was committed which should be prosecuted in Israel. If no prosecution results from such an investigation, Israeli authorities will transmit all available evidence [and transfer the suspected offender] via formal channels to the requesting country for the purpose of prosecution there. In the United Kingdom, legislation and case law dealing with certain terrorism-related crimes involving activity outside the United Kingdom (including via the Internet) allow British authorities to assert jurisdiction if it can be shown that a "substantial measure" of the activities constituting the crime took place in the United Kingdom, and if it can reasonably be argued that these activities should not be dealt with by another country.

330. In resolving issues related to concurrent jurisdiction or related international cooperation, central authorities (often prosecutors) need, at an early stage, to be cognizant of the need for early and collaborative communication with their counterparts in other

[154] International Bar Association, Legal Practice Division, *Report of the Task Force on Extraterritorial Jurisdiction* (2008), pp. 172-173.

[155] *R. v. Hape* [2007] 2 SCR.292, 2007 SCC 26, para. 62.

jurisdictions that might have an interest in instituting proceedings against the same suspected offender. The decision of when and how to initiate this communication should be taken on a case-by-case basis, after full consideration of the various factors that might be at play in the particular case. Useful guidance for prosecutors considering such issues can be found in the 2007 Guidance for Handling Criminal Cases with Concurrent Jurisdiction between the United Kingdom and the United States, issued by the Attorneys General of the United Kingdom and the United States,[156] which provides, in the context of "the most serious, sensitive or complex criminal cases" (to which the report related) for improved information-sharing and communication between prosecutors in the two countries. As the test for initiating such contact, the report provides the following: "does it appear that there is a real possibility that a prosecutor in the [other country] may have an interest in prosecuting the case? Such a case would usually have significant links with the [other country]." While the timing and method of communication on jurisdictional and international cooperation issues will vary according to the circumstances of the particular case, prosecutors might consider this test a useful guide to apply in the course of their work.

8. National privacy and data protection laws

331. National data protection or privacy legislation can often restrict the ability of law enforcement and intelligence agencies to share information with both national and foreign counterparts. Again, striking the appropriate balance between the human right to privacy and the legitimate interest of the State to effectively investigate and prosecute crime is and ongoing challenge for Governments and, in some cases (including responses to terrorism), has been the subject of concern.[157]

332. In addition to legislation that provides clear guidance to investigators, prosecutors and (in the case of Internet data) the ISPs holding data on the obligations pertaining to the collection and use of personal data, it is equally important that countries establish and operate effective mechanisms for the oversight of intelligence and law enforcement agencies. Governments should ensure that appropriate mechanisms are included in their national laws to enable authorities to share, subject to appropriate privacy safeguards, information relevant to the investigation and prosecution of terrorism cases with both national and foreign counterparts.

9. Treaty-based versus non-treaty-based requests

333. National approaches to the facilitation of non-treaty-based requests for cooperation vary, with some countries having restrictions on their ability to provide formal cooperation in the absence of a treaty. In recognition of this, the universal instruments against terrorism and transnational organized crime make provision for the instruments

[156] Available from www.publications.parliament.uk/pa/ld200607/ldlwa/70125ws1.pdf.

[157] See the 2009 report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (A/HRC/10/3), in which the Special Rapporteur expressed concerns related to the incursion of individual rights to privacy caused by heightened surveillance and intelligence sharing between State agencies.

themselves to be regarded as the legal basis for cooperation and for specified unlawful conduct to be treated as qualifying offences for mutual legal assistance and extradition purposes within the national laws of States parties.

334. Many countries, including China, rely upon the principle of reciprocity as the basis for providing international cooperation. Under Chinese law, law enforcement agencies and judicial authorities can conduct international cooperation, including mutual assistance or judicial cooperation (including extradition), on a treaty basis. In the absence of a treaty, reciprocity can also be a legal basis for mutual assistance and extradition cooperation. At the expert group meeting, the expert from China highlighted one example of successful cooperation between authorities in China and the United States that resulted in the closure of the world's largest Chinese-language pornography website, which was hosted in the United States and aimed at Internet users in China and other Asian countries.

335. Several participants at the expert group meeting referred to issues related to the sensitive nature of much information (often intelligence-based) associated with terrorism investigations and the inherent challenges, not only in the international cooperation context but also nationally, facing agencies wishing to share such information with counterparts. Several experts highlighted that information was often highly sensitive in nature and that sharing it became difficult in the absence of a formal information-sharing mechanism containing appropriate conditions regarding its use and disclosure.

336. This issue is considered in more detail in the next chapter, relating to prosecutions, in the context of evidential issues associated with translating intelligence material into admissible evidence and the disclosure of evidence in criminal proceedings.

VI. Prosecutions

A. Introduction

337. An integral part of the universal legal framework against terrorism, and of the United Nations Global Counter-Terrorism Strategy, is the obligation imposed on States to deny safe haven and bring to justice perpetrators of terrorist acts, wherever such acts might occur. In order to achieve the last of these objectives, countries not only require effective counter-terrorism legislation, criminalizing terrorist acts and facilitating necessary international cooperation, but also the capacity to apply specialized investigative techniques and prosecution strategies to ensure the collection, preservation, production and admissibility of evidence (often intelligence-based) when prosecuting suspected terrorists, while ensuring international standards of treatment for accused persons.

338. The role of prosecutors in the prosecution of terrorism cases has become increasingly complex and demanding. In addition to responsibility for the conduct of criminal proceedings, prosecutors are becoming more involved in the investigative and intelligence-gathering phases of terrorism cases, providing guidance or supervision on the legal and strategic implications of various investigative techniques. In the present chapter, the role of prosecutors in terrorism cases involving the use of the Internet by terrorists is considered, with a view to identifying, from a prosecutor's perspective, common challenges or obstacles and strategies and approaches that have been proven to be effective in the successful prosecution of perpetrators.

B. A rule-of-law approach to criminal prosecutions

339. An investigation and prosecution that is not conducted in full accordance with the principles generally associated with the rule of law and international human rights standards risks the integrity of the very fabric of the social and institutional norms and structures that terrorists themselves seek to undermine. It is therefore of fundamental importance that any prosecution of the perpetrators of terrorist acts be conducted with the utmost attention to the need to ensure a fair trial and fair treatment of accused persons.

340. The well-recognized principle that suspected terrorists should be afforded the same procedural safeguards under the criminal law as any other suspected criminals is strongly embedded and reflected in the universal instruments against terrorism and at the political level internationally. Just one of many examples of high-level recognition of this principle is General Assembly resolution 59/195, on human rights and terrorism, in which the Assembly highlighted the need for enhanced international cooperation

measures against terrorism, in conformity with international law, including international human rights and humanitarian law. In addition to incorporating this fundamental principal at a political level, the United Nations, through its Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, regularly reports to the Human Rights Council and to the General Assembly on areas of concern related to the human rights aspects of criminal justice measures targeting terrorism and makes recommendations for remedial action by relevant actors. Issues raised by the Special Rapporteur have included those related to the detention and charging of suspects.[158]

341. There are several publications dealing specifically with, and aimed at, promoting respect for human rights and the rule of law within the remit of prosecutors and criminal justice officers involved in terrorism prosecutions. In 2003 the Office of the United Nations High Commissioner for Human Rights produced the *Digest of Jurisprudence of the United Nations and Regional Organizations on the Protection of Human Rights while Countering Terrorism*. Within the Council of Europe, which has fully recognized and integrated the obligation to implement the protection of human rights as a fundamental principle into its instruments dealing with crime prevention and criminal justice issues, including terrorism, this principle is reaffirmed in the Guidelines of the Committee of Ministers of the Council of Europe on Human Rights and the Fight against Terrorism, adopted by the Committee of Ministers on 11 July 2002.[159] These documents provide valuable guidance for prosecutors working in the counter-terrorism field.

C. Role of prosecutors in terrorism cases

342. The role of the prosecutor in the conduct of criminal proceedings, including terrorism cases, varies between countries. In some countries, particularly civil-law jurisdictions, prosecutors have formal responsibility for overseeing the conduct of criminal investigations, supervising teams of investigators throughout, making decisions on search and surveillance activities and the laying of charges or indictments and dealing with international cooperation issues and the conduct of proceedings before the courts.

343. In an inquisitorial judicial system like the French one, for example, the prosecutor is generally tasked with beginning the legal action and with initiating preliminary investigations, defining the scope of the crimes; however, an examining judge, or *juge d'instruction*, will lead the formal judicial investigation, collecting and examining evidence. When the culpability of the subject can be excluded, the examining judge will close proceedings; otherwise, the subject will be committed for trial before a different judge. In terrorism cases, in addition to presenting the prosecution case to a judge, the chief prosecutor may petition or submit a motion for further investigation.

[158] Ibid.

[159] Any text created within the Council of Europe, irrespective of whether it is a binding convention or a "soft law" instrument, such as a recommendation or resolution issued by the Parliamentary Assembly or the Committee of Ministers, including any guidelines on various topics, must always be in compliance with the extensive case law of the European Court of Human Rights on the respective issue.

344. In other countries, particularly common-law jurisdictions, prosecutors have traditionally had less direct involvement with, or responsibility for, the conduct of criminal investigations, which are usually led by law enforcement agencies. Typically, in these jurisdictions, prosecutors assume formal responsibility for the conduct of prosecutions at the point of charging or the laying of indictments through to the final disposition of the proceedings. For example, in Nigeria, the national police are responsible for conducting criminal investigations. Upon completion, cases are referred to a prosecution authority that hold responsibility for the laying of charges and the conduct of the criminal proceedings.

345. A similar approach is taken in Indonesia, where a separation exists with regard to the investigation and prosecution of a criminal case. After the commencement of a criminal investigation, the investigator must report the progress of the case to the public prosecutor (art. 109, para. 1, of the Indonesian Criminal Procedure Code) and, once the investigation is concluded, must hand the case files over to the Public Prosecutor (art. 110, para. 1, of the Criminal Procedure Code), who will decide whether a case can be brought to trial (art. 139 of the Criminal Procedure Code).

346. Regardless of the specificities of the particular jurisdiction, however, the role played by prosecutors in terrorism cases continues to evolve to meet the increased demands placed on them by ongoing developments in the type, methods and complexity of terrorism-related crimes, counter-terrorism laws, new investigative techniques and international cooperation arrangements.

347. Experience shows that prosecutors are increasingly being required to play a more direct role in the investigation of crimes, not merely during the prosecution phase. Prosecutors are increasingly adopting a more technical and strategic role, not only informing counter-terrorism policy and legislation but also providing legal and strategic advice and guidance on legal issues during investigations that influence the likely success of any resulting prosecution. Experience shows that they are likely to undertake their role as part of a multidisciplinary/multijurisdictional team.[160]

348. Moreover, with increased visibility and scrutiny of terrorism prosecutions, including media coverage and monitoring by human rights groups and international bodies, prosecutors play a crucial role in ensuring that investigations and prosecutions not only are, but are seen to be, conducted in a way that is fair and efficient and that upholds international human rights standards.

D. The investigative phase

349. During the intelligence-gathering or investigative phase of counter-terrorism operations, prosecutors are often called upon to provide legal advice on issues related to the use of specialized investigative techniques.

[160]Yvon Dandurand, "The role of prosecutors in promoting and strengthening the rule of law", paper presented to the Second World Summit of Attorneys General, Prosecutors General and Chief Prosecutors, held in Doha from 14 to 16 November 2005.

1. Specialized investigative techniques

350. While new or emerging technology and search and surveillance techniques offer intelligence and law enforcement agencies enhanced opportunities to target terrorist activities on the Internet, they also carry legal risks in the context of prosecutions, to which prosecutors need to remain constantly vigilant. Moreover, owing to differences in national laws related to the collection and admission of evidence, these risks are higher when actions giving rise to evidence occur in a different jurisdiction from that in which the prosecution will be conducted. At the European level, the Council of Europe, being aware of these risks and the implied human rights issues, has elaborated a recommendation on special investigation techniques in relation to serious crimes, including acts of terrorism,[161] which contains, inter alia, general principles, operational guidelines and a chapter on international cooperation.

351. The legal risks related to emerging investigative techniques reinforce the need for prosecutors to be actively involved, at the earliest possible stage, in decisions taken during the investigative phase of terrorism cases to ensure that actions taken in the collection of potential evidence do not compromise the success of any subsequent prosecution. Issues related to the admissibility of evidence are dealt with in more detail elsewhere in the present chapter.

352. Constant and rapid changes in the technological capabilities of intelligence and law enforcement agencies with respect to surveillance and the monitoring and collection of intelligence or evidence of terrorist activity highlight the critical importance of the prosecutor's role in providing advice to investigators on the legal implications of such activities for prosecutions. Moreover, owing to the increasing likelihood, particularly in cases involving Internet-related activities across national borders, of authorities being required to coordinate and collaborate with foreign counterparts on related legal issues (e.g. preservation of Internet-related data held by ISPs), it is increasingly important that prosecutors be consulted and involved in decisions about investigative strategies at the earliest possible opportunity.

2. The use of multidisciplinary teams

353. Increasingly, authorities are turning to the use of multidisciplinary/multiagency teams, comprising law enforcement and intelligence agencies, as well as prosecutors, in the interdiction, disruption and prosecution of terrorist activities. The high level of trust, coordination and communication that was identified by the expert group meeting as vital to effective cooperation at an international level also needs to exist between national law enforcement, intelligence and prosecuting agencies. While there is no single approach through which these elements can be fostered, a clear understanding of the mandates and roles of contributing agencies, appropriate information-sharing powers and mechanisms (perhaps based on memorandums of understanding or similar arrangements) and regular coordination meetings or training activities will serve to strengthen these important national partnerships.

[161] Committee of Ministers of the Council of Europe, Recommendation Rec (2005)10 (20 April 2005).

354. While there are differences in how authorities in different countries coordinate and operate multiagency investigations, there are nevertheless broad similarities. In the United States, a task-force approach, using multidisciplinary teams from all relevant agencies, including prosecutors, is employed in conducting investigations related to terrorism in that country.

355. Under this approach, prosecutors are joined to, and form an integral part of, teams of intelligence, law enforcement and other specialist agencies that constantly monitor, assess and reassess different aspects of investigations into suspected terrorist activity. Counter-terrorism task forces and/or joint terrorism task forces coordinate the efforts of local, state and federal law enforcement agencies and prosecutors' offices. Many state and federal prosecution offices participate in such task forces, with methods and tasks varying from attendance at inter-agency meetings to the collocation of staff and legal advice in obtaining search warrants to reviewing cases and making recommendations on charges.[162]

356. In Canada, authorities use integrated national security enforcement teams (INSETs). In the *Namouh* case, the INSET comprised the Royal Canadian Mounted Police, the Canada Border Services Agency, the Canadian Security Intelligence Service, the Quebec Provincial Police, the Montreal Police Service and the Public Prosecution Service of Canada.

357. In Japan, it is common practice in terrorism-related investigations for police, even though they are legally independent, to report the case to the public prosecutor in the early stages of an investigation and to consult with them when evaluating evidence and interpreting laws.[163] A similar approach applies in Egypt.

358. In order to enhance the effectiveness and efficiency of counter-terrorism prosecutions, Governments often develop, within national prosecution agencies, specialized departments or units to deal with terrorism-related cases. This is the case in Indonesia, which has adopted a number of special measures, including the creation of a task force within the Attorney General's office on the prosecution of terrorism and transnational crimes. This task force is charged with facilitating and expediting law enforcement, during both the investigative stage, by coordinating with police (e.g. the involvement of state prosecutors during the interrogation of suspects), and during any subsequent prosecution, up to the final execution of the court's ruling.

359. While there may be variations at the international level in the means by which prosecutors become involved in, and integrated into, criminal investigations, the general approach adopted in many countries highlights the desirability of such integration and of a multidisciplinary, holistic approach to strategic and operational decisions taken during the investigative phase of terrorism cases.

[162] M. Elaine Nugent and others, *Local Prosecutors' Response to Terrorism* (Alexandria, Virginia, American Prosecutors Research Institute, 2005).

[163] United Nations Office on Drugs and Crime, *Digest of Terrorist Cases*, para. 212.

E. International cooperation

360. Issues related to international cooperation have already been dealt with in chapter VI above and need not be restated here. Specific issues of relevance to prosecutors, raised by experts at the expert group meeting, in cases involving elements of international cooperation relate to the mediation and resolution of issues related to the mode of cooperation, jurisdictional issues, dual-criminality requirements and the admissibility of foreign evidence, which experience shows presents an ongoing challenge. Given the common interest of all States in the successful prosecution of crimes related to terrorism, it is important not only that States have in place the legislative frameworks to facilitate this cooperation but also that prosecutors deal with the resolution of these issues in a proactive and collaborative manner.

F. The charging phase

1. Decisions whether to charge

361. In most countries, prosecutors have wide discretion in deciding whether to institute criminal proceedings and with which charges. Often such decisions are taken in accordance with guidelines or codes designed to ensure the fair, transparent and consistent exercise of this discretion. For example, in the United Kingdom, prosecutors make these decisions in accordance with the Code for Crown Prosecutors, which provides a threshold for charging based on evidential sufficiency and public interest. Prosecutors must be satisfied that the evidence before them discloses a "realistic prospect of conviction" before charging a suspect with a particular offence.[164] A similar approach applies in Egypt.

362. In the terrorism context, the public interest element of assessments of whether to charge is likely to be very strong, given the need, whenever possible, to prosecute terrorist acts or related crimes to protect the public and deter similar offences. In many cases, issues related to the sufficiency of available evidence may be determining factors and may be affected by the ability to use intelligence-based evidence without compromising its sources and methods of collection or other investigations. For this reason, in some cases prosecutors may need to elect to charge suspects with non-terrorism-specific charges in order to protect the integrity of intelligence material.

2. Use of general or non-terrorism specific criminal offences

363. In cases in which they need to intervene to prevent the commission of terrorist acts before there is sufficient evidence available to initiate a prosecution for the terrorist acts being planned, authorities might well need to rely upon other criminal offence provisions to provide the legal basis for their actions. In many cases in which suspected

[164] Crown Prosecution Service, "The Code for Crown Prosecutors" (London, 2010). Available from www.cps.gov.uk/publications/docs/code2010english.pdf.

terrorists have used the Internet as part of criminal activities, authorities have successfully used criminal offences such as solicitation, conspiracy or participating in, or providing material support to, terrorist groups, rather than substantive offences related to terrorist acts being planned. In this context, the availability of offences such as solicitation, conspiracy or criminal association is particularly useful. In some cases, authorities have been able to use other general criminal offences such as fraud or offences related to the possession or use of unlawful articles (e.g. false identity or travel documents, weapons), which provide investigators and prosecutors with an opportunity to disrupt or compromise the activities of terrorist groups before their planned attacks or activities can be carried out.

G. The trial phase: evidential issues

1. Issues related to the use of intelligence-based evidence

364. The integration of intelligence activities into criminal justice systems remains a fundamental problem for authorities in dealing with terrorism. As previously stated, in many terrorism cases evidence used by the prosecution has been derived from intelligence-based sources. A common challenge for authorities in all countries when prosecuting terrorism-related cases is how to protect the sensitive material underlying intelligence-based evidence while meeting their obligation to ensure a fair trial and effective defence for accused persons, including the obligation to disclose all material parts of the prosecution case to the defence.

2. Issues related to the collection and use of digital evidence

365. In terrorism cases involving the use of computers, similar devices or the Internet, digital evidence will be an important part of the prosecution case. In cases in which suspects were not physically present at the location where a terrorist act occurred, but nevertheless supported the commission of the act via some action on the Internet, the presentation of evidence showing their "digital fingerprints" can be compelling evidence of their complicity and culpability.

366. Experience shows that the use of digital evidence invariably gives rise to issues related to admissibility. It is therefore critical that great care be taken throughout the investigation and prosecution of the case to ensure that the methods used for its collection, preservation, analysis and production are in full conformity with the relevant rules of evidence or procedure, and that they follow established good practice.

367. Digital evidence can be technically complex and involve terms and concepts that are unfamiliar to the judge, jury or tribunal hearing the case. Prosecutors need to consider, in close coordination with investigators and experts, how best to present such evidence in a way that is easily understood and compelling. In this regard, the use of diagrams and similar visual aides showing the movement of data or linkages between computers and users might be beneficial.

368. As part of its case in prosecutions based on some form of computer use, the prosecution will need to identify the defendant as the user, at the material time, of the computer, device or Internet service used in the commission of the crime with which he or she is charged, and establish links proving that fact. There are several ways in which this can be done: *(a)* the defendant might make a confession or admit this fact; *(b)* his or her presence at the computer might be established by circumstantial means (e.g. he or she was the only person present where the computer was located or at the material time, he or she was the registered user of the relevant hardware or software, or there is other information on the computer that is solely within the defendant's knowledge); or *(c)* the link can be established by analysing the contents of the device/service the defendant was alleged to have used. This might involve the prosecutor producing evidence about specific characteristics of the material on the device (e.g. a document) or a comment made in an intercepted communication that are unique to the defendant. Finally, although they are not infallible, time and date stamps on digital files can be a compelling method of linking the defendant to the relevant device at times material to the commission of a crime.[165]

369. While the specifics may vary, the general approach taken by courts in many countries when determining the admissibility of evidence in criminal trials is based on relevance and reliability: is the evidence which a party seeks to adduce relevant, and is it reliable? In the case of relevant digital evidence, the challenge for prosecutors in many cases will be to satisfy the court of its reliability, both in terms of content and the methods used to collect and bring it before the court. The process of satisfying a court that digital evidence is admissible often involves proving the lawfulness of the methods used to collect it and preserve its integrity from the point at which it is collected through to its production in court. This is known as the "chain of custody" or "chain of evidence": the procedures, both operational and legal, for preserving the integrity of evidence. In most countries, there are strict legal rules relating to the chain of custody, which require evidence to be immediately recorded, centralized, sealed and protected against contamination pending trial, in some cases under the supervision of a judicial officer.

370. In terrorism cases involving the collection and use of intercepted communications or digital forensic evidence, prosecutors should ensure, in close collaboration with intelligence and/or law enforcement agencies, that such evidence has been collected in a lawful manner and preserved and produced in a manner that meets the evidential requirements of the jurisdiction in which it will finally be used. Collecting and producing digital data as admissible evidence, especially when it is held remotely by a suspect or related third party in other jurisdictions, is a challenging task for both investigators and prosecutors. In addition to the technical complexities of capturing and preserving the integrity of required data, the need in some situations to rely upon the cooperation of foreign intelligence, law enforcement or prosecuting agencies, acting under different laws and procedures regulating the collection and use of such data, can make such processes lengthy and resource-intensive.

[165] United States Department of Justice, Office of Justice Programs, National Institute of Justice, *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors* (2007), chap. 4, sect. IV. Available from www.ncjrs.gov/pdffiles1/nij/211314.pdf.

371. In investigations involving the collection of digital data located entirely within one jurisdiction, issues relating to its admissibility as evidence are likely to centre largely to the legal basis on which it was collected and its subsequent handling and preservation (i.e. the chain of custody or evidence). As always, care needs to be taken to ensure that the legal basis for its collection, forensic examination, preservation and production is in full accordance with applicable rules and procedures relating to the admissibility of evidence.

372. In the case of digital data collected in one or more jurisdictions for use in criminal proceedings in a different jurisdiction, the situation is considerably more complicated and requires careful attention on the part of investigators and prosecutors.

373. As soon as practicable after identifying the party holding and the location of data in a foreign jurisdiction relevant to an investigation, investigators and prosecutors should explore both informal and formal means of obtaining and preserving it for evidential purposes. Whenever possible and feasible, informal channels to secure the data for later use as evidence should be favoured, provided that the methods by which it is collected, preserved and transmitted to the receiving country comply with applicable evidential rules and procedures. In order to collect such data, investigators may need to consider requesting foreign counterparts to obtain search warrants to search and seize data or might need to consider using other means (e.g. publicly available web pages) or the use of voluntary foreign witnesses.

374. A case from Germany, concluded in 2009 and relating to the successful prosecution of four members of the Islamic Jihad Union, illustrates the size and complexity of many terrorism investigations and prosecutions. The case, which involved an investigation carried out over nine months, involved more than 500 police officers, many hours of electronic interception and surveillance and the collection of many exhibits, as well as extensive international cooperation between German authorities and their counterparts in Turkey and the United States. The size and complexity of the case highlight the significant resources that can be required to undertake investigations and prosecutions and the necessity and strengths of a team approach.

Fritz Gelowicz, Adem Yilmaz, Daniel Schneider and Atilla Selek

In September 2007, after an intensive investigation, German authorities, acting on intelligence received from their counterparts in the United States, arrested four members of the Islamic Jihad Union (often referred to as the "Sauerland cell"), who were in the final stages of preparations for a series of bombings at various public locations in Germany. Intended targets included bars and nightclubs in multiple locations in Munich, Cologne, Frankfurt, Dusseldorf and Dortmund, as well as the United States Air Force base at Ramstein. The total volume of explosive material that the defendants thought they had collected (it had been covertly replaced by authorities with a weaker harmless substance) was massive, potentially enough to exceed the force of the terrorist bombings in Madrid (2004) and London (2005).

Three of the defendants—Gelowicz, Schneider and Selek—were German nationals; the fourth, Yilmaz, was a Turkish national. Over the course of several months, the defendants acquired through legitimate sources 780 kg of hydrogen peroxide. On 4 September 2007, the authorities arrested the defendants when they met at a holiday home located in the Sauerland region of Germany and started to "cook" the hydrogen peroxide by adding other ingredients to heighten its explosive effect. (Unbeknown to the defendants, authorities had earlier replaced the hydrogen peroxide solution with a weaker, harmless solution.)

In August 2008, indictments were laid against Gelowicz, Schneider and Yilmaz by federal prosecutors. Selek was extradited from Turkey in November 2008 on the basis of an extradition request under the European Convention on Extradition and was indicted in December 2008. The charges included conspiracy to commit murder, preparing to carry out an explosion and membership of a terrorist organization.

The trial of all four defendants commenced in April 2009, lasting for three months before the defendants elected to admit the charges. The volume of evidence that the prosecution intended to present was huge, comprising 521 loose-leaf folders (enough to fill a 42-metre single shelf) and an estimated 219 witnesses. A large part of the prosecution case related to extensive electronic monitoring and surveillance that had been undertaken by German authorities during the investigation. Electronic investigative techniques included the use of wiretaps of audio conversations between the defendants and listening devices planted in vehicles and the house where they met to prepare the hydrogen peroxide for the explosive device, as well as the interception of their e-mail traffic. The prosecution proposed producing extensive digital evidence; however, there had been clear signs during the plot that the defendants were taking precautions against surveillance or monitoring. Over the course of the nine-month investigation, authorities faced a number of technical challenges. For example, the defendants had communicated using e-mail drafting (i.e. opening and reading draft messages in e-mail accounts) to prevent wiretapping by law enforcement agencies, and had used the insecure wireless LAN connections of innocent private citizens and encrypted communication via VoIP providers (e.g. Skype).

In the case of Gelowicz, the alleged ringleader of the group, he had used random Internet access via unsecured private residential LAN networks, employed at least 14 different e-mail accounts, changed vehicle licence plates and used a police scanner to monitor police radio traffic. He had protected data on his computer using encryption, which forensic experts tried without success to decrypt and access. Gelowicz eventually supplied the encryption key, but investigators found only traces of shredded data.

During the trial, the defence challenged the validity of the prosecution, questioning the basis for the investigation, which it asserted was inherently flawed, being based on United States intelligence, which it asserted included electronic monitoring of the defendants' communications, which was unlawful and had been provided in breach of their rights under the Constitution of Germany.

On 4 March 2010, the four defendants were found guilty of all charges and sentenced: Gelowicz and Schneider to 12 years of imprisonment, Yilmaz to 11 years of imprisonment and Selek to 5 years of imprisonment.

3. Issues related to use of foreign evidence

375. Legal principles and procedures related to the collection and admissibility of evidence in criminal proceedings often differ between jurisdictions. One of the major

challenges confronting investigators and prosecutors in any criminal investigation and prosecution with a cross-border character (in both the requested and requesting countries) is ensuring that necessary evidence is collected, preserved, transmitted and produced in accordance with the legal procedures and rules of evidence applicable in the respective jurisdictions in a form that is admissible where the trial will take place.

376. The process of "mediating" different aspects of evidence between countries can be a complex, time-consuming process but is a critical factor in the success of prosecutions. Any legal deficiencies in the methods by which evidence ultimately used at trial is collected or produced will almost certainly be challenged by defence lawyers.

377. A useful example, highlighting the types of issues that can arise in this context, can be found in the Belgian case of *Malika el Aroud and Others*, which related to the activities of a group of defendants involved in establishing and administering several websites used to disseminate terrorist propaganda and information useful to terrorists as well as serve as a forum for communication. Several of the defendants lived in Belgium, but the primary website on which they carried out their activities (minbar-sos.com) was hosted in Canada.

Malika el Aroud and Others

Introduction

In December 2008, after lengthy, intensive and complex investigations coordinated between intelligence, law enforcement and prosecution authorities in France, Belgium, Switzerland, Italy, Turkey, the United States and Canada, a number of persons with suspected links to the Al-Qaida terrorist organization were arrested and charged in France and Belgium with a range of criminal charges, including participation as a member of a terrorist group, financing of terrorism and providing information and material means to a terrorist group.

In carrying out the alleged acts forming the basis of these charges, the suspects had made extensive use of the Internet. The investigation into their activities involved complex electronic surveillance, wiretaps and other forms of monitoring by intelligence and law enforcement agencies. In successfully bringing the case to a conclusion, authorities in several jurisdictions were required to cooperate, on both a formal and an informal basis.

The case is an example of highly successful cooperation in criminal prosecutions related to terrorism with Internet-related aspects between national authorities across participating States, and highlights many aspects of good practice referred to in the present publication. References to these aspects are made throughout chapters V and VI, on international cooperation and prosecutions.

The case, which had linkages to other cases in several countries, revolved primarily around the activities of Malika el Aroud, a female Belgian national of Moroccan descent, and her husband, Moez Garsallaoui, a Tunisian national. Both were actively involved in the dissemination of radical jihadist propaganda and the recruitment, organization, direction and funding of a group of young men from Belgium and France to take part as jihadists in Afghanistan and elsewhere.

While some of these activities were undertaken using other methods, the couple used the Internet extensively to undertake these actions, including for communication. In addition to El Aroud and Moez Garsallaoui (who, together with an accomplice, Hicham Beyayo, were tried in absentia), other defendants tried were Ali el Ghanouti, Said Arissi, Jean-Christophe Trefois, Abdulaziz Bastin, Mohamed el Amin-Bastin and Hicham Bouhali Zrioul

The Belgian case has close linkages to both a French case, involving the defendants Walid Othmani Hamadi Aziri, Samira Ghamri Melouk, Hicham Berrached and Youssef el Morabit, who were tried and convicted before the Tribunal de Grande Instance de Paris,[a] and an investigation and prosecution in Italy relating to Bassam Avachi and Raphaël Gendron.

Background

In August 2007, Belgian authorities received information from their French counterparts concerning the activities on the Minbar SOS website (itself hosted in Canada), which they suspected was being used to disseminate Salafist propaganda calling for jihad against France. The site was allegedly administered by El Aroud and Garsallaoui. As the investigation widened, other similar websites were identified.

Authorities suspected that El Aroud and Garsallaoui, acting together through the site, were identifying and recruiting individuals from Belgium to fight in Afghanistan. El Aroud posted inflammatory material calling upon young people to sign up for jihad.

Malika el Aroud and Moez Garsallaoui

Malika el Aroud and Moez Garsallaoui were already well known to European counter-terrorism agencies. In 2003, El Aroud had been tried and acquitted by a court in Belgium of alleged involvement in a jihadist logistical support network used in the murder of an anti-Taliban resistance leader in September 2001. One of the two assailants was El Aroud's first husband.

In 2007, El Aroud was prosecuted in Switzerland, along with Garsallaoui, her second husband, for providing "support to a criminal organization" and "public incitement to violence and crime" through different websites they had both set up in Switzerland. She was convicted and sentenced to a six-month suspended sentence by the Tribunal pénal fédéral de Bellinzone.

On 21 December 2007, El Aroud was arrested in Belgium on suspicion that she had attempted to help a prison inmate, Nizar T., to escape from custody; she was released after 24 hours, however, owing to insufficient evidence. In 2004, Nizar T. had been convicted by a court in Belgium and sentenced to 10 years of imprisonment for preparing a terrorist attack on the United States military base at Kleine-Brogel in 2007. This arrest occurred while investigations were already under way in relation to her suspected activities on Minbar SOS.

The websites

The websites established by El Aroud, including Minbar SOS, were used as a platform for posting propaganda (e.g. videos and photographs), circulating books and publications and communicating. Each of the members was provided with a login/pseudonym and an electronic address so that they could exchange private messages, sometimes encrypted in closed chat rooms hosted on the sites. These would contain instructions, intelligence, propaganda and constant calls for massive jihad. Some material contained clear references to Al-Qaida leadership and included postings of attacks on United States troops in Iraq.

Messages with explicit threats (e.g. a message entitled "Against French terrorism in Afghanistan, only one solution") were posted, along with a map of the Paris RER commuter train network, on which some of the main stations had been highlighted with radioactivity or biological contamination symbols. Some messages gave explicit instructions on how to transfer funds to members of the jihad. By the end of 2008, the primary site, Minbar SOS, had more than 1,400 subscribers.

As part of a joint investigation, Belgian and French authorities intercepted communications on websites, e-mails and phone calls, and monitored and traced financial flows. Nevertheless, while Belgian security agencies closely monitored Internet activity on the Minbar SOS website aimed at recruiting fighters for Afghanistan, they could do little to prevent El Aroud from administering the site, owing to strong freedom of speech protection under Belgian law.

The French tribunal, which eventually dealt with judicial proceedings in that country related to the case, observed, when referring to the websites:

> The activity on these websites cannot be analysed as a simple search for information or intelligence, but on the contrary, characterizes a conscious participation in a terrorist-oriented undertaking/mission.

In addition, in testimony at later trials, defendants Saïd Arissi and Hicham Beyayo stated, respectively, "I consider myself as a victim of the Internet propaganda" and " websites like Ribaat and Minbar SOS influence people like me who went to fight", illustrating the influential effect the activities undertaken through the site had on some individuals.

In a rare interview, for an article that appeared in The New York Times on 28 May 2008, El Aroud called herself "a female holy warrior for Al-Qaida. She insists (…) she has no intention of taking up arms herself. Rather, she bullies Muslim men to go and fight and rallies women to join the cause. 'It's not my role to set off bombs—that's ridiculous … I have a weapon. It's to write. It's to speak out. That's my jihad. You can do many things with words. Writing is also a bomb.'"[b]

Travel of recruits to the Federally Administered Tribal Areas of Pakistan

In addition to the activities conducted via the websites, Garsallaoui also toured the immigrant neighbourhoods of Brussels to recruit people face-to-face. Hicham Beyayo, a 23-year-old Belgian national of Moroccan descent who was arrested in the case and was a Minbar SOS site administrator before travelling to Pakistan, admitted being recruited in that way.

Garsallaoui's recruiting was not restricted to Belgium; he also recruited two French subscribers to Minbar SOS. One of those recruits, who travelled to the Federally Administered Tribal Areas of Pakistan and was later arrested, referred to the calls to "jihad" on Minbar SOS as "incessant" and said that the video propaganda he viewed on the site made him want to volunteer.

In December 2007, Garsallaoui and six recruits, including Hicham Beyayo, Ali el Ghanouti and Y. Harrizi, travelled to the Federally Administered Tribal Areas via Turkey and the Islamic Republic of Iran. The group remained there until the second half of 2008. While there, Garsallaoui was in regular contact with El Aroud via e-mail and sometimes Skype. In addition to sending photographs and other propaganda material, he posted statements and periodically tuned in to the forums on Minbar SOS.

On 26 September 2008, Garsallaoui posted an online statement on Minbar SOS calling for attacks in Europe: "The solution, my brothers and sisters, is not fatwas but booooooooms", the posting stated.

The arrests

Over a period of some months in the second half of 2008, some of the suspects began returning to Belgium. Belgian security services were placed on alert after El-Ghanouti and Harrizi returned from the Federally Administered Tribal Areas, and on 4 December 2008 Beyayo himself returned to Belgium.

Differing explanations are offered for the reasons the recruits returned to Belgium at this time. Some of the suspects suggested dissatisfaction with the treatment and conditions in the Federally Administered Tribal Areas, including restrictions on their ability to participate in jihad, and denied the existence of any "sleeper cell" aimed at carrying out attacks in Belgium. Belgian authorities, however, considered indications from intercepted communications as providing strong grounds for suspecting that the group might be in the final stages of planning a suicide terrorist attack (possibly using Hicham Beyayo) within Belgium, which required immediate action.

On 11 December, a week after Beyayo's return, Belgian authorities raided 16 locations within Belgium and arrested nine suspects, including El Aroud, Garsallaoui and Beyayo. Similar operations were conducted in France and Italy.

Criminal proceedings

Belgium

At trial, defence lawyers challenged different aspects of the prosecution case, including procedural grounds and the admissibility of certain evidence, including Internet-related data obtained on an informal basis from the FBI relating to ISPs based in the United States. Issues related to such evidence are dealt with in more detail later in the present publication.

Beyayo had been interviewed by authorities in Morocco on 20 May 2008. His defence lawyers argued that a violation of the right to a fair trial had occurred, based on suspicions that torture had been carried out by the Moroccan authorities on detainees suspected of terrorism. The court rejected those arguments.

Activities of Bryan Neal Vinas (United States)

In January 2009, United States national Bryan Neal Vinas travelled to Afghanistan, where he attempted to kill American soldiers during an Al-Qaida rocket attack against a military base. He was later arrested and returned to the United States, where he was charged with conspiring to murder United States nationals, providing material support to Al-Qaida and receiving military training from the group. Vinas pleaded guilty and received a prison term.

Belgian authorities prosecuting Beyayo, an accomplice of El Aroud, produced evidence from Vinas' trial to establish the extent of their activities and involvement in the Al-Qaida network. In statements, Vinas admitted to having met some of the Belgian recruits. The defence challenged the admissibility of this evidence on a number of grounds, but those arguments were rejected by the court.

Trial outcome

Following trial, on 10 May 2010, the Tribunal de Première Instance de Bruxelles dealt with the cases of nine defendants who had been prosecuted on different charges, falling into three groups: A, B and C.

The group A and C charges, respectively, comprised participation as a leading member of a terrorist group and participation in the activities of a terrorist group, including by providing information or material means or through any form of financing of a terrorist group's activity, knowing that such participation would contribute to the commission of a crime or offence by that group.

The group B charges comprised the commission of offences or the provision of assistance in executing offences by means of donations, promises, threats, abuse of authority or power, plots or schemes with the intent to commit crimes against people or assets in order to cause serious harm, as well as offences that, by their nature or context, could seriously harm a country or an international organization and that were committed intentionally with the aim of seriously intimidating a population or unduly forcing public authorities or an international organization to take action, or of seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization.

The sentences under the group A charges were as follows:

- Malika el Aroud: eight years of imprisonment and a €5,000 fine
- Moez Garsallaoui: eight years of imprisonment and a €5,000 fine (in absentia)
- Hicham Beyayo: five years of imprisonment and a €1,000 fine (in absentia).

The sentences under the group B charges were as follows:

- Ali el Ghanouti: acquitted
- Said Arissi: acquitted.

The sentences under the group C charges were as follows:

- Ali el Ghanouti: three years of imprisonment and a €500 fine
- Said Arissi: 40 months of imprisonment and a €500 fine
- Hicham Bouhali Zrioul: five years of imprisonment and a €2,000 fine (in absentia)
- Abdulaziz Bastin: 40 months imprisonment and a €500 fine
- Mohamed el Amin-Bastin: 40 months of imprisonment and a €500 fine
- Jean-Christophe Trefois: acquitted.

France

In France, five suspects (all French nationals of North African descent) were tried before the Tribunal de Grande Instance de Paris. Walid Othmani, Hamadi Aziri, Samira Ghamri Melouk, Hicham Berrached and Youssef el Morabit were charged with a variety of offences: financing of terrorism, conspiracy to commit a terrorist act and participating in a group constituted for the purpose of preparing a terrorist act specified in article 421-1 of the French Penal Code.

Italy

Bassam Ayachi and Raphaël Gendron (both French nationals) were charged by Italian authorities with criminal association with the aim of terrorism under article 207 bis, paragraph 1, of the Italian Criminal Code, which provides a penalty of 7 to 15 years of imprisonment for anyone found guilty of constituting, promoting, organizing, managing or financing groups that intend to carry out violent activities in furtherance of terrorist aims or the subversion of the democratic structure of the state, and a term of imprisonment from 5 to 10 years for individuals who associate with such groups.

The case established links between the two defendants and some of the defendants in the Belgian proceedings, as well as common elements of evidence, including evidence on a DVD of a suicide note written by one of the Belgian suspects.

On 3 June 2011, Ayachi and Gendron were sentenced to eight years of imprisonment.

Source: Eurojust, *Terrorism Convictions Monitor*, Issue 8, September 2010

[a] Judgement 18 February 2011 (No. d'affaire 1015239014).

[b] See "Al Qaeda warrior uses Internet to Rally Women", The New York Times (28 May 2008). Available from www.nytimes.com/2008/05/28/world/europe/28terror.html?_r=1&pagewanted=all.

378. In the El Aroud case, the prosecution produced evidence of Internet data, related to postings and chat room discussions. In the case of the e-mails (the latter sent from accounts held by Yahoo and Microsoft), the data was held on servers in the United States. Following an informal request for assistance, Belgian authorities were provided (within two weeks) with a CD by the FBI containing the data related to the specified e-mail accounts and other related accounts. The FBI stipulated that it had been provided by Yahoo and Microsoft voluntarily, as permitted by the provisions of the United States Patriot Act.

379. The defence challenged the admissibility of this evidence, asserting that the procedures used to collect, transmit and produce the evidence were unlawful, as it was collected in the absence of a search warrant, and on the basis that the informal procedures used did not follow the usual methods for international exchange of judicial information, thereby contravening article 7, paragraph 1, of Belgium's law of 9 December 2004 on international mutual assistance in criminal matters.

380. The Court rejected this argument, holding that: *(a)* the exchange of information had not occurred within the framework of mutual legal assistance; *(b)* no examining judge had been appointed to the case at the material time, which was being handled on an informal police-to-police basis; and *(c)* the procedure used was justified by the emergency aspect of the circumstances (i.e. the discovery of a suicide note posted on the Minbar SOS website by one of the suspects, leading to the belief that an attack on French soil orchestrated by Malika el Aroud and her conspirators was imminent). The Court held that on those grounds the Federal Magistrate was justified in concluding that this emergency police cooperation was founded on grounds of article 15, paragraph *(b)*, of

the International Convention for the Suppression of Terrorist Bombings (1997),[166] which provides for "exchanging accurate and verified information in accordance with their national law, and coordinating administrative and other measures taken as appropriate to prevent the commission of offences as set forth in article 2".[167]

381. Finally, the Court held that, as the legal basis for the information transmitted to Belgian police by United States authorities was valid, it could de facto be used by the Belgian judicial authorities. The Court added that the analysis relating to the United States-based e-mail addresses (or most of them) had been included in the judicial file following a letter rogatory executed in France.[168]

382. The case highlights the careful consideration that needs to be given, during the investigation phase of cases involving the use of foreign evidence, to the methods used in the collection and transmission of such evidence. This reinforces the importance, emphasized by several experts at the expert group meeting, of having prosecutors integrated into the investigation at the earliest possible opportunity, to identify and mediate potential evidential issues prior to trial.

383. In the *Namouh* case (Canada), it was necessary, at trial, for the prosecution to produce evidence collected by an Austrian police officer; this proved problematic. Under Austrian law, the police officer's evidence could be admitted as evidence in the form of a written deposition. This was not the case, however, under Canadian law, which generally excludes hearsay evidence and requires witnesses to appear in court and give oral testimony. In order to facilitate the production of the officer's evidence, Canadian prosecutors had to liaise closely with Austrian police and prosecutors to explain the applicable rules of evidence under Canadian law, as well as with defence counsel to facilitate an agreement that the officer's evidence could be produced in written form.

4. The use of expert evidence

384. In terrorism-related cases, it will often be necessary for prosecutors to present expert evidence to prove some specialized aspect or aspects of a case. The range of potential issues that might necessitate this type of evidence is very wide, however. From prosecutions already undertaken involving terrorist-related activity over the Internet, it is possible to broadly identify some areas in which investigators or prosecutors might need to give consideration to this issue.

385. The technology and communications fields continue to evolve at a rapid pace, with increasing complexity and specialization. It is quite likely that prosecutors might require several expert witnesses to explain different, but related, technical aspects of computer or communications systems or related activity in the course of the same

[166] United Nations, *Treaty Series*, vol. 2178, No. 38349.

[167] Eurojust, *Terrorism Conviction Monitor*, Issue 8, September 2010.

[168] Ibid.

proceedings, especially when there is proof that a suspect has used a particular computer, device or Internet-related service.[169]

386. In addition to evidence related to computer forensics in cases involving alleged participation in, or provision of material support to, terrorist groups, or incitement, recruitment or training, expert evidence might be required on the ideologies, objectives activities and organizational structures of particular terrorist groups or individuals.

387. Typically, cases involving the use of expert witnesses involves three steps or phases: *(a)* clear identification of the issues (and their scope) that require an expert opinion; *(b)* identification of a qualified expert; and *(c)* ensuring that the qualified expert uses admissible means.[170]

(a) Clear identification of the issues

388. Prosecutors, working in close coordination with investigators, should at the earliest possible opportunity identify the issues with respect to which they consider expert evidence will be required and engage the experts to undertake the necessary analysis, providing clear guidance on the key elements of evidence.

(b) Identification of a qualified expert

389. When selecting expert witnesses to give expert testimony on specialized aspects of evidence in terrorism prosecutions, prosecutors need to consider whether governmental or non-governmental experts should be used. While the use of governmental experts is permissible, and offers some advantages, this might not be desirable if pretrial disclosure processes or defence cross-examination of such witnesses at trial is likely to identify sensitive intelligence sources and the methods by which information supporting their opinions has been obtained. In order to avoid this potential pitfall, prosecutors might prefer to rely upon academic or non-governmental experts, who can base their evidence on publicly available information that can be readily disclosed without the risk of compromising intelligence sources or methods.[171]

390. A good example of a case in which non-governmental experts were engaged by the prosecution is the *Namouh* case, in which two witnesses were called to explain the goals and modi operandi of the Global Islamic Media Front (GIMF). The background to this evidence is described in paragraph 394 below.

391. Identifying a suitable expert, particularly in highly specialized fields, can be a significant challenge for less developed jurisdictions. Prosecutors, working with investigators, should take a proactive, cautious approach, exploring all avenues to secure (whenever possible) the necessary, suitably qualified, witness at the national level but, when necessary, taking steps to secure a suitable witness internationally.

[169] Walden, *Computer Crimes and Digital Investigations*, p. 383.

[170] National Institute of Justice, *Digital Evidence in the Courtroom*, chap. 3, sect. III.E.

[171] United Nations Office on Drugs and Crime, *Digest of Terrorist Cases*, para. 194.

(c) Ensuring that the expert uses admissible means

392. The need for prosecution witnesses to follow and apply recognized good practice in any examination or analysis they undertake in the particular field on which they are being called is clearly very important. This is particularly so for any specialist forensic analysis they undertake for the purpose of establishing the opinions they will offer as part of the evidence that will be presented by the prosecution. Investigators and prosecutors should consider, at the earliest possible opportunity, whether expert evidence will be required on any specialized aspects of the prosecution case and, if so, should consult and engage with suitable experts at the earliest possible point to ensure that the evidential basis for later expert testimony is preserved in an admissible form.

393. In some cases, especially those involving computer technology, evidence can be technically complex, and prosecutors and expert witnesses need to consider innovative ways of presenting such evidence to judges, juries or other fact finders at trial in a manner that is clear, easily understood and compelling. For example, the visual depiction of system design or data traffic, rather than oral testimony alone, might help fact finders to better understand technical aspects connected with computer or communication systems. Clearly, it is also important that the prosecutor have a sound working knowledge of the particular subject area so that he or she can present terms and concepts to the judge, jury or tribunal and effectively present the prosecution case.

394. The Canadian case of *Namouh* involved the extensive use of expert evidence (provided by an Royal Canadian Mounted Police expert on digital forensics) on digital evidence issues. These centred on the defendant's alleged use of a computer (seized from his home), and related Internet use, when participating in online discussion forums, uploading material onto websites and communicating with another accomplice located in Austria. This detailed expert evidence on digital forensic issues was necessary to satisfy the court that it was the accused who had operated the computers from which incriminating messages were sent, as well as to describe the ideologies and methods of GIMF, the global group in which the accused was an active participant.

395. Part of Namouh's defence focused on undermining this aspect of the prosecution case. It was asserted that, owing to the fundamental fallibility of the Internet, it could not be reliably used as a source of information for the expert witnesses to opine on the activity of GIMF and other terrorist groups. In particular, the defence asserted that the expert witnesses could not reliably ascertain whether postings on Internet chat forums, and other forms of electronic communications, were in fact authored by alleged terrorists or, in the alternative, were attributable to agents of the State, acting as agent provocateurs. In this case, an expert for the prosecution offered testimony sufficient to satisfy the court of the reliability of the methods and Internet-based materials relied upon, and to assign the corresponding weight to the expert testimony.

396. It is noteworthy that these electronic communications took place in Arabic and had been translated into French, with the translation in French being filed in court by the prosecution along with the original transcript in Arabic. This aspect of the case also highlights the care that is required when authorities seek to produce, as evidence,

translations of conversations or documents, including transcripts of intercepted communications, in other languages.

397. In addition to expert testimony on critical digital evidence, the prosecution called expert evidence on the activities and goals of GIMF; its methods of coordinating and recruiting new members, propagating radical ideology and conducting military training; and the methods by which it communicated via the Internet. In fact, the prosecution produced written reports of two experts on these issues, with one of the experts testifying in court to support the report conclusions. The expert from Canada at the expert group meeting, emphasized the importance of prosecutors having more than one potential expert witness on key evidential issues, both in terms of corroborative effect and as a contingency plan.

398. The value of this type of expert evidence in prosecutions involving charges related to support for a terrorist organization is illustrated in the following statement by the trial judge, referring to the "real actions counselled by the GIMF", which was the subject of this expert prosecution testimony:

> Counsel for the defence invites the Court to regard the various messages circulated by the GIMF as being used figuratively. The Court has no doubt on this point. The context of these messages clearly refers to *real actions counselled* by the GIMF. Death and destruction are everywhere. *The jihad that GIMF promotes is violent.* [emphasis added] This promotion clearly constitutes counselling and sometimes a threat of terrorist activities. As a result, this activity clearly falls within the definition of terrorist activity under section 83.01 [of the] Criminal Code.[172]

H. Other issues

1. The need for contingency planning and continuity

399. The complexity of terrorism-related prosecutions, particularly those involving international cooperation or highly technical elements, make it highly desirable that a team of prosecutors conduct cases, and that each be familiar with and, if necessary, competent to continue the proceedings in the event any member of the team is unexpectedly unavailable to continue with the case. This precaution will ensure that the proceedings are conducted to a high standard and minimize the likelihood of an unsuccessful outcome. The cases of Namouh (Canada) and Gelowicz, Yilmaz, Schneider and Selek (Germany) are two useful examples of large, complex prosecutions that required a team approach, with at least one prosecutor being involved throughout the case. In the case from Germany it is noted that the original estimate of the trial's duration was two years. The actual duration was much shorter, owing to guilty pleas by the defendants, but even then the trial itself took three months.

[172] Justice C. Leblond, 1 October 2009.

2. The need for enhanced training and capacity

400. In order to ensure an integrated rule-of-law approach and to preserve the integrity of criminal justice responses to terrorism, countries need to have robust and ongoing processes to strengthen the capacity of prosecutors to implement national counter-terrorism legislation and related international cooperation obligations. The nature of counter-terrorism legislation and investigations and the speed, complexities and cross-border nature of Internet-related activity mean investigative teams, including prosecutors, need to make many decisions regarding different aspects of the case within tight time constraints. It is important that they be adequately trained and competent to discharge their core functions in terrorism cases.

401. In countries where the risk of terrorist activity is high and institutional capacity within prosecution services and other criminal justice agencies is low, a high priority should be placed on developing specialist capacity within these agencies, both in terms of prosecuting cases and with respect to related international cooperation mechanisms.

VII. Private sector cooperation

A. The role of private sector stakeholders

402. While the responsibility for countering the use of the Internet for terrorist purposes ultimately lies with member States, the cooperation of key private sector stakeholders is crucial to effective execution. Network infrastructure for Internet services is often owned, in whole or in part, by private entities. Similarly, private companies typically own the social media platforms that facilitate the dissemination of user-generated content to a broad audience, as well as popular Internet search engines, which filter content based on user-provided criteria.

403. The effectiveness of the Internet as a medium for disseminating content related to acts of terrorism is dependent on both the originator of the communication and its audience having access to Internet technologies. As such, the primary approaches to limiting the impact of such communications are by controlling access to the network infrastructure, by censoring Internet content or a combination of both.[173] While the level of government regulation of the Internet varies greatly among member States, in the absence of a global, centralized authority responsible for Internet regulation, private stakeholders such as service providers, websites hosting user-generated content and Internet search engines continue to play an important role in controlling the availability of terrorism-related content disseminated via the Internet. Self-regulation by these private sector stakeholders may also assist in countering terrorist communication, incitement, radicalization and training activities conducted by means of the Internet. Private monitoring services also play a role in timely identification of Internet activity which may promote acts of terrorism.

1. Internet service providers

404. In many Member States, user access to the Internet is controlled by non-State actors, such as private sector telecommunications providers, which own or manage the network infrastructure. These service providers may be well placed to assist in the collection of communications data or to disclose such data, as may be appropriate,[174] in furtherance of a specific investigation by law enforcement, criminal justice and intelligence agencies into potential terrorist activity. Communications data held by ISPs may constitute key evidence against perpetrators of Internet-related crime, or may provide links to additional evidence or collaborators relevant to the investigation.

[173] Conway, "Terrorism and Internet governance: core issues", p. 26.

[174] Subject to applicable safeguards and privacy regulations.

405. For example, ISPs may require users to provide identifying information prior to accessing Internet content and services. The collection and preservation of identifying information associated with Internet data, and the disclosure of such information, subject to the appropriate safeguards, could significantly assist investigative and prosecutorial proceedings. In particular, requiring registration for the use of Wi-Fi networks or cybercafes could provide an important data source for criminal investigations. While some countries, such as Egypt, have implemented legislation requiring ISPs to identify users before allowing them Internet access, similar measures may be undertaken by ISPs on a voluntary basis.

(a) Cooperation with Government authorities

406. Given the sensitivities associated with terrorist-related cases, private sector stakeholders may be incentivized to cooperate with law enforcement authorities by the positive reputational impact of such cooperation, when appropriately balanced with due care to respect fundamental human rights, such as freedom of expression, respect for private life, home and correspondence, and the right to data protection. The avoidance of detrimental consequences arising out of a failure to cooperate may also be a motivating factor. For example, ISPs may cooperate out of concern regarding the possible negative connotations of being associated with supporting terrorist activity. Liability concerns associated with hosting certain types of Internet content may also influence the level of cooperation from private sector entities.

407. The Egyptian expert indicated that the national experience of Egypt reflected a cooperative response by relevant private sector stakeholders to reasonable requests from governmental authorities for the disruption of access to terrorism-related Internet content. Additionally, ISPs in Egypt were reportedly motivated to collaborate, in part, by the recognition of the alignment of the interests of the ISPs, which could themselves be the subject of a terrorist attack, and governmental authorities, which sought to prevent and prosecute such acts of terrorism.

408. While private sector actors may demonstrate a willingness to voluntarily remove unlawful content, they may also be compelled to do so pursuant to domestic legislation. For example, in the United Kingdom, section 3 of the Terrorism Act 2006 provides for "take-down" notices, which may be issued to ISPs by law enforcement authorities (see para. 172 ff above). Take-down notices are used to advise those hosting content that such material is deemed to be unlawfully terrorism-related, in the opinion of the law enforcement official. ISPs that have been issued a take-down notice are required to remove the terrorist-related content within two working days. While other jurisdictions also employ take-down notices for certain offences, this is more commonly applied in connection with cases of copyright infringement or sexually explicit content.

409. The State of Israel highlighted its successes in relation to the cooperation of foreign private sector representatives in Israel. For example, in several investigations involving computer crimes, requests were made to representatives of Microsoft and Google in Israel. Upon receipt of a duly served court order, information requested by the investigative authorities was immediately provided. In some cases in which it was

necessary to address requests to private sector representatives based in the United States, the formal process of requesting legal assistance via governmental authorities was typically employed, with occasional resort being successfully made to direct requests to foreign private sector corporations for identification data.

(b) Data retention

410. Several Member States have recently introduced, or proposed the introduction of, legislation requiring telecommunications service providers to routinely capture and archive communications data relating to their users. In 2006, driven in part by the terrorist attacks in Madrid in 2004 and in London in 2005,[175] the European Union enacted a directive on the mandatory retention of communications traffic data (directive 2006/24/EC of the European Parliament and of the Council of the European Union of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending directive 2002/58/EC).[176] Directive 2006/24/EC acknowledges the challenges posed by legal and technical differences between national provisions concerning the types of data to be retained, and the conditions and periods of data retention.[177] The directive therefore seeks to harmonize the minimum data retention obligations of electronic communications service providers operating in European Union member States for the purpose of prevention, investigation, detection and prosecution of criminal offences.

411. Directive 2006/24/EC obliges member States to adopt legislation[178] requiring telecommunications providers to retain certain traffic data related to electronic communications[179] for a period of between six months and two years. This traffic data includes the information necessary to identify the originator and the recipient of Internet mail and telephony communications, together with information on the time, date and duration of those communications, but does not extend to the content of electronic communications.[180] Such data must be made available in connection with the investigation, detection and prosecution of serious crime to the national law enforcement authorities and, through the national authorities,[181] to their counterparts in other European Union member States, in accordance with the requirements of their respective national laws.

[175] European Commission, "Report from the Commission to the Council and the European Parliament: evaluation report on the Data Retention Directive (Directive 2006/24/EC)", document COM(2011) 225 (Brussels, 18 April 2011), sect. 3.2.

[176] *Official Journal of the European Union*, L 105, 13 April 2006.

[177] Ibid., preamble, para. 6.

[178] As at April 2011, enacting legislation was in force in 22 European Union member States.

[179] This includes data generated or processed by service providers in the course of their activities, such as for the purpose of transmitting a communication, billing, interconnection, payments, marketing and certain other value-added services.

[180] *Official Journal of the European Union*, L 105, 13 April 2006, art. 5.

[181] Ibid., art. 4.

412. For example, once transposed into domestic legislation, and subject to applicable procedural requirements, national law enforcement authorities may request access to data from service providers to identify subscribers using a specific IP address and those with whom that individual has been in contact over a given period of time.[182] Further, investigations of terrorist acts may rely on data retained by service providers which reflects the length of time taken to plan the act to identify patterns of criminal behaviour and relations between accomplices to the act and to establish criminal intent.[183] Some European Union member States[184] have indicated that data retention records are the sole means of investigating certain crimes involving communication over the Internet, such as chat room postings, which are traceable only through Internet traffic data.[185] Several European Union member States[186] have also reported using data retained by service providers to clear persons suspected of crimes without having to resort to other, more intrusive, methods of surveillance such as interception and house searches. Location data is also important when used by law enforcement to exclude suspects from crime scenes and to verify alibis. Data retained pursuant to enacting legislation also enables the construction of trails of evidence leading up to an act of terrorism, including by facilitating the identification or corroboration of other forms of evidence on the activities and links between suspects.[187]

2. Websites and other platforms hosting user-generated content

413. Terrorist-related content hosted on popular websites containing user-generated content has the potential to reach a significantly broader audience than content on traditional specialized websites, bulletin boards and web forums, which generally appeal to a self-selected group of individuals. According to the video-sharing website YouTube, 48 hours of user-generated videos are uploaded to its website every minute, resulting in the equivalent of almost eight years of content being uploaded every day.[188] Making content available to the estimated 8 million unique YouTube users per month significantly lowers barriers to accessing terrorist-related content. The sharp rise in popularity of user-generated content in recent years increases the logistical difficulty of monitoring terrorism-related content. Additionally, users of video-hosting websites may inadvertently encounter terrorism-related content as a result of searching for, or viewing, more moderate material, owing to embedded mechanisms which automatically suggest related content.

[182] European Commission, "Report from the Commission to the Council and the European Parliament: evaluation report on the Data Retention Directive (Directive 2006/24/EC)", sect. 5.2.

[183] Ibid., sects. 3.1 and 5.2.

[184] Belgium, Ireland and the United Kingdom.

[185] European Commission, "Report from the Commission to the Council and the European Parliament: evaluation report on the Data Retention Directive (Directive 2006/24/EC)", sect. 5.4.

[186] Germany, Poland, Slovenia and the United Kingdom.

[187] European Commission, "Report from the Commission to the Council and the European Parliament: evaluation report on the Data Retention Directive (Directive 2006/24/EC)"sect. 5.4.

[188] YouTube statistics available from www.youtube.com/t/press_statistics.

The Filiz G. case

In this German case, the defendant, Filiz G., was found guilty on charges of recruiting members or supporters for foreign terrorist organizations (Al-Qaida, the Islamic Jihad Union and Deutsche Taliban Mujahideen) and of providing support to those organizations.

In March 2009, the defendant joined an Internet forum and started publishing translations into German of communiqués of terrorist organizations denouncing alleged crimes of international armed forces in Iraq and Afghanistan and calling on users to join or support jihad. Being the spouse of an incarcerated German terrorist, Filiz G. was soon granted administrator rights for the Internet forum. By the time of her arrest in February 2010, the defendant had posted more than 1,000 contributions and commentaries, in both a publicly accessible part of the Internet forum and in a closed section that was accessible only to registered members. She opened nine video channels on the YouTube portal, and posted 101 videos in all on those channels, including both publications by terrorist groups such as Al-Qaida and the Islamic Jihad Union and videos she had produced herself. The defendant cooperated very closely with M., the "media focal point" of the Islamic Jihad Union. He contacted her via the Internet and initially asked her to translate texts with religious content from Turkish into German. Subsequently, he gave her links to videos, which the defendant posted on YouTube, and asked her to assist in collecting donations.

In one instance, the defendant translated material published on a Turkish-language web page into German and published it on a German web page. The material appealed to donors to support "families of the mujahideen in Afghanistan who are resisting the cruel attacks of the crusading nations". The text was accompanied by seven pictures, one showing various food items and the other six showing children armed with assault rifles and other weapons.

In addition to publishing fundraising material, the defendant was also involved in the actual collection of funds. To preserve the anonymity of donors, she opened a post office box, to which the donors addressed envelopes with their Internet user names containing cash (generally contributions of a few hundred euros). She then used Western Union Financial Services to transfer the funds to an intermediary in Turkey, who forwarded it to M. in Waziristan. The defendant also posted videos on the Internet thanking the donors (who for this purpose were assigned nicknames linked to their Internet user names) and informing them of the progress of the fundraising campaign.

At trial, in March 2011, the defendant admitted the charges and was sentenced to two-and-a-half years of imprisonment. In sentencing her, the court found that she had been fully aware that the propaganda material she was disseminating came from terrorist organizations and that the funds she collected and transferred were intended to buy, in addition to humanitarian goods, arms and munitions for those organizations. In noting that the offences had taken place mainly over the Internet, the sentencing judge remarked:

> […] the court attributes particular weight to the significant dangerousness of the dissemination of jihadist propaganda through the Internet. Materials once uploaded on the Internet can practically no longer be controlled or removed from the web, as other users can download, make use of and further disseminate them. Considering the nearly worldwide use of this medium and the immensely high and continuously growing number of users, the Internet constitutes a platform of ever greater importance for terrorist groups to disseminate their aims and their propaganda and to evoke a worldwide climate of fear of omnipresent terrorist threats. The dissemination of contributions such as those published by the accused thus amounts to "intellectual arson". It is incomparably more durable in effect and therefore more dangerous than, for instance, the dissemination of propaganda by leaflets or other printed media.

414. The United Kingdom case of *R. v. Roshanara Choudhry* provides an example of a self-taught individual, Ms. Choudhry, who was radicalized to commit a violent act exclusively through material accessed via the Internet and, in particular, by means of video-hosting websites. Ms. Choudhry's case drew international attention to the ease with which the video-sharing platform containing user-generated content enabled her to locate and view videos of extremist Islamic content, and the process by which her conviction to execute an act of terrorism was formed through consistently viewing such content over the course of several months.

415. In 2010, following discussions with the Governments of the United Kingdom, led by the law-enforcement-based Counter Terrorism Internet Referral Unit, and the United States, where the YouTube servers are located, YouTube's parent company, Google Inc., voluntarily introduced a system which enabled content viewers to flag potential terrorism-related content on the YouTube website. This mechanism represents an important tool in proactively identifying content which may promote acts of terrorism.

416. Some websites and social media platforms also include provisions in their terms of use that prohibit the use of their services to promote, inter alia, terrorist activities. For example, the terms of service of Twitter,[189] a real-time information network, prohibit the use of the service for publishing direct, specific threats of violence against others or for any unlawful purposes or in furtherance of illegal activities.[190] In the event of breach of such terms, the service provider reserves the right (although does not have an obligation) to remove or refuse to distribute the offending content or to discontinue service. Further, Twitter users are limited to those not barred from receiving services under the laws of the United States or other applicable jurisdiction, thus excluding the use of its services by designated terrorist organizations. Nevertheless, even when such terms are in place, difficulties may arise in enforcement, owing in part to the broad user base and resulting high volume of user-generated content to be monitored.

417. Recent news reports indicate that, in the case of copyright infringement, Google often acts to remove illegal content or links within six hours of receiving a request to do so, despite having been inundated with over five million requests related to such content in 2011.[191] The combination of a content-flagging mechanism and a similarly diligent and timely response to suspected terrorism-related content would be a very positive step forward in the fight against the use of the Internet for recruitment, radicalization, training and glorification of and incitement to acts of terrorism.

418. Content disseminated by terrorist organizations is often marked with trademarks known to be associated with particular organizations.[192] The monitoring and removal

[189] Available from https://twitter.com/tos.

[190] See http://support.twitter.com/articles/18311-the-twitter-rules#.

[191] Jenna Wortham, "A political coming of age for the tech industry", *The New York Times*, 17 January 2012. Available from www.nytimes.com/2012/01/18/technology/web-wide-protest-over-two-antipiracy-bills.html?hp.

[192] "Jihadist use of social media: how to prevent terrorism and preserve innovation", testimony of A. Aaron Weisburd, Director, Society for Internet Research, before the United States House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, 6 December 2011.

of such easily identifiable content by hosting websites could offer significant gains in countering the dissemination of unlawful terrorist propaganda. Further, the use of flagging mechanisms, similar to those introduced on YouTube, as a standard feature across other social networking media and Internet search engines may improve the likelihood of timely removal of propaganda intended to further terrorist purposes. Increased measures to identify terrorism-related content, combined with enhanced formal and informal information-sharing partnerships between State and private stakeholders, could significantly assist in identifying and countering terrorist activity involving use of the Internet.

419. Information-sharing is particularly important in the context of distinguishing online content that may be objectionable from that which may be illegal (see discussion in section I.B.1). For example, while the flagging system employed by YouTube may assist in prioritizing certain content for review, it must subsequently be determined whether such content meets the necessary threshold to be removed or blocked. Informal dialogue between ISPs or hosting websites on the one hand, and criminal justice officials on the other hand, may facilitate this process. To that end, relevant private sector stakeholders may be encouraged to cooperate with law enforcement authorities by reporting objectionable content suspected to be connected with any user affiliated with a known terrorist organization or promoting the activities of such an organization.

3. Internet search engines

420. Internet search engines provide a bridge between Internet content and the end user. Content excluded from such search engines has a significantly reduced audience. Some Internet search engines, such as Google and Yahoo, voluntarily censor content deemed to be sensitive or harmful to their interests. For example, following the 11 September 2001 attacks in the United States, many Internet search engines removed search results relating to potential terrorist organizations.[193] Policymakers and law enforcement officials in several member States have encouraged similar voluntary initiatives to reduce ease of access through Internet search engines to content which may promote violent acts. Voluntary implementation by search engines of a flagging system for terrorist-related content, similar to that used by YouTube, may also be beneficial.

4. Monitoring services

421. Some private actors have also taken a more structured approach to countering terrorist activity on the Internet. Monitoring services such as the United-States-based Search for International Terrorist Entities (SITE) and Internet Haganah monitor and collect open-source information related to terrorist organizations.[194] Search for International Terrorist Entities, which operates as an intelligence-gathering service, obtains significant revenues from fee-based subscriptions. As such, it and similar organizations may therefore have better access to resources to enable the prompt identification and

[193] Conway, "Terrorism and Internet governance: core issues", p. 30.

[194] Ibid, p. 31.

translation, where applicable, of Internet activities which may promote acts of terrorism. Internet Haganah, by contrast, monitors Internet-based activity by Islamist extremist groups with the aim of identifying and disrupting access to terrorist-related content. Internet Haganah is funded in part through donations and operated primarily based on the contributions of a network of volunteers. This monitoring service proactively researches and identifies Internet content deemed to be terrorist-related and the corresponding hosting website. This information may be shared with law enforcement authorities or the public or be used to contact the hosting website to promote the removal or disruption of access to such content.[195] While the purpose and operating models of these monitoring services differ, the actions of both promote the rapid identification of terrorist-related content on the Internet, which may be useful for intelligence, investigation and prosecution of such activity.

B. Public-private partnerships

422. There are many potential benefits from establishing public-private partnerships with interested stakeholders in countering the use of the Internet for terrorist purposes. Often-cited challenges to public-private cooperation in connection with cybercrime generally are the lack of communication between law enforcement and service providers regarding the efficient gathering of evidence, and the tension between privacy and the need for data retention for enforcement purposes. Creating a forum for formal and informal dialogue between counterparts from the public and private sectors could significantly allay such concerns. In addition to the opportunities provided through regular meetings among the partners involved, activities such as joint training programmes could also assist in breaking down communication barriers and further enhancing trust between participating partnership members.[196]

423. Significant progress has been made in establishing public-private partnerships in security-related matters associated with potential terrorist attacks on vulnerable targets or infrastructure, or relating to the prevention and prosecution of cybercrime generally. The establishment of similar public-private partnerships in connection with the regulation of the use of the Internet for terrorist purposes would be beneficial. An example of a successful security-related public-private partnership is the Overseas Security Advisory Council, established between the United States Department of State and American private sector organizations operating abroad. The Council provides a forum for the exchange of best practices and a platform for the regular and timely interchange of information between the private sector and the Government of the United States concerning developments in the overseas security environment, including in relation to terrorism, as well as political, economic and social factors that may have an impact on the security environment globally and on individual countries.[197]

[195] Ariana Eunjung Cha, "Watchdogs seek out the web's bad side", *Washington Post*, 25 April 2005. Available from www.washingtonpost.com/wp-dyn/content/article/2005/04/24/AR2005042401473.html.

[196] United Nations Interregional Crime and Justice Research Institute, "Public-private partnerships for the protection of vulnerable targets against terrorist attacks: review of activities and findings" (January 2009), para. 23.

[197] Ibid., para. 9.

424. The Indonesia Security Incident Response Team on Internet Infrastructure provides another example of a security-focused public-private partnership initiative. It brings together representatives from the postal and telecommunications services, the national police, the Attorney General's office, Bank Indonesia, the Indonesian Internet Service Providers Association, the Indonesian Internet Café Association, the Indonesian Credit Card Association and the Indonesian ICT Society (MASTEL). Members cooperate to, inter-alia, conduct monitoring, detection and early warning of threats and disruptions to Internet-protocol-based telecommunications networks; conduct research and development; provide simulation laboratories and training on the security of the use of Internet-protocol-based telecommunications networks; provide consultative services and technical assistance to strategic agencies or institutions; and serve as a coordination centre for relevant agencies or institutions, both domestic and international.[198]

425. In November 2006, the Global Forum for Partnerships between States and Businesses to Counter Terrorism was convened in Moscow. As a result of this forum, the Group of Eight[199] adopted the Strategy for Partnerships between States and Businesses to Counter Terrorism,[200] which promotes, inter alia, cooperation between Internet service providers and other businesses and Government authorities to counter the misuse of the Internet by terrorists and to prevent the facilitation of the final steps that lead from extremism to terrorism. Pursuant to this Strategy, Governments are encouraged to build closer voluntary national and international partnerships with Internet service providers to tackle the use of the Internet for activities such as recruitment, training and incitement to commit terrorist acts.

426. Other relevant public-private partnership initiatives include the Council of Europe working group established in 2007, with participants from law enforcement, industry and service provider associations, to address issues relating to cybercrime generally. The aim of this initiative is to enhance cooperation between law enforcement authorities and the private sector, with a view to tackling cybercrime more efficiently.

427. In 2010, the European Commission approved and provided funding for a project, involving collaboration between academia, industry and law enforcement, intended to create a network of Cybercrime Centres of Excellence for Training, Research and Education (2CENTRE) in Europe. That network currently provides training through national centres of excellence located in Ireland and France. Each national centre is founded on a partnership among representatives of law enforcement, industry and academia, which collaborate to develop relevant training programmes and tools for use in the fight against cybercrime (see section IV.G).

428. Public-private partnerships specifically targeting terrorist use of the Internet could also provide a means to promote clear guidelines regarding information-sharing between

[198] Written submission of expert from Indonesia.

[199] Unofficial forum of the heads of the following industrialized countries: Canada, France, Germany, Italy, Japan, Russian Federation, United Kingdom and United States.

[200] A/61/606-S/2006/936, annex.

the private and public sector, consistent with applicable data protection regulations. A good basis for information-sharing guidelines is provided by the Council of Europe "Guidelines for the cooperation between law enforcement and Internet service providers against cybercrime".[201] The focus of these guidelines is the establishment of relationships of mutual trust and cooperation between public and private sector stakeholders as a foundation for cooperation. The guidelines also emphasize the need to promote efficient and cost-effective cooperation procedures. Law enforcement authorities and Internet service providers are encouraged to engage in information exchange to strengthen their capacity to identify and combat cybercrime through regular meetings and the sharing of good practices and feedback. The guidelines also encourage the establishment of formal partnerships and written procedures as a basis for longer-term relationships, to ensure, inter alia, that appropriate protections are provided that the partnership will not infringe upon the legal rights of industry participants or the legal powers of law enforcement authorities.[202]

429. Recommended measures to be taken by law enforcement authorities pursuant to the guidelines include:

- Engaging in broad strategic cooperation with ISPs, including by conducting regular technical and legal training seminars, as well as providing feedback on investigations conducted or intelligence gathered, based on ISP-initiated reports/complaints
- Providing explanations and assistance to ISPs regarding investigation techniques not directly related to the case at hand, in order to facilitate an understanding of how ISP cooperation will result in more efficient investigations
- Prioritizing requests for large volumes of data while avoiding unnecessary cost and disruption of business operations.[203]

430. Recommended measures to be taken by Internet Service providers pursuant to the guidelines include:

- Cooperating to minimize the use of services for illegal purposes
- Reporting criminal activity to law enforcement authorities
- When possible, providing a list, upon request, of which types of data could be made available for each service to law enforcement, upon receipt of a valid disclosure request.[204]

431. Public-private partnerships may also provide a forum to promote minimum standards for the secure retention of data by private sector stakeholders and enhance the channels of communication for the provision of information by private sector stakeholders regarding suspicious activities.

[201] Council of Europe, Economic Crime Division, "Guidelines for the cooperation between law enforcement and Internet service providers against cybercrime" (Strasbourg, 2 April 2008). Available from www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf.

[202] Ibid., paras. 10-13.

[203] Ibid., paras. 17, 29, 30 and 33.

[204] Ibid., paras. 41, 42 and 50.

VIII. Conclusion

A. Use of the Internet for terrorist purposes

432. The introductory chapters of the present document provided an overview, developed along functional lines, of the means by which the Internet is often utilized to promote and support acts of terrorism, in particular with respect to propaganda (including for the purposes of recruitment, radicalization and incitement to terrorism), training and financing, planning and executing such acts. Emphasis is also placed on the opportunities offered by the Internet to prevent, detect and deter acts of terrorism. These may include the gathering of intelligence and other activities to prevent and counter acts of terrorism, as well as the gathering of evidence for the prosecution of such acts.

433. Counter-narratives and other strategic communications may be an effective means of disrupting the process of radicalization to extremist ideals, which may in turn be manifested through acts of terrorism. A demonstrated understanding of the broader issues underpinning radicalization is also important in engaging in constructive dialogue with potential recruits to a terrorist cause, and in promoting alternative, lawful means to pursue legitimate political, social or religious aspirations.

434. Respect for human rights and the rule of law is an integral part of the fight against terrorism. In particular, Member States reaffirmed those obligations in the United Nations Global Counter-Terrorism Strategy, recognizing that "effective counter-terrorism measures and the protection of human rights are not conflicting goals, but complementary and mutually reinforcing". The effective implementation of a rule-of-law approach to countering the use of the Internet for terrorist purposes must be continually assessed during all stages of counter-terrorism initiatives, from preventive intelligence-gathering to ensuring due process in the prosecution of suspects.

B. The international context

435. There is currently no comprehensive United Nations treaty on terrorism, nor is there an official definition of the term "terrorism". Nevertheless, the Member States of the United Nations are in the process of drafting a comprehensive convention on international terrorism, which will complement the existing international legal framework related to counter-terrorism. This framework is contained in a range of sources, including resolutions of the General Assembly and Security Council, treaties, jurisprudence and customary international law. Several regional and subregional instruments also offer valuable substantive and procedural standards for criminalizing acts of terrorism which may be perpetrated by means of the Internet.

436. Member States have resolved, pursuant to the Global Counter-Terrorism Strategy, to take urgent action to prevent and combat terrorism in all its forms and manifestations and, in particular:

(a) To consider becoming parties without delay to the existing international conventions and protocols against terrorism, and implementing them, and to make every effort to reach an agreement on and conclude a comprehensive convention on international terrorism;

(b) To implement all General Assembly resolutions on measures to eliminate international terrorism, and relevant General Assembly resolutions on the protection of human rights and fundamental freedoms while countering terrorism;

(c) To implement all Security Council resolutions related to international terrorism and to cooperate fully with the counter-terrorism subsidiary bodies of the Security Council in the fulfilment of their tasks.

C. Policy and legislative frameworks

1. Policy

437. Effective criminal justice responses to threats presented by the use of the Internet by terrorists require Governments to develop clear national policies and laws dealing with, inter alia: *(a)* the criminalization of unlawful acts carried out by terrorists over the Internet or related services; *(b)* the provision of investigative powers for law enforcement agencies engaged in terrorism-related investigations; *(c)* the regulation of Internet-related services (e.g. ISPs) and content control; *(d)* the facilitation of international cooperation; *(e)* the development of specialized judicial or evidential procedures; and *(f)* the maintenance of international human rights standards.

438. The broad classification of strategic approaches provided by the Counter Terrorism Implementation Task Force's Working Group on Countering the Use of Internet for Terrorist Purposes, involving the use of general cybercrime legislation, general (non-Internet-specific) counter-terrorism legislation and Internet-specific counter-terrorism legislation, provides a useful conceptual framework for policymakers and legislators. Currently, few States have developed legislation specifically targeting acts carried out by terrorists over the Internet. Most countries use general criminal laws, cybercrime, and/or counter-terrorism legislation to criminalize and prosecute these types of crimes.

2. Legislation

439. In addition to using the Internet as part of actions in carrying out substantive crimes (e.g. bombings), terrorists can use the Internet to carry out other support activities (e.g. disseminating propaganda or recruiting and training members). Countries have used different approaches to criminalizing unlawful conduct associated with terrorism carried out by using the Internet.

440. In its resolution 1624 (2005), the Security Council, inter alia, called upon States to criminalize the incitement of terrorist acts. States are obliged, under the resolution and other international instruments, to ensure that measures targeting acts inciting terrorism fully conform with their international obligations under human rights law, refugee law and humanitarian law.

441. The development and enforcement of laws criminalizing the incitement of acts of terrorism while fully protecting human rights (e.g. the right to freedom of expression) presents an ongoing challenge for policymakers, legislators, law enforcement agencies and prosecutors in all countries. Countries have adopted different approaches in criminalizing acts of incitement of terrorism. Some countries have specifically criminalized acts of incitement or glorification of terrorist acts, while others rely upon on inchoate offences such as solicitation or conspiracy.

442. The investigation of terrorism cases involving the use of the Internet or other related services by suspected terrorists often necessitates the use of specialized types of investigative powers by law enforcement agencies. Most Governments have adopted legislation that permits law enforcement agencies to undertake such activities in terrorism-related investigations. These investigative techniques should be properly authorized under national laws and carried out in a manner that upholds fundamental human rights protected under international human rights law.

443. Authorities will require the cooperation of telecommunications operators when undertaking electronic monitoring, wiretaps and similar electronic investigative technique. It is desirable that Governments provide a clear legal basis for the obligations on private sector parties, including the technical specifications required of their networks and how the cost of providing such capabilities is to be met.

444. There is evidence that terrorists have used Internet cafes to carry out their activities; however, the extent to which this is a problem is unknown. Some Governments have imposed specific duties on operators of Internet cafes for law enforcement purposes (including anti-terrorism) to obtain, retain and, upon request, produce to law enforcement agencies photo identification, addresses and usage/connection data of customers. There is some doubt about the utility of targeting such measures at Internet cafes only when other forms of public Internet access (e.g. airports, libraries and public Wi-Fi hotspots) offer criminals (including terrorists) the same access opportunities and are unregulated.

445. The issue of the extent to which Governments should regulate terrorism-related content on the Internet is problematic, requiring the balancing of law enforcement and human rights considerations (e.g. the right to freedom of expression). Approaches to regulation of terrorism-related content vary, with some States applying strict regulatory controls on ISPs and other related service providers, including in some cases the use of technology to filter or block access to some content. Other States adopt a lighter regulatory approach, relying to a greater extent on self-regulation by the information society sector. Most ISPs, web hosting companies, file-sharing sites and social networking sites have terms-of-service agreements that prohibit certain content; some terrorism-related content might contravene these contractual restrictions.

D. Investigations and intelligence-gathering

446. Effective investigations relating to Internet activity rely on a combination of traditional investigative methods, knowledge of the tools available to conduct illicit activity via the Internet and the development of practices targeted to identify, apprehend and prosecute the perpetrators of such acts. A proactive approach to investigative strategies and supporting specialist tools that capitalize on evolving Internet resources promotes the efficient identification of data and services likely to yield the maximum benefit to an investigation.

447. There is a range of specialized utilities and hardware available to investigators with the appropriate technical background. Due care should be taken, where possible, in cases involving the acquisition of digital evidence to implement standardized data recovery procedures to promote the retrieval of the maximum available evidence and the preservation of the integrity of the data source and the chain of custody to ensure its admissibility in court proceedings. Owing to the fragile nature of digital evidence, its assessment, acquisition and examination is most effectively performed by specially trained forensic experts.

E. International cooperation

448. Effective international cooperation is an important factor in many terrorism-related prosecutions, including those involving some aspect of Internet use by perpetrators. States are obliged, under many different international, regional, multilateral and bilateral instruments related to terrorism and transnational organized crime, to establish policies and legislative frameworks to facilitate effective international cooperation in the investigation and prosecution of acts of terrorism or related serious organized crime. Currently, there is no universal instrument related to cybercrime or terrorism imposing specific obligations on States in relation to international cooperation. This is an impediment to effective international cooperation in some terrorism-related investigations and prosecutions.

449. While formal channels of international cooperation remain vital, in practice informal channels are becoming equally as important. Regardless of the mode of cooperation, trust between respective national authorities is a key element in effective international cooperation in many cases. In addition to cooperation under formal treaties or similar legal instruments, regional or subregional non-treaty-based initiatives aimed at strengthening law enforcement cooperation are also important. Countries with common security interests in thematic areas might enter into collective arrangements that provide for information exchange and intelligence sharing.

450. The existence of a national legislative framework providing for effective international cooperation is a fundamental element of an effective framework for the facilitation of international cooperation in the investigation and prosecution of terrorism cases. Such legislation should incorporate into a country's domestic law the principles espoused in the universal instruments against terrorism relating to cooperation and relevant transnational organized crime.

451. While legislation is a fundamental component of any effective regime for international cooperation, it is not in and of itself the entire answer. The existence of a properly resourced and proactive central authority which can facilitate mutual legal assistance, using all available channels, is also key. The development and maintenance of relationships of trust and confidence with foreign counterparts involved in cooperation in cross-border criminal investigations is also important.

452. In addition to formal channels for cooperation, authorities need to develop and utilize available informal channels for bilateral cooperation. Many national law enforcement agencies operate a network of international liaison posts, which assist greatly with the facilitation of international cooperation requests. There is no express reference to the use of joint investigation teams in the universal counter-terrorism instruments; however, this cooperation strategy is entirely consistent with the underlying principles and spirit of the international cooperation elements of these instruments. Some countries, notably in Europe, have successfully adopted this approach to a number of terrorism-related investigations.

453. Despite improvements, formal mutual legal assistance procedures in criminal cases can still be lengthy processes, involving considerable amounts of bureaucracy. In cases involving the preservation of Internet-related data held by ISPs in another jurisdiction, it might be possible for authorities to cooperate with ISPs directly on an informal basis to preserve such data for the purpose of the investigation or prosecution of a criminal offence. In other situations, the exercise of a coercive power and judicial authorization may be required, for example, with regard to the preservation, search and seizure of Internet-related data for production and use as evidence in criminal proceedings.

454. Investigators and prosecutors should be fully cognizant of the potential importance of such data and the need to take steps at the earliest possible moment to preserve it in a manner that ensures its admissibility as potential evidence in any later proceedings. To the extent possible, national law enforcement agencies should develop, either directly with ISPs or with their counterpart agencies in other countries, clear procedures, involving both formal and informal elements, aimed at ensuring the earliest possible retention and production of Internet-usage data required for a criminal investigation.

455. Some experts at the expert group meeting highlighted the fact that the need, on the part of national authorities, to protect sensitive intelligence material often presents an obstacle to information-sharing.

456. When considering investigative actions in other jurisdictions involving the collection of digital evidence, authorities should be mindful of the sovereignty implications that such actions might have for other States. Whenever possible, authorities considering investigative steps relating to persons or objects located in another jurisdiction should notify and coordinate such actions with their foreign counterparts in relevant countries.

457. Internet-related data (e.g. customer usage) will be important evidence in many terrorism cases. In such cases, authorities should ensure that relevant data is preserved for later evidential use in proceedings. In this regard, it is important to note

the distinction between "retention" of data (data retained by ISPs under a regulatory obligation) and "preservation" of data (data that has been preserved on the basis of a judicial order or authority). In many countries, ISPs are obliged by law to retain certain types of communications-related data for a specified time period. Nevertheless, despite some efforts (for example, at the regional level in Europe), there is no international agreement on the type of data that should be retained by ISPs or the retention period. As a result, internationally there is a wide variation in the specific type of data retained by ISPs and the time period for which it is kept. This can be problematic in cases in which authorities require communications-related data located in one country as evidence in criminal proceedings being held in another country.

458. The development of a universally agreed regulatory framework imposing consistent obligations on all ISPs regarding the type and duration of customer usage data to be retained would be of considerable benefit to law enforcement and intelligence agencies investigating terrorism cases. In the absence of a universally agreed framework for data retention by ISPs, authorities should identify, at the earliest possible stage, whether ISP data relevant to an investigation exists and where it is located, and initiate steps at the earliest possible time to preserve it for possible use as evidence.

459. To the extent possible, authorities should establish informal relationships or understandings with ISPs (both domestic and foreign) that might hold data relevant for law enforcement purposes about procedures for making such data available for law enforcement investigations. In the absence of such informal procedures, during investigations authorities should liaise at the earliest possible opportunity with foreign counterparts, if necessary through formal channels and appropriate judicial authorizations, regarding the preservation of such data.

460. From an evidential perspective, terrorism cases involving cross-border investigations add an additional layer to what might already be a complex task for investigators and prosecutors, requiring them to ensure that the methods used to collect evidence (potentially in one or more countries) and to produce it as evidence in a prosecution conducted in another jurisdiction are in full accordance with the applicable laws and principles of all relevant jurisdictions.

461. The dual criminality requirement (that the acts to which extradition and mutual legal assistance relate constitute crimes in both States), commonly found in many multilateral and bilateral instruments relating to terrorism and transnational organized crime, can present difficulties in criminal cases, including those relating to terrorism, that involve some element of international cooperation.

462. Terrorism cases in which constituent acts forming part of a crime are carried out over the Internet can raise complex jurisdictional issues, particularly in cases in which a suspected offender is located in one country and uses Internet sites or services hosted by ISPs in another to carry out constituent acts of a crime. Such cases have involved persons resident in one country setting up and administering websites used to promote jihad and other violent acts related to terrorism.

463. There are no binding rules under international law that deal with the issue of how States should handle cases in which more than one State might assert jurisdiction to prosecute a crime involving the same suspect. Typically, national authorities balance or weigh relevant factors, including the degree of connectivity between various jurisdictions and the alleged crime, in determining whether to assert and exercise jurisdiction in the particular case. In cases involving competing jurisdictional claims, early and collaborative communication between relevant central authorities (often national prosecuting agencies) is important in resolving such issues.

464. National data protection or privacy legislation can often restrict the ability of law enforcement and intelligence agencies to share information with both national and foreign counterparts. Striking a sensible balance between the human right to privacy and the legitimate interest of the State to effectively investigate and prosecute crime is an ongoing challenge for Governments and, in some cases, including those which involve responses to terrorism, has been the subject of concern.

F. Prosecutions

465. An integral part of the universal legal framework against terrorism, the United Nations Global Counter-Terrorism Strategy is the obligation imposed on States to deny safe haven and bring to justice perpetrators of terrorist acts, wherever they might occur. In addition to the existence of the necessary legislative framework, institutional capacity within national prosecution agencies to uphold the rule of law when prosecuting terrorism-related cases, in accordance with the human rights of suspects and accused persons under international human rights law, is an integral part of an effective criminal justice response to terrorism.

466. Often, prosecutors are not merely involved in the prosecution phase of terrorism cases but also play a direct role in the investigative phase, providing legal and strategic advice on issues that will influence the outcome of any resulting prosecution. They are likely to undertake their role as part of a multidisciplinary/multijurisdictional team. The high level of trust, coordination and communication vital to effective cooperation at the international level also needs to exist between national law enforcement, intelligence and prosecuting agencies.

467. While new investigative techniques offer authorities enhanced opportunities to target terrorist activities on the Internet, they also carry legal risks to which prosecutors need to remain vigilant. Differences in national laws related to the collection and admission of evidence mean these risks are higher when actions from which evidence has been derived occur in a different jurisdiction from that in which the trial will be conducted.

468. In most countries, prosecutors exercise wide discretion with regard to whether to institute criminal proceedings and the charges with which to do so. These decisions are often taken in accordance with guidelines or codes which are designed to ensure the fair, transparent and consistent exercise of this important discretion, and which often apply thresholds based on evidential sufficiency and public interest.

469. The primary objective of terrorism-related investigations is public safety. In some cases, authorities need to intervene to prevent the commission of terrorist acts before there is sufficient evidence available to initiate a prosecution for the terrorist acts that authorities suspect are being planned.

470. In these situations, authorities might need to rely upon other criminal offences to provide the legal basis for their actions, including offences such as solicitation, conspiracy, criminal association or providing material support to terrorists, rather than substantive crimes related to terrorist acts being planned. Other general penal provisions related to fraud or the possession or use of unlawful articles (e.g. false identity/travel documents, weapons) can be used to disrupt or compromise the activities of terrorist groups before their planned attacks or activities are carried out.

471. In many terrorism cases, evidence used by the prosecution is based on intelligence. The integration of intelligence activities into criminal justice systems remains a fundamental problem for authorities in dealing with terrorism, i.e. how can authorities protect sensitive intelligence underlying evidence while meeting obligations to ensure a fair trial and effective defence for accused persons, including the obligation to disclose all material parts of the prosecution case to the defence?

472. In terrorism cases involving the use of computers or the Internet, digital evidence will be an important part of the prosecution case. The use of such evidence invariably gives rise to issues related to admissibility. It is critical that great care be taken throughout the investigation and prosecution of the case to ensure that the methods used for the collection, preservation, analysis and production of digital evidence are in full conformity with the relevant rules of evidence or procedure and follow established good practice

473. Prosecuting authorities will need to satisfy a court of the reliability of digital evidence, including its methods of collection, analysis and production. The procedures for preserving the integrity of evidence is known as the "chain of custody" or "chain of evidence". When such evidence is collected in one jurisdiction for use at trial in another, the situation is considerably more complicated and requires careful attention by investigators and prosecutors. In cases in which authorities identify the existence and/or location of relevant digital evidence, they should explore means (informal and formal) of obtaining and preserving it for evidential purposes. The channel chosen should ensure the admissibility of the evidence in the country where the trial will take place.

474. Legal principles and procedures related to the collection and admissibility of evidence in criminal proceedings often differ between jurisdictions. A significant part of the work of authorities in cross-border investigations involves "mediating" different aspects of evidence. This can be a complex, time-consuming process but is a critical factor in the success of prosecutions. Any legal deficiencies in the methods by which evidence ultimately used at trial is collected, preserved, transmitted or produced will almost certainly be challenged by the defence.

475. In terrorism cases, it will often be necessary for prosecutors to present expert evidence to prove some specialized aspect(s). Areas in which expert testimony is often required include the technology and communications fields and the ideologies, activities and organizational structure of terrorist groups. It is quite possible that prosecutors might require several expert witnesses. Typically, cases involving the use of expert witnesses involve three steps or phases: *(a)* clear identification of the issues (and their scope) that require an expert opinion; *(b)* identification of a qualified expert; and *(c)* ensuring that the qualified expert uses admissible means.

476. Prosecutors should at the earliest possible opportunity identify the issues on which expert evidence is likely to be required and engage experts to undertake the necessary analysis, if necessary, providing clear guidance on the key rules of procedure or evidence. When selecting expert witnesses, prosecutors need to consider whether governmental or non-governmental experts should be used. While there are benefits to using governmental witnesses, using non-governmental experts might be desirable in cases in which sensitive intelligence sources or methods have been used as the basis for their evidence. Identifying a suitable expert, particularly in highly specialized fields, can pose a significant challenge for less-developed jurisdictions. Wherever applicable, expert witnesses should follow and apply recognized good practice in the particular field with respect to which they are being called. Owing to the complexity of some expert testimony, consideration should be given to innovative ways of presenting complex evidence to judges, juries or other fact-finders at trial in an easily understood way. It is important that the prosecutor has a sound working knowledge of the particular subject area.

477. The complexity of many terrorism-related prosecutions, particularly those involving international cooperation or highly technical elements, make it highly desirable that a team of prosecutors conduct cases. In order to ensure an integrated rule-of-law approach and to preserve the integrity of criminal justice responses to terrorism, countries need to have robust and ongoing processes to strengthen the capacity of prosecutors to implement national counter-terrorism legislation and related international cooperation obligations. In countries where the risk of terrorist activity is high and institutional capacity within prosecution services and other criminal justice agencies is low, a high priority should be placed on developing specialist capacity within these agencies, not only in terms of prosecuting cases but also with respect to related international cooperation mechanisms.

G. Private sector cooperation

478. While the responsibility for countering the use of the Internet for terrorist purposes ultimately lies with Member States, the cooperation of key private sector stakeholders is crucial to effective execution. Proactive engagement with private sector stakeholders such as service providers, websites hosting user-generated content and Internet search engines will continue to play an important role in controlling the availability of terrorism-related content disseminated via the Internet.

479. The establishment of public-private partnerships in connection with the regulation of the use of the Internet for terrorist purposes would be beneficial. Similar initiatives have been successfully developed with respect to other areas of counter-terrorism, and to combat cybercrime generally. These initiatives provide a forum for formal and informal dialogue between counterparts from the public and private sectors, and also support activities such as joint training programmes which may assist in breaking down communication barriers and further enhancing trust, understanding and the development of harmonized practices between participating partnership members.

UNODC

United Nations Office on Drugs and Crime

Vienna International Centre, PO Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

United Nations publication
Printed in Austria

V.12-52159—September 2012—350