CTC Special Meeting on Communications and IT  
New York  
May 2013

Ms Marta Requena  
Chief, Terrorism Prevention Branch  
United Nations Office on Drugs and Crime

Excellencies,  
Distinguished Delegates,  
Ladies and Gentleman,

Thank you very much. I am very pleased to be here to participate in this special event of the Counter Terrorism Committee on countering terrorism through the use of new communications and information technologies. The Terrorism Prevention Branch of the United Nations Office on Drugs and Crime has been very active in developing tools to help prevent and combat the use of the internet for terrorist purposes and I look forward to sharing some of our efforts in this area today.

We all know that the use of the Internet continues to grow. Currently more than 1/10 of the global population holds a mobile broadband subscription. The internet allows individuals to communicate quickly across borders to an almost unlimited audience at low cost and with relative anonymity. Unfortunately this is also what allows the internet to be so effectively exploited by terrorists.
Given that terrorist use of the internet defies national borders, it is particularly appropriate to offer a coordinated international response to combat this threat. As you know, the Global Counter-Terrorism Strategy of 2006 explicitly references the role that the United Nations can play in helping to counter the use of the Internet as a tool for the spread of terrorism.

And in more recently in December 2011, the General Assembly adopted resolution 66/178, reaffirming UNODC’s mandate and requesting it “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, where appropriate, [...] the use of the Internet for terrorist purposes”.

With this additional guidance from the General Assembly and given the lack of legal resources on this topic, the Terrorism Prevention Branch of UNODC developed a technical assistance tool on The Use of the Internet for Terrorist Purposes. We did this in cooperation with CTITF and in the framework of its Working Group on Countering the Use of the Internet for Terrorist Purposes and with the generous support of the United Kingdom.

The new technical assistance tool is unique in that it is the first of its
kind to provide Member States with actual judicial cases where the internet was the key tool for the commission of the terrorist act. Therefore, it is not only a report but also a practical guide providing concrete examples and guidance for policy makers, investigators, and prosecutors to help them deal with the specialized nature of these cases.

We created the publication with the input of two meetings of international experts from 25 countries, numerous international organizations, and the private sector which allowed us to draw on the collective experiences of Member States, specialized institutions and individual experts representing different geographic regions and legal approaches. It was truly a collaborative effort and we are very grateful for the input of all of the experts.

However, I should note that the publication does not cover all uses of the internet for terrorist purposes. We chose to specifically exclude the issues of cyber-security and ‘cyber-attacks’, from the scope of the tool. Instead, the publication focuses on the legal issues surrounding cases where terrorists use the internet as a tool rather than as the means of attack. Practical legal assistance in this area has been limited and terrorist use of the internet in this way constitutes a very serious threat.
The publication discusses terrorist use of the internet for:

1) Glorification and public provocation to commit a terrorist act
2) incitement
3) recruitment
4) radicalization
5) financing,
6) training,
7) planning and
8) the commission of terrorist acts.

For each of these categories, the publication provides practical guidance and detailed examples of ways to effectively criminalize, investigate, and prosecute cases involving those types of internet-based terrorist activities.

In addition, the publication offers a number of specific conclusions and recommendations. I will highlight a few of the key conclusions:

1. While the benefits of the internet for modern society are numerous, this same technology which facilitates such communication can also be exploited by terrorists. However, the use of the internet by terrorist organizations also presents unique opportunities to prevent, detect and deter acts of
terrorism, by allowing intelligence gathering, the collection of evidence for prosecution, and the use of counter-narratives.

2. The need for legislation that criminalizes various aspects of the use of the internet for terrorist purposes, which of course is particularly important to UNODC given our mandate.

3. The importance for investigators and prosecutors of utilizing trained personnel and specialized techniques in the collection of data and the challenges of using sensitive intelligence in a criminal prosecution.

4. The need of international cooperation in this area and the difficulties of dealing with extradition and mutual legal assistance requests across legal systems and varying criminal codes.

5. Potential areas of cooperation between member states and the private sector

Given the focus of this special meeting, please allow me to elaborate further on a few of these points, highlighting some of the unique technological challenges and opportunities faced by criminal justice officials when investigating and prosecuting cases involving the use of the internet. As we detail in our handbook, the famous case of Malika el Aroud and others highlights many of the challenges surrounding prosecuting cases of this kind. El Aroud and her husband were both actively involved in the dissemination of extremist propaganda and the
recruitment, organization, and funding of a group of young men to take part in terrorist activities.

This case highlights several of the challenges that criminal justice officials face.

1. **Use of servers and cloud technology where the data is stored in other jurisdictions.** In the el Aroud case, the website which was used for promoting violent extremism and supporting terrorist activities was administered by al Aroud in one country but the website was hosted in another. This is a very common occurrence and presents challenges in coordinating the recovery of potential evidence across jurisdictions. Along these same lines, the increased use of cloud technology to remotely store information means that little data is stored on the individual's device but is instead offsite, often in another jurisdiction, which is another complication that investigators are increasingly facing when working to recover potential evidence in a terrorism case.

2. **The use of chat rooms and data encryption.** In the el Aroud case, members using the websites established by El Aroud were given a login and pseudonym and an electronic address so that they could exchange private messages, which were sometimes encrypted in closed chat rooms which would contain instructions, intelligence, and propaganda. Online messenger sessions are often not recorded by the service provider and therefore may not be available for retrieval after the
online session is terminated. (Although, computer forensic experts may be able to recover chat sessions from the hard drive of the perpetrator.) In addition, breaking encryption and layers of data protection requires specialized expertise that not all criminal justice official possess.

3. **The increased use of voice-over-protocols.** Malika el Aroud used Skype and email to remain in contact with her husband and six recruits. Communication using Skype and other voice-over-internet protocols does not leave all of the geolocational information provided by traditional calls. In addition, invoices are based upon total data usage, not per call like traditional land-lines and mobile phones. All of this can also limit investigators access to critical information on the time and location of each call.

4. **The increased use of email** including the use of saved but unsent emails as a means to avoid detection.

In addition, careful consideration needs to be given to the methods used in the collection and transmission of digital evidence during the investigation phase. For example, in the el Aroud case, in December 2009, after a lengthy and complex investigation coordinated between intelligence, law enforcement, and prosecution authorities in numerous countries and a number of persons with suspected links to Al-Qaida terrorist organizations were arrested with a range of criminal charges
including: the glorification of a terrorist group, the financing of terrorism, propaganda/incitement.

However, during the trial, the prosecution produced internet data related to postings and chat room discussions as evidence. The e-mails were sent from accounts held on servers on another country. Following an informal request for assistance, authorities from the country prosecuting the case were provided with data on the e-mail accounts within two weeks of their request.

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 that the informal procedures used did not follow the usual methods for international exchange of judicial information, thereby contravening national law.

The Court rejected this argument, for several reasons including that the procedure used was justified by the emergency nature of the situation because a suicide note had been posted on one of the websites raising fears that an attack was eminent but, nevertheless, this clearly shows the importance of careful planning in the collection of evidence, particularly across jurisdictions.
Finally, in May 2010, eight defendants including Malika el Aroud and her husband Moez Garsalloui were convicted of various charges related to participation in a terrorist group. The sentences varied from 40 months to eight years in the case of el Aroud and her husband.

Of course this is just a few examples of the challenges facing investigators and prosecutors in cases involving the use of the internet for terrorist purposes. As terrorists use the internet in new ways, criminal justice officials will have to continue to adjust with new investigative techniques and new specialized technology. The Terrorism Prevention Branch is working to assist national criminal justice practitioners to address these challenges. The Branch is currently providing highly specialized capacity building training to prosecutors and judges and is currently piloting a training program for investigators which will address many of specialized techniques and technologies that are needed to combat the use of the internet for terrorist purposes.

Thank you very much for allowing me to share some of the work that UNODC is doing in this important area. The Terrorism Prevention stands ready to assist Member States, as requested, in developing the specialized skills needed to prevent and combat terrorist use of the internet.