CTED
Counter-Terrorism Committee
Executive Directorate

Bringing Terrorists to Justice

Challenges in the Prosecution of Terrorists Acting Alone or in Small Cells

I. Introduction

1. Security Council resolution 1963 (2010) notes that the terrorist threat has become "more diffuse" and reaffirms that Member States must bring terrorists to justice in accordance with Security Council resolution 1373 (2001). A strong criminal justice system, including a robust, proactive prosecution service, is an essential part of this process. However, the Counter-Terrorism Committee's visits to Member States have shown that bringing terrorists to justice often poses major challenges. As the complexity of terrorism cases continues to evolve, investigative, prosecutorial and judicial authorities must continue to develop new and more effective judicial responses.

2. In order to help Member States address this challenge, the Counter-Terrorism Committee Executive Directorate (CTED), acting on behalf of the Committee, has been engaged in facilitating a series of seminars for prominent national counter-terrorism prosecutors on the theme, "Bringing Terrorists to Justice". The initial seminar, held at United Nations Headquarters, New York, in December 2010, was followed by seminars in Ankara, (July 2011), Algiers, (June 2012) and Dar es Salaam (February 2013).

3. Each follow-up seminar has addressed one of the major themes identified at the initial event. In Ankara, participants focused on the use of intelligence and information obtained through special investigative techniques as evidence in terrorism cases. The Algiers seminar focused on the strategic and operational roles of the prosecutor in preventing terrorism. In Dar es Salaam, seminar participants addressed the policy considerations and implications of prosecuting terrorist acts.

4. CTED has also developed a number of spin-off projects, based on the experiences shared and lessons learned during the above events. In May 2013, in Kampala, CTED launched a series of five workshops for law enforcement officers and prosecutors of East African Member States, with the support of Australia and New Zealand. The series aims to strengthen the capacities of prosecutors and police officers of Burundi, Kenya, Rwanda, Tanzania and Uganda to investigate and prosecute terrorism cases at the national and regional levels. CTED is also working with the Terrorism Prevention Branch of the United Nations Office on Drugs and Crime (UNODC/TPB) to help States conduct effective counter-terrorism investigations and prosecutions while ensuring respect for human rights and the rule of law. This initiative was launched in Geneva, in October 2013, with the support of Switzerland.

5. CTED and UNODC/TPB are also developing long-term regional programmes in the Maghreb (with the support of the European Union) and in South Asia (with the support of the United States of America). Both programmes will include country-specific activities and subregional workshops aimed at strengthening States' criminal justice responses to terrorism within a rule of law framework and ensuring compliance with the relevant counter-terrorism instruments, human rights standards and Security Council resolutions. In November 2013, CTED and UNODC/TPB, with the support of the European Union, launched a long-term programme to support the security and justice authorities of Nigeria.

II. Seminar on Challenges in the Prosecution of Terrorists Acting Alone or in Small Cells

A. Introduction

6. The fifth seminar was held in Tunis from 10 to 12 December 2013. In accordance with Security Council resolution 1963 (2010), which "directs CTED to identify emerging issues, trends and developments related to resolutions 1373 (2001) and 1624 (2005), while taking into account the United Nations Global Counter-Terrorism Strategy, as appropriate, at all levels, in consultation with relevant partners, and to advise the CTC on practical ways for Member States to implement resolutions 1373 (2001) and 1624 (2005)", the seminar focused on "Challenges in the Prosecution of Terrorists Acting Alone or in Small Cells", a topic addressed in Algiers and Dar es Salaam.

7. Terrorism is a unique and evolving crime. The prosecution of terrorism is recognized as a key component of a State's overall approach to effective prevention and suppression. Terrorism cases, nevertheless, pose particular challenges to prosecutors, with respect in particular to the collection of admissible evidence and the successful prosecution of relevant preparatory offences. The fifth seminar was attended by around 40 prominent national counter-terrorism prosecutors, senior Government officials, and representatives of international and regional organizations and civil society.[1] The participating States represented various world regions, development levels and legal systems. The discussions were held in accordance with the Chatham House Rule.

8. The opening statements were delivered by Mr. Adelkader Bahloul, Prosecutor-General of the Court of Appeals of Tunis, and Ms. Samia Ladgham, Acting Chief of Africa Cluster, CTED. Both speakers highlighted the timeliness of the event, the complex and changing nature of terrorism (including in Tunisia), and the invaluable contributions made by the participants in previous seminars towards identifying good counter-terrorism practices. Mr. David Scharia, Coordinator of the CTED Legal and Criminal Justice Working Group, described the context and aims of the practitioners' series, highlighting the main challenges and priorities identified thus far.

9. The three-day seminar consisted of several panel discussions, each of which addressed a specific aspect of the central theme *(agenda attached as annex)*. The seminar thus enabled participants to discuss the current threats, risks and challenges posed by the phenomenon of terrorists acting alone or in small cells, with reference in particular to (i) the current scope and nature of the challenge; (ii) operational commonalities and the modus operandi of the lone actor; (iii) current approaches and legal provisions, including critical gaps and challenges in the prosecution of terrorists acting alone; and (iv) human rights considerations. The summary below is a reflection of participants' comments. In accordance with the Chatham House Rule, no comment is specifically attributed to any one individual or Government.

[1] African Centre for Studies and Research on Terrorism (ACSRT), African Prosecutors' Association, Bundeskriminalamt (German Federal Police), Canadian Security Intelligence Service, Europol, La Trobe University, Office of the High Commissioner for Human Rights (OHCHR), Terrorism Prevention Branch of the United Nations Office on Drugs and Crime (UNODC/TPB).

B. Summary of discussions

1. The current scope and nature of the challenge

10. The threat posed by "terrorists acting alone or in small cells" is a global one. However, it is not yet well documented, and difficult to define. The terms *terrorist acting alone*, *lone actor* and *lone wolf* are used interchangeably in the present document to refer to an individual who perpetrates political violence, acting independently, with no clear connection to the leadership of a terrorist group and/or outside an organizational hierarchy. This definition might equally refer to individuals acting in a small group. Participants cited the modus operandi of the Irish Republican Army (IRA), the Basque *Euskadi Ta Askatasuna* (ETA) and the German National Socialist Underground (NSU) as examples of the division of a large organization into "small groups", which poses similar challenges.

11. Clearly, this is not a new phenomenon. In recent history, it may be said to have emerged with the anarchist movements of the 1970s. However, participants agreed that, as with terrorism in general, the strategy or tactic of lone wolf terrorism could not be associated with a single philosophy, motivation, religion, ethnicity or race. Although it appeared to manifest itself more commonly in Western States (and in the United States of America, in particular), it was driven by beliefs and ideologies that were found in all regions of the world and increasingly disseminated across national borders through modern communications technologies, particularly the Internet.

12. This global phenomenon brought individuals into contact with distant conflicts, groups and ideologies, and terrorist organizations took advantage of Internet communities and chat forums to air their grievances and spread their messages. Terrorist organizations perceived the lack of operational ties as a strength, rather than a weakness, because it enabled them to protect their core operations while encouraging multiple individual operators, motivated by a common cause, to act on their behalf. Al-Qaida's Anwar al-Awlaki, for example, had appealed to followers to "think globally, but act locally", and several high-profile public appeals by Al-Qaida and other religiously-inspired terrorist groups, had issued similar appeals. On-line magazines such as "Inspire" had not only encouraged operationally independent action, but even shown how individuals could equip and train themselves.

13. The rapid pace of technological progress facilitated global communication, travel and access to information. This provided fertile ground for the recruitment of lone actors across vast distances and the dissemination of, and identification with global causes. These factors also presented particular challenges for judicial authorities. For example, the greater the number of participants involved in a crime, the greater the opportunity for judicial authorities to intercept the planning, preparation, plotting or implementation of a terrorist act. However, judicial authorities were at a disadvantage in cases that involved lone actors, who were more insulated from detection by the nature of their individualized process. This was especially true in cases where judicial authorities relied on human sources for intelligence. Consequently, opportunities to identify the perpetrator or obtain information in advance of an operation were greatly reduced.

14. The expansion of Al-Qaida had changed the nature of the terrorist threat. Social media were increasingly used by terrorist groups seeking to take advantage of instant, mass communication forums such as "Facebook", "Twitter" "Instagram" and "YouTube", which were considered to be "tripwires" or catalysts for individual would-be terrorists.

15. As the Internet played an increasingly important role, judicial authorities were also increasingly concerned by the physical movement of individuals to and from conflict zones. Tackling the phenomenon of "foreign fighters" was rapidly becoming a priority for many States. Online "rulings" by terrorist organizations had urged individuals to conduct "violent jihad" in other States. "Returnees" could have an immediate impact on other would-be extremists by offering expertise; serving as role models; or providing physical links to guns, ammunition and other equipment. Governments must also be aware that their own citizens might travel to foreign jurisdictions to take part in violence or terrorism abroad. These factors could lead to an increase in cases involving terrorists acting alone.

16. However, it would be difficult for Governments to justify measures to prevent citizens from travelling to conflict zones. Moreover, restrictions imposed by judicial authorities in an effort to anticipate and prevent terrorist acts might also restrict fundamental human rights such as freedom of movement, expression and association. It was impossible to predict with any certainty why certain individuals become radicalized, but others did not. Judicial authorities should focus on monitoring "radicalization enablers" (potentially troublesome situations) that would indicate when to intervene to prevent a violent act from occurring.

17. Governments must be alert to all possibilities and employ the full range of potential tools at their disposal, from "soft" intervention to criminal justice. Authorities had attempted to contain the problem by limiting travel (whether by revoking passports or refusing to renew travel documents). In some States, "no fly" orders could also be very effective. However, such measures often failed to meet the legal requirement of an "immediate threat to aviation". In Canada, judicial authorities increasingly engaged parents in an effort to alert them to the potential risks associated with their children's online activities. An effective prevention strategy required that security, law enforcement and judicial authorities engage closely with the community. Other institutions, such as schools, community centres and health services, should also be involved in early intervention efforts.

18. Although there was no easy formula for identifying a potential lone actor, there were certain behavioural predictors, enablers or "tripwires":

- Interest in, or attempt to travel aboard to certain conflict zones or to areas where he could get training and connections with other "like-minded".
- Length of time spent abroad in conflict zones. (A "jihadi tourist"[2] might spend his time more superficially, but deeper interest might be indicated by a longer stay and more intensive engagement with a particular cause)
- Attempts to join, or engage with a terrorist organization
- Frequenting certain websites or chat forums
- Increasingly extremist views.

[2] As previously stated, participants recognized that neither terrorism nor the phenomenon of terrorists acting alone or in small cells was associated with any particular religion, ethnicity, group or country. Similarly, the use of specific terms such as "jihad" was not intended to cause offence or insult. As many participants noted: terrorists co-opt religions, terms and metaphors to suit their purposes. The use of such terms in this report is not intended to associate terrorism with a particular religion, but rather to reflect the comments and references made during the discussions. For this reason, such terms are distinguished by the use of quotation marks.

19. Germany's judicial authorities had been tackling the phenomenon of "lone wolves" for several years and regarded it as a priority concern. The cases of *Arid Uka* (who shot and killed two American airmen (2010)); Hali Simsek (who continued to operate following the arrest of other members of his cell (2011)); and Keramut Gul (who educated himself by following the bomb-making recipe published in "Inspire" magazine (2011)) had acted as catalysts for an analysis of the German Joint Internet Centre (GIZ), which had concluded in 2013. The study had found that, in general, "lone wolves":

- Lacked a consistent profile
- Might experience problems of socialization
- Were prone to introversion
- Had "issues" with their cultural roots
- Might have encountered difficulties in their transition to adult life
- Demonstrated certain parallels with spree-killers
- Were open to simple concepts (enabling radicalization over the Internet, for example)
- Sought peer groups
- Were avid consumers of (Internet) propaganda.

20. The GIZ study recommended the following steps:

- Initiatives focused on awareness-raising (by police, schools, physicians, employers)
- Measures to delete aggravating content on the Internet
- Amending legislation to, inter alia, (i) enable physicians to report information protected by doctor-patient privilege; (ii) reduce access to weapons; and (iii) increase the monitoring of persons acquiring bomb-making materials.

21. Efforts by a range of different officials could also pose challenges. For example, the efforts of judicial authorities to engage community leaders in order to defuse potential causes of conflict could lead to further tensions if those efforts were confused with the mandate of security and law enforcement officials to gather information for subsequent use as evidence in a prosecution. The process of converting, or developing, intelligence into evidence for a successful prosecution was complex. (Hence the importance of information sharing by the various institutions involved.) It also raised key questions concerning the protection of sources and other confidential methods of intelligence collection that were central to "disruption" efforts and concerning the need to protect fundamental human rights and respect the rule of law. Nonetheless, intelligence organizations that used to operate much more independently now realize that they must support court processes as much as possible.

2. Operational commonalities and modus operandi

22. Although there were observable differences in the profiles of lone actors and it might therefore be impossible to define the "type" of person who would resort to this kind of terrorism, it was possible to identify certain operational commonalities. The successful lone wolf would certainly need to be relatively self-sufficient. His or her ambitions might not be matched by qualifications or skills. There was a distinct, meticulous planning phase involved. The weapons of choice were generally the improvised explosive device (IED) or the firearm. The Internet also played a decisive role.

23. The Internet not only provided an instant community of believers, but also acted as a "replacement social environment" in which the relatively isolated individual could not only feel that he or she belonged, but also take action on behalf of a group without physical contact. The Internet was not just a key enabler of radicalization and recruitment, but also a source of practical knowledge. In the view of one participant, the Internet "enabled autodidactic extremism, including practical support and ideological development". Many participants noted in this context that the popular do-it-yourself manual, "How to Make a Bomb in Your Mother's Kitchen", published in an edition of "Inspire" magazine[3], had served as a fundamental resource for more than one lone actor.

24. Examination of a suspected individual's relationship to the Internet might therefore enable the authorities to pre-empt an act of violence. Analysis of several cases of terrorists acting alone had revealed certain shared patterns. It was unclear whether an individual's clear dissemination of violent intent on the Internet was sufficient to secure prosecution. Anders Breivik, for example, had been very active on "Twitter" before carrying out his attacks. He had not only researched how to carry our such an attack online, but also published his manifesto and a detailed manual on the Internet. The question of whether intent and public expression constituted evidence that proved an offence was complex, and ultimately depended on the specific laws of each jurisdiction. As one participant noted: "intent alone is not a crime". Nevertheless, it could, in some cases trigger an investigation. It could amount, in some cases, to public provocation to commit a terrorist offence (see article 5 of the Council of Europe Convention on the Prevention of Terrorism) or to the offence of "glorification of terrorism" introduced by several Member States (see, e.g., *Leroy v. France*[4])

25. Analysis of "lone wolf" cases had revealed that the term was somewhat misleading. Most "lone wolves" had a history of having, or having attempted to establish, an association to a radical group, and most had developed contacts with like-minded individuals. Many also had a history of committing petty offences (often related to obtaining material resources). Prevention strategies should therefore include monitoring to detect extremist ideologies and groups and online broadcasting of intent, as well as efforts to raise public awareness, counter terrorist narratives, and mount undercover operations aimed at preventing acts from occurring. Judicial authorities might also seek to intervene at the preparatory phase (which typically involved research, acquisition of weapons and reconnaissance), when the risk of identification or exposure was highest. Breivik's attacks had been calculated and based on meticulous planning. Some of these activities could amount to preparatory offences (pursuant to, e.g., the common law concept of conspiracy to commit a crime or the French offence of *association de malfaiteurs en relation avec une entreprise terroriste* ("criminal association relating to a terrorist undertaking").

26. However, effective monitoring of the Internet was resource-intensive. The resources available to judicial authorities were limited in comparison to the number of potential operational targets and the number of websites and online communication forums involved. Moreover, it was difficult to distinguish between a message that was intended as a first step

[3] The spring 2013 special issue of "Inspire" was entitled "Lone Mujahid Pocketbook: A step–by-step guide on how to become a successful lone mujahid." Similarly, white supremacist Tom Metzger wrote "Laws for the Lone Wolf."

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

towards violence or as an incitement to violence and radical, non-violent expressions of extremist beliefs that are protected by freedom of speech.

3. Available approaches and tools

27. During the meeting participants discussed different legal approaches to meet this challenge. The different approaches could be divided into two categories. The first one focuses on giving law enforcement new tools that would allow them to better detect potential "lone wolves" before they move to the perpetration of the act itself. The second approach introduces new offences that target the perpetration stage. Some countries have opted for a mixed approach that contain both elements. All models have human rights implications that will be discussed in a separate section.

(i) Evolving legislation

28. The Dutch Intelligence and Security Service (AIVD) noted that the Netherlands was a target for terrorist activities, including by terrorists acting alone or in small cells. Four Dutch cases put the nature of this threat into context: (i) the assassination of politician Pim Fortuyn nine days before a general election in 2002; (ii) the actions of Karst Tates, who drove into a crowd on a national holiday in 2009, killing seven bystanders and injuring 11; (iii) the shooting and killing of six people, injuring of 17, in a shopping mall in Alphen on the Rhine in 2011; and (iv) the recovery, from the house of Omar H., in 2012, of bomb-making materials and DVDs with "jihadist" content, including manuals on how to make your own explosives from the Internet.

29. The close relationship between the Dutch prosecution service and the AIVD strengthened the capacity of prosecutors to intervene at the early stages of a crime. Decisions of the Dutch Supreme Court had confirmed that information gathered by the AIVD could be used in court as evidence,[5] provided that it had been channelled through the Dutch Public Prosecutor to the designated public prosecutor and to the police, in the form of an official notification (admissible as evidence). Only the Public Prosecutor was allowed to view the information that formed the basis of the notification. If that information was called into question during a proceeding, the Public Prosecutor would be requested to intervene.

30. Dutch legislation further enabled the prosecution of a range of offences, including recruitment of individuals to join foreign military service and recruitment of persons for armed conflict (Crimes of Terrorism Act, article 205). These provisions could be interpreted broadly to encompass the act of trying to persuade someone to participate in a conflict or merely "trying to convince someone that he would be idolized for dying as a martyr in the fight again the West".

[5] A ruling of the Dutch Supreme Court (HR 5 September 2006, *Eik*) stated that, with two exceptions, material gathered by a security service within the framework of its own powers and competencies might in principle be used as: (1) intelligence for the initiation or conducting of an investigation; and (2) evidence. The two exceptions are willful disregard of criminal procedure safeguards and violation of the fundamental rights of a suspect so that a fair trial guaranteed in article 6 of the European Convention on Human Rights is not possible.

31. Moreover, innovations in Dutch legislation had increased the ability of the judicial authorities to intervene at an early stage[6], to develop a robust prosecution, and thus prevent a terrorist act. For example, under the new legislation, pre-trial detention could be extended to two years, increasing the period of time during which evidence could be gathered, including through mutual legal assistance, and prioritizing the interests of the investigation over the right of the defence to inspect the case file.

32. In addition, the previous requirement of "grave evidence" to justify remanding a suspect in custody had been dropped. Lastly, and perhaps most significantly, special investigative techniques could now be authorized on the basis of "indication" rather than "suspicion". Previously, the threshold of "suspicion" required elements to show the preparation of a terrorist act. However, it was now necessary only to show information that contained facts and circumstances that "indicated" a terrorist crime could or would be committed ("verifiable rumours that an attack is being prepared or that a conspiracy is taking place…"), as well as a factual basis to show justification for a specific measure. A hypothetical example in this regard would be the purchase of chemicals, which were not "explosive material" per se, but of course could constitute the base material to make a bomb. Previously, the purchase of such chemicals would not have met the requirements necessary to authorize a special investigative technique, since there was neither an element of conspiracy nor a "finished product". Pursuant to amendments introduced in 2006, however, those facts would be sufficient to establish an "indication" that a terrorist crime might take place and enable the authorization of an special investigative technique aimed at verification.

33. Strengthened cooperation and information sharing between intelligence and security agencies and the prosecution made it more likely that the potential "lone wolf" would be identified before he or she struck. The Public Prosecutor thus had greater powers to act at an early stage to prevent terrorist crimes. Nevertheless, the effectiveness of those tools still depended on the efforts and vigilance of the judicial authorities involved.

(ii) Applying experience and lessons learned

34. "Lone wolf" terrorism perhaps occurred more often in the United States of America than in any other State, and the frequency of such cases had even increased in recent years. Further research might help explain why this was the case and how the criminal justice approach could be adjusted in response. However, any such approach must take into account the country's strong human rights protections and its belief in the fundamental freedoms of expression and association. With a proven track record in addressing drug offences and organized crime, the American judicial authorities applied their substantial experience and existing tools to investigate and prosecute terrorists acting alone or in small cells. The available investigatory tools included physical and electronic surveillance, search warrants, and the use of undercover officers, confidential sources and other forms of intelligence. Investigations were tailored to specific terrorist-related offences, such as providing material support to a foreign designated terrorist organization, soliciting membership in a designated foreign terrorist organization, or attempting to set off explosives.

[6] Crimes of Terrorism Act, 10 August 2004; Investigation and Prosecution of Terrorist Offences (Extension of Powers) Act, which entered into force in February 2004.

35. In France, efforts to counter terrorists acting alone relied on traditional methods. Nevertheless, the earlier that judicial authorities could recognize that a terrorist act was taking place, the earlier the dedicated Antiterrorism Division of the Judicial Police and terrorism prosecutors could become involved and the earlier the judicial authorities could focus their resources on identifying perpetrators and preventing further offences.

36. The *Mohamed Merah* case[7] offered a good example of the benefits of early identification. A review of Mr. Merah's circumstances confirmed certain commonalities between his case and those of other "lone wolves' and also showed how lone actors could be connected to the wider community. It also shows how a terrorist operating in one State could draw inspiration or "justification" from a situation in another. During the final confrontation with the police, Merah, referring to the French Army in Afghanistan, stated: "You kill my brother, so I will kill you." Before carrying out his crimes, Merah had travelled to Germany, Syria, Turkey, Lebanon, Israel, Egypt, Tajikistan, and Afghanistan. The French police had attempted to contact him about his travels to Afghanistan, but had discovered that he was in Pakistan. The police were told that he would contact them upon his return. It was later discovered that Merah had in fact gone to Waziristan and crossed over to Kandahar, where he had been seen with a known recruiter of French apologists for Al-Qaida.

37. Merah had apparently been asked to commit certain crimes against American interests in France, but had refused on the grounds that such crimes would expose him to the judicial authorities too early. He had preferred instead to choose his own targets and timeline in order to be able to kill as many people as possible. Although Merah had operated independently, he had been trained in Afghanistan and instructed to commit crimes. Thus, as in many other cases of terrorists acting alone, he had never been truly alone in his cause. Moreover, U.S. and French intelligence had identified Merah as a potential "jihadist" before the attacks, but there had been insufficient elements to confirm his intentions or to attract the full attention of French judicial authorities.

38. Judicial authorities around the world were hampered by lack of resources. Effective cooperation with foreign partners in obtaining proper intelligence and information was crucial and could help compensate for lack of resources. Mutual legal assistance treaties, law enforcement cooperation and provision of reliable, useable intelligence to partners were also essential. Prosecutors must be equipped with full knowledge of a case in order to be able to anticipate challenges to evidence, weaknesses in proving elements of an offence, and ensure a fair trial. Evaluation of sensitive information that might need to be protected took place both during the assessment of the charge and throughout the case.

(iii) New types of offence

39. In the United Kingdom, lawyers in the Counter-Terrorism Division provided advice and guidance on cases to police forces in England and Wales and handled prosecutions. United Kingdom prosecutors were armed with provisions that facilitated prosecution of lone actors at an early stage. The 2000 United Kingdom Terrorism Act and 2006 Terrorism Act contained a range of offences that facilitated the prosecution of both group and lone actors.

[7] A string of offences occurred in Montauban and Toulouse in March 2012, resulting in the deaths of seven people and injury to five others (four serious). Ultimately, the perpetrator, Mohamed Merah, was shot and killed after a prolonged engagement with police.

40. With respect to terrorists acting alone, sections 57 and 58 of the 2000 Act were two of the most commonly used provisions. Section 58 was particularly versatile and required, not proof of specific intent, but only that the person knowingly collected information that was "likely to be useful" in committing a terrorist act, or that some kind of link could be established. A person would not be convicted if he had "reasonable excuse for his action or possession". It was not essential to prove the source of the information, via the Internet or otherwise. Similarly, the 2006 Act provided that encouragement of a terrorist act (section 1) and the dissemination of a terrorist publication (section 2) could be proven regardless of the means of communication employed (whether mail, e-mail or the physical passing of material).

41. Prosecutors and police alike, nevertheless, are conscious of the key role of the Internet, which enables: interaction between like minded persons; the sharing of information and material; and the collection of material, in particular in vast amounts. Both sections 57 and 58 of the 2000 Act could be committed by a lone actor in his or her own home, using a computer. Challenges of investigating such offences could include identifying: the offending material on the Internet; who had uploaded that information; what device had been used to store or place the material on the Internet. Where material was found on a computer in a shared household, identifying the person responsible for the material found on the computer, or uploaded from that computer to the Internet, could pose real difficulties. Similarly, considering the vast amounts of information that might be attached to a particular charge, prosecutors must consider what offences to lay, what material to serve as evidence, and how to present the evidence to court in an accessible manner. The Counter-Terrorism Division maintained a database of cases that served as references points for further prosecutions.

42. *R v. Ahmed* was described as an example of a "section 58" case and the early intervention afforded by pursuing such a charge. Ahmed was arrested and his home searched on the basis of intelligence. No violence had yet been committed. A large amount of extremist material had been found on several media devices in his house, leading to six charges under section 58. Prosecutors linked him to media devices, which contained incriminating material, such as the infamous "Inspire" article on how to make a bomb, and other recovered documentation, such as Ahmed's CV. He was also found to be a habitual user of a room in which the devices were found, and the "creation" and "last author" dates on documents were matched to him. Ahmed plead guilty to four offences and was sentenced to 14 months in custody.

43. By contrast, the prosecution service decided not to charge "section 58" offences in the case of *R v. Lapshyn*, instead relying on offences that carried higher penalties: murder; 2006 Act, section 5 (preparation of a terrorist act); and two counts contrary to the 1883 Explosive Substance Act, section 2. Lapshyn had been found to have operated independently in the commission of a string of offences, starting with the murder of Mr. Mohamed Saleem Chaudhry. The Internet had been a clear enabler for Lashyn's crimes. Among other things, Lapshyn had researched sites on the Internet to identify the components and ingredients for an IED, as well as available suppliers. He had performed reconnaissance, based on information retrieved from the Internet, for subsequent crimes at three different mosques, where he had later attempted to explode devices. Following the murder and attempts to set off IEDs, Lapshyn had been identified through the careful review of CCTV, which had recorded him at the locations of all the incidents. After pleading guilty, Lapshyn had been sentenced to a minimum of 40 years in prison for the murder and 12 years concurrent for each of the other offences.

(iv) Strengthening cooperation

44. One of the most important elements in improving States' response to the threat posed by terrorism in general and terrorists acting alone in particular is to strengthen cooperation among all agencies involved in the prevention and prosecution of terrorism. In Europe, regional efforts also reinforced national approaches. Europol brought together law enforcement, intelligence, political and prosecutorial agencies to cooperate through the Europol Counter-Terrorism Centre. In order to support specific cases, Europol had established a first-response network, which had been activated for the first time in the *Breivik* case. Europol databases also offered a shared resource for participating States.

45. The regional cooperation and exchange of information required for an effective counter-terrorism approach must take into account the context of regional challenges and be sensitive to the specific issues and circumstances of each region and State. In Europe, it was easier to adopt an agreed regional approach towards "lone wolves" because an agreed framework and definition of terrorism were already in place.

46. Drawing on this need, Germany had established an interagency structure aimed at facilitating the cooperative approach of German judicial authorities, law enforcement and intelligence. The German Joint Counter-Terrorism Centre (GTAZ), formed to address religiously motivated terrorism, defined the collaborative approach of its 14 member authorities. The GTAZ had improved cooperation and coordination among these authorities by establishing direct communication structures, distributing the workload according to responsibilities, emphasizing joint assessment and coordinated operations and, in particular, strengthening cooperation between intelligence, law enforcement and the Federal Prosecutor-General. As operations and final decisions remained within the power of the separate agencies, the establishment of the GTAZ had not required new legislation.

47. With increased importance placed on the Internet, the GIZ had been established in 2007 to monitor "jihadist activities" on the Internet. It aimed at improving cooperation by Federal German security agencies, facilitating the shared use of resources and expertise, and producing harmonized assessments and reports. The Federal Prosecutor-General, a GIZ member, had thereby improved access to intelligence and information.

4. Human rights considerations

48. The phenomenon of lone wolves and the approach taken by Member States to meet the challenge raise important human rights questions. The manner in which judicial authorities brought terrorists to justice revealed the depth of the State's commitment to human rights and fair-trial standards.

49. Clearly, there were significant human rights risks involved in lowering the threshold for prosecutorial intervention at a very preliminary stage of suspected criminal activity. Similar concerns might be raised in regard to the United Kingdom offence of "collection of material likely to be useful in committing a terrorist offence", especially given the absence of a required showing of specific intent. Participants noted that it was often impossible to know the intentions of lone actors and equally difficult to distinguish between terrorists with violent intent and persons simply expressing or disseminating what might be qualified as "extremist" ideas. The latter were protected by the right to freedom of expression (which included

"freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers").[8]

50. In order to prevent misuse of these offences the United Kingdom requires its prosecutors to balance the potentially competing interests. From the initial charge to the conclusion of the case, the prosecutor must continually assess whether the actions taken and offences pursued were firmly grounded in compelling reasons of public safety. The Netherlands, much like the United Kingdom, relied in this regard on the integrity of its prosecution service, as well as on its active and independent judiciary. Both States were also bound on such issues by the extensive jurisprudence of the European Court of Human Rights.

51. Participants noted that criminalization of any action must be based on necessity and carefully tailored to the conduct at issue. The international counter-terrorism instruments were not "Internet-specific". Judicial authorities must apply human rights law, while guarding against inappropriate Government conduct intended to "control" certain actions, with respect in particular to the prosecution of preparatory acts of terrorism. Although it was appropriate to criminalize acts preparatory to the commission of acts of terrorism, this must always be done in compliance with human rights obligations.

52. More broadly, participants cautioned against the export of solutions adopted in one State to another State. For example, when it came to criminalizing preparatory acts such as collection of information, jurisdictions which did not require a compelling showing of necessity or in which the level of integrity and independence of the judicial authorities might not provide a guarantee against over-use might be left with a dangerously vague offence that lacked the necessary framework of checks and balance. Similarly, lowering the threshold for the authorization of special investigative techniques from "suspicion" to "indication" without robust checks against misuse as exist in the Netherlands, might be abused in a different context, where neither the active engagement of an independent judiciary or effective oversight mechanisms were guaranteed.

53. Participants also noted that it was important not to confuse the issue of "freedom to use the Internet" with issues relating to "monitoring the Internet". International human rights standards protected not only the rights to freedom of expression and opinion, but also the right to privacy. The Internet had become an indispensible means of expression and a repository of a vast trove of ideas. Monitoring use of the Internet through electronic surveillance directly implicated the right to privacy. Since monitoring might compromise this right, it was necessary to ensure independent judicial oversight, prior authorization, and appropriate standards for admissibility of evidence, in order to safeguard human rights and the rule of law. Moreover, more practically, if a website were shut down it could easily be recreated elsewhere. Rather than closing down websites and chat rooms, it might be preferable to embrace the unique opportunities they offered for gathering intelligence or engaging in counter-narrative.

C. Concluding observations

54. Participants agreed that there was no simple way to define the phenomenon of "terrorists acting alone". It might be understood as a spectrum, ranging from the individual

[8] See article 19, International Covenant on Civil and Political Rights.

who acts in total isolation to the individual who is closely influenced by, or linked to a group by philosophical or political motivation. Even where a terrorist was acting alone and was operationally separate from any group, there was often a "collective" element to his actions. In cases where the information provided by a terrorist organization was highly accessible and the organization's message was deeply and effectively embedded into the psyche and choices of the lone actor through the Internet, it was difficult to see how the lone actor could be perceived as "alone". It might be unnecessary to "name" or "label" the phenomenon, but it was important to recognize the patterns involved and thus the potential for effective intervention. Moreover, like other terrorism typologies, the phenomenon of "terrorists acting alone" was far from static.

55. "Lone actor" terrorism represented a small percentage (perhaps as little as 1.8 per cent) of total terrorist incidents. Moreover, it had resulted in relatively few fatalities. However, there appeared to be a troubling correlation between the recent successes achieved against "group terrorism" and the simultaneous increase in incidences of "terrorists acting alone or in small cells." Participants agreed that judicial authorities should be careful not to overstate the threat posed by "lone wolves" but better yet be alert to it. It was not necessary to develop an entirely new or different counter-terrorism strategy. Countering terrorism, in whatever form, depended on the ability of the judicial authorities to cooperate, to detect crime at the earliest possible stage, and to work closely together with the shared goal of bringing terrorists to justice, within a framework of respect for human rights and rule of law.

56. Robust national legislation would facilitate the necessary international cooperation and help build more effective approaches to countering "terrorists acting alone" and related trends, such as the threat posed by individuals travelling to and returning from conflict zones. The earlier the judicial authorities were able to act, provided that they had an appropriate basis for intervention, the more effective the prevention strategy. Identifying how individuals were radicalized or self-radicalized remained a challenge for judicial authorities. The sharing of intelligence by States and among national agencies was central to any effective approach. Intelligence and information should flow as easily as the ideologies that gave rise to terrorism.

57. States should not only cooperate, but also learn from their respective experiences, laws and cases. The main challenge was to enhance cooperation at the national level.. Participants noted with appreciation that regional and international networks of prosecutors provided valuable forums in which to address and understand global threats such as "terrorists acting alone" and to exchange good practices in the development of effective national approaches. Participants noted the value of establishing an online forum for the discussion of cases and general issues by prosecutors, the sharing of research and good practice guides, and the contribution of specialized academics. The United Kingdom database of cases was noted as a good example, in that regard.

58. Lastly, participants agreed that like in life, "prevention was better than cure". Engagement with civil society and the development of programmes to counter violent extremism were crucial to countering the "terrorist" narrative. It was also essential to take into account the power of the media to affect both relations between judicial authorities and communities and the individual's perception of events.