Counter-Terrorism Committee Executive Directorate (CTED)

CTED input for report on the protection and promotion of the right to privacy to be submitted by the High Commissioner for Human Rights to the United Nations Human Rights Council and the General Assembly in accordance with General Assembly resolution 68/167 on the right to privacy in the digital age

1. United Nations Member States, international and regional organizations, and other concerned actors are unanimous, not only in their condemnation of terrorist acts, but also in their recognition that terrorist acts represent an unusual danger that has resulted in the loss of thousands of lives and injuries to countless victims over recent years. However, it is not always easy to determine the best response. The threat of terrorism may be exceptional in certain respects, but it does not always require exceptional responses. Indeed, it is essential that States measure their responses to terrorism very carefully. This is as true with respect to action in the field of information and communications technologies as it is with respect to other areas of counter-terrorism. In all cases, actions taken with respect to information and communication technologies must comply with Member States' obligations under international law, including international human rights law.

2. Technological progress presents Governments and terrorists alike with a vast array of high-tech tools. Information and communications technologies can be used to finance, recruit, prepare and commit terrorist acts, but they may also be employed to help prevent terrorist acts and bring terrorists to justice. They also offer the potential for abuse and overreach. International human rights law places an obligation on States to utilize the benefits provided by technology in a careful, proportionate and clearly defined manner.

3. In paragraph 3 of its resolution 1373 (2001), the Security Council calls upon Member States to cooperate to prevent and suppress terrorist acts and to take action against the perpetrators of such acts. Exchange of operational information regarding the use of communications technologies by terrorist groups should be conducted in accordance with international law. Cooperative agreements between intelligence and law enforcement agencies that authorize the conduct of extra-territorial surveillance or the interception of communications in foreign jurisdictions should be concluded and implemented in full compliance with the obligations stemming from international human rights law, including the preference for targeted communications surveillance and the principle of accountability.

4. Security Council resolution 1624 (2005) recognizes the need, in an increasingly globalized world, for Member States to act cooperatively to prevent terrorists from exploiting sophisticated technology, communications and resources to incite support for terrorist acts. The monitoring of Internet communications to identify possible cases of incitement and recruitment to commit terrorist acts can therefore be an appropriate activity for intelligence and law enforcement agencies. However, improper monitoring, interception of communications, and collection of personal data (including on a mass scale) can also have an impact on the right to privacy. Furthermore, improper monitoring can have a serious impact on other fundamental rights, including the rights to freedom of expression, opinion and association.

5. On 24 May 2013, the Counter-Terrorism Committee held a special event, open to the wider United Nations membership, to explore the link between information and communication technologies, terrorism and counter-terrorism. The discussions focused on several areas, including the use of mobile telephones to facilitate the commission of terrorist

acts, the use of enhanced controls at the border and the storage of information collected when screening the movement of people at border checkpoints, and the tools available to effectively counter the use of the Internet to commit terrorist acts. The speakers included representatives of Member States, international and regional organizations, civil society and the private sector. The Chair's summary of the meeting reaffirmed that the use of telephone technology for surveillance and monitoring purposes should take into account the risk of affecting human rights obligations. In this regard, proportionality, appropriateness and limitation should be taken into consideration, and there should be effective oversight of domestic mechanisms. Additionally, measures taken by Member States to prevent, detect and deter acts of terrorism via the Internet should be subject to effective independent oversight and exercised in a careful, balanced and proportional manner.

6. More recently, Security Council resolution 2129 (2013) noted the evolving link between terrorism and information and communication technologies (in particular the Internet) and the use of such technologies to commit terrorist acts and to facilitate such acts through incitement, recruitment, funding or planning. The resolution also tasks the Counter-Terrorism Committee Executive Directorate (CTED) with advising the Committee on how to further address this issue, in consultation with Member States; international, regional and subregional organizations; the private sector; and civil society.