Special event of the Counter-Terrorism Committee with Member States on “countering terrorism through the use of new communications and information technologies”
United Nations Headquarters, 24 May 2013

Chair’s summary

Excellencies, distinguished delegates, ladies and gentlemen,

I hope that you have found our discussions to be rewarding and thought-provoking.

We are all of us all-too-familiar with the potentially devastating impact of the use of new communications and information technologies by terrorists (whether acting alone or as members of organized groups).

Managing and regulating the use of such technologies (whether to perpetrate terrorist acts, incite terrorism, or radicalize vulnerable individuals) constitutes one of the most rapidly evolving and complex challenges to Governments around the world. And yet, the use of such technologies in countering terrorism is a complex and often controversial topic, which brings us, as it were, into difficult terrain.

The issue discussed today stands at a fragile border between two clear imperatives: on the one side, the need to protect our societies from harm; on the other, the need to protect human rights and fundamental freedoms.

Terrorists will always try to exploit new communications and information technologies to their maximum advantage, and we must therefore act strongly to prevent them from succeeding.

However, if we stray too far and use such technologies in violation of fundamental human rights principles, we risk undermining our own cause and reinforcing the terrorist narrative.

This is the principal challenge before us.

It is therefore essential to develop a broad dialogue on this topic: a dialogue that includes, inter alia, the voices of international organizations, Government, civil society and the private sector.

Today we have listened to experts from many sectors of society (including States, international organizations, industry bodies, think tanks and private corporations), who have informed us about recent developments in complex areas of communications and information technology.

We have also discussed ways to use these technological advances to prevent terrorist acts, and learned about good practices developed and effective measures taken in this area.
During our first session, it was recognized that the growing threat posed by terrorist misuse of mobile-telephone technology required a well-coordinated, multi-dimensional and balanced approach; that the legitimate use of such technologies should not be unduly restricted; and that mobile banking, if administered properly, could help further promote financial inclusion.

We also noted the need for Governments to adopt a holistic and flexible approach in introducing national legislation and regulations designed to mitigate risks and keep pace with rapidly evolving technologies. A tailored approach should be taken to standard-setting, research, and technical assistance activities.

Moreover, in view of the tremendous scope of the potential threats, the sensitive nature of the issues involved, and the difficulty of achieving a balanced approach in the application of relevant legislation, the building of mutual trust and confidence among Member States is a prerequisite for the development of robust, successful counter-terrorism strategies.

The use of mobile 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.

During session 2, we were informed about the latest technologies and methodologies used to regulate the movement of persons at border checkpoints, including monitoring technologies, biometric technologies and technologies that detect explosives and other hazardous or prohibited substances.

It was noted that the use of standardized and machine-readable travel identification documents and measures to preserve the integrity of such documents were effective ways to balance effective border security with the individual right to privacy.

Increased security must be weighed against the need to efficiently process the expected increases in border traffic.

Member States and other relevant actors are bound to cooperate and consider legal means to strengthen cooperation on border security.

Member States should ensure that the use of more stringent monitoring and surveillance technologies at international borders, including through biometric technologies, remains proportionate and subject to appropriate limitations in order to safeguard human rights.

Member States must also make sure that the information obtained through these technologies is reliable, stored securely and used effectively in combination for the purposes defined, in order to prevent misuse, errors and privacy violations.
During our third and final session, it was clearly stated that although the Internet offers numerous benefits to modern society, those same benefits may also be exploited by terrorists for incitement, recruitment, the promotion of violent extremism, fundraising, training and the operational planning and commission of terrorist acts.

In this regard, it should be recalled that Security Council resolution 1624 (2005) calls upon States to prohibit and prevent the incitement to commit acts of terrorism. The Committee is also guided in its work in this area by the provisions of Security Council resolution 1963 (2010) and the United Nations Global Counter-Terrorism Strategy. Sharing effective strategies to counter violent extremism is seen as key to preventing radicalization. Community engagement is also essential.

The Internet presents a wide variety of means and opportunities to prevent, detect and deter acts of terrorism and to bring terrorists to justice through intelligence gathering, evidence-collection, and the introduction of measures to counter the terrorist narrative.

There is a need for user education, more effective information-sharing between the public and private sectors, and exceptional levels of security. It was also recognized that involving communities in counter-violent-extremism strategies would increase their resilience.

Measures taken by States should be subject to effective independent oversight and exercised in a careful, balanced and proportional manner. Governments themselves should also make increased use of the Internet to counter the terrorist narrative.

Excellencies, ladies and gentlemen,

Member States face a constant challenge to anticipate and stay ahead of new methods developed by terrorists. In the case of new communications and information technologies, as in all other areas of counter-terrorism, it is essential to ensure that legal frameworks and international cooperation keep pace with new developments.

It is also essential to achieve an appropriate balance by ensuring that the use of such technologies does not violate human rights, individual right to privacy, or the rule of law. This represents a major challenge, which has political, cultural, social, legal, and human rights dimensions. However, it is a challenge that must be addressed as a matter of urgency, and the international community has expressed a clear determination to do so.

The Counter-Terrorism Committee, for its part, is determined to address this challenge within the framework of the mandates conferred by the relevant Security Council resolutions. Many States face significant challenges in their efforts to mount an effective law enforcement response, and the Committee and CTED stand ready to facilitate the provision of necessary technical assistance.

It is essential that all sectors of society pool their respective ideas and capacities in confronting this rapidly developing threat to global peace and security.
In this regard, the Committee welcomes the open, constructive and interactive nature of today’s discussions, and welcomes the valuable insights provided by the participating experts, including the representatives of the private sector.

It has been emphasized that cooperation with the private sector will be essential in our efforts to achieve our common goals in this highly technology-driven area, and the Committee looks forward to fostering such partnerships in its future work.

It is our hope that today’s special event will serve as a useful starting point for further work in this area; help raise awareness of the many complex issues involved in the use of these technologies; and help strengthen the emerging international dialogue on ways to explore this difficult terrain.

In view of the complexity of this theme, there is also a need to encourage more interaction between the various international entities involved.

In closing, I wish once again to thank the Governments of Argentina, Australia, Nigeria, the Republic of Korea and the United States of America for making their experts available for today’s event, to thank all participating Member States, United Nations entities and international organizations; and to thank the Committee Vice-Chairs for acting as moderators.

On behalf of the Committee, I wish to thank you all for joining us today and for sharing your insights and suggestions.

Thank you.