UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

CONCEPT NOTE

International High-level Conference on Counter-Terrorism in Belarus
"Countering terrorism through innovative approaches and the use of new and emerging technologies"
3-4 September 2019, Minsk

Introduction

This Concept Note provides relevant substantive details of the International High-level Conference on *Countering terrorism through innovative approaches and the use of new and emerging technologies* to be hosted by the Republic of Belarus and the United Nations Office of Counter-Terrorism (UNOCT) on 3-4 September 2019, in Minsk, Belarus.

The High-level Conference is being organised in follow up to the first-ever High-level Conference on "strengthening international cooperation to combat the evolving threat of terrorism," held under the auspices of United Nations Secretary-General Antonio Guterres on 28-29 June 2018, in New York.

One of the four thematic sessions at the June 2018 High-level Conference in New York addressed the issue of "strengthening global action in response to the misuse of new technologies and the internet by terrorists". The High-level Conference in Belarus will seek to further explore this issue, with three plenary thematic sessions, each providing an opportunity for participating Member States and other partners to consider the practical implementation of relevant aspects of the United Nations Global Counter-Terrorism Strategy.

The Conference will convene the United Nations Member States that are also members or partners of the Organisation for Security and Cooperation in Europe (OSCE), and/or members of the Association of South East Asian Nations (ASEAN).

Session I: The Nature of Threat: Misuse of New Technologies and Artificial Intelligence by Terrorists

As new and emerging technologies become increasingly sophisticated and increasingly accessible, terrorists and terrorist groups are seeking to adapt and employ them as part of their efforts to carry out deadly attacks.

We already know that terrorists exploit the internet and social media to facilitate a wide range of terrorist activities, including incitement, radicalisation, recruitment, training, planning, collection of information, communication, preparation, and financing. We also know that social media algorithms are structured to exacerbate individual grievances and polarise intergroup dynamics, encouraging so-called "echo-chambers". These echo-chambers provide optimal conditions for societal exclusion, radicalisation and recruitment. Terrorist operators also use encrypted communication and the dark web to share expertise, such as improvised explosive device (IED) designs and attack strategies, as well as to coordinate and facilitate

attacks. While social media platforms have begun actively removing content from terrorist groups such as ISIL, increasingly creative solutions are required to counter increasingly sophisticated misuses by terrorists.

Meanwhile, other technological developments in the fields of artificial intelligence (AI), robotics technology, big data and biotechnology may also be misused by terrorists to expand the range and lethality of their attacks. The threat of attack against critical infrastructure, previously thought of as impenetrable, is growing. AI-driven weaponry currently being developed by national armies is equally at risk. Already, ISIL operatives are reported to have used drones in their operations.

Security Council resolution 1624 (2005) recognizes the importance of cooperative action by Member States aimed at preventing terrorists from exploiting sophisticated technology, communications, and resources to incite support for criminal acts. The resolution calls for necessary and appropriate measures in accordance with Member States' obligations under international law to prohibit by law incitement to commit a terrorist act and prevent such conduct. Security Council resolutions 2178 (2014) and 2396 (2017) call for Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology and communications for terrorist acts. Resolution 2396 (2017) also encourages Member States to enhance cooperation with the private sector, especially with information communication technology companies, in gathering digital data and evidence in cases related to terrorism.

This session will address the following key questions:

- What further steps can be taken to counter terrorist propaganda and incitement to violence, in particular through the internet and social media?

- Can Member States engage in efforts to curtail the threat of radicalisation in online echo-chambers? What kind of private sector engagement is necessary to meet this challenge?

- Terrorists are increasingly using new technologies to promote their agenda and may do so in the future to orchestrate attacks. Which new technologies are being misused by terrorists and how can Member States prevent such abuses?

- Is terrorism being given proper consideration by governments engaged in the development of new weapons systems based on emerging technologies and artificial intelligence?

Session II: Innovative Use of New Technologies to Strengthen Detection Capacity (Advance Passenger Information/ Passenger Name Record);

Following major military setbacks experienced by ISIL, the threat from foreign terrorist fighters (FTFs) has evolved. Fighters from former ISIL-held territories continue to take advantage of porous borders across the globe, with many of them either returning home or relocating to other countries such as Libya, Yemen, Afghanistan and the Philippines, fuelling

existing conflicts, further destabilising fragile regions and adding complexity to border security and management. The cross-border mobility of FTFs is further complicated by the expansion of air travel, which is projected to double over the next 20 years. Airlines face increasingly complex responsibility for air passenger travel. Processing passenger data is essential to the identification, detection and interception of FTFs and other high-risk passengers, including those that are otherwise unknown to authorities, both before and after international travel.

In its resolution 2178 (2014), the Security Council called upon Member States to require airlines operating in their territories to provide advance passenger information (API) to appropriate national authorities to detect the departure from, attempted travel to, entry into or transit through their territories of FTFs by means of civil aircraft.

In resolution 2396 (2017), the Security Council built on resolution 2178 (2014) by creating new international obligations to strengthen border security and information sharing. In addition to reaffirming its previous requirements on API, the Security Council called on Member States to develop the capability to collect, process and analyse, in furtherance of ICAO standards and recommended practices, passenger name record (PNR) data and to ensure that PNR data is used by and shared with all competent national authorities, with full respect for human rights and fundamental freedoms.

To support Member States to enhance their capacity to use API and PNR data to curb the flow of FTFs in compliance with international law obligations, UNOCT has developed a new capacity-building initiative entitled the "United Nations Countering Terrorist Travel Programme," which is coordinated by the Office and is implemented in partnership with CTED, ICAO, UNODC and OICT. The programme provides Member States most affected by the FTF phenomenon with the Travel Information Portal (TRIP) system, an IT software solution on API and PNR data. The United Nations acquired the software through a generous contribution from the Kingdom of the Netherlands, configured it and branded 'goTravel'. The United Nations is able to provide 'goTravel' to other interested Member States to facilitate the collection, processing and transmission of passenger data.

This session will address the following key questions:

- What are the legal, practical, operational and technological challenges to the implementation of the API and PNR requirements of Security Council resolution 2396 (2017)? How can these be addressed?

- How can Member States harmonize the way that passenger data is collected and shared to prevent, detect, investigate and prosecute terrorist offences, including the cross-border travel of FTFs?

- What are the key human rights considerations for Member States regarding the collection, transmission, use, retention and sharing of API and PNR data?
- What are the best practices in collecting, handling, retaining and sharing evidence from conflict zones, which can be used to prosecute terrorist offences, including the cross-border travel of foreign terrorist fighters, in line with international law?

- How can Member States support the implementation of the United Nations Foreign Terrorist Fighters Capacity Building Implementation Plan at national, regional and global levels? How can the Plan be further adapted to support the implementation of the API and PNR requirements of Security Council resolution 2396 (2017)?

Session III: Development of National, Regional and International Approaches and Strategies to Address the Misuse of New Technologies and Artificial Intelligence by Terrorists

There is a strong international framework to counter terrorism through the United Nations Global Counter-Terrorism Strategy, General Assembly and Security Council resolutions, as well as nineteen international conventions and protocols and many regional and bilateral instruments. Since the adoption of the United Nations Global Counter-Terrorism Strategy in 2006, there have been many examples of Member States working together and establishing new coalitions, involving a wide range of actors, to coordinate their counter-terrorism efforts. However, much more can and needs to be done on practical and operational areas of cooperation, and specifically in response to the misuse of new technologies and artificial intelligence.

As terrorist attacks have spread and become more lethal in recent years, further challenges will be posed by the development of lethal autonomous weapons systems, due to the vulnerability of such systems, the risk of hacking, proliferation, and acquisition by terrorists. No country is completely immune from this threat, and no country can address this challenge alone. The complex and transnational nature of the recruitment, planning of, and carrying out acts of terrorism requires a concerted multilateral effort at global, regional and national levels.

In resolution 70/291 on the fifth review of the United Nations Global Counter-Terrorism Strategy, the General Assembly recognized the importance of preventing violent extremism as and when conducive to terrorism and encouraged United Nations entities, in line with their mandates, to provide technical assistance to Member States upon their request. The resolution also invited Member States, regional and sub-regional organizations to consider developing national and regional plans of action to prevent violent extremism as and when conducive to terrorism, in accordance with their priorities and taking into account, as appropriate, the Secretary-General's Plan of Action. A growing number of Member States affected by terrorism have developed such plans and many have sought the support of the United Nations.

Security Council resolution 2396 (2017) calls upon Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications and resources to support terrorist acts, while respecting human rights and fundamental freedoms and consistent with their obligations under domestic and applicable international law.

This session will address the following key questions:

- How should the international community work together, to prioritize the prosecution of those who use information and communications technologies for terrorist purposes?

- What are the experiences and best practices of Member States in developing national and regional plans of action to prevent violent extremism?

- How can Member States prevent the hacking and interference of lethal autonomous weapons, as well as their proliferation and acquisition by terrorists?

- How can Member States share national policies and practices guiding the development, testing and use of intelligent autonomous systems technologies, bearing in mind national security considerations and commercial restrictions on proprietary information?