UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

VIRTUAL **COUNTER-TERRORISM** WEEK

6-10 JULY 2020

Interactive Discussion I: Responding to the Threat of Bio and Cyber Terrorism

6 July, 12:30-14:00 EST

Concept Note

The possibility of terrorist attacks involving biological agents is a concern for the international community, as materials such as bacteria, viruses and toxins are relatively inexpensive, easy to produce, handle and transport while difficult to detect and control. Cyber disruption of critical infrastructure by terrorists is an equally growing concern, as malicious software and the technical skills to use it to exploit vulnerabilities are becoming more and more available. Adding to these concerns, new scientific developments and emerging technologies such as biotechnology, synthetic biology and Artificial Intelligence, present significant potential for misuse by terrorist groups when combined with other known biological and cyber threats.

The threat posed by biological terrorism is recognized in the United Nations Global Counter-Terrorism Strategy, several Security Council resolutions, including 1373 (2001), 1540 (2004), and 2325 (2016), as well as the Secretary-General's Agenda for Disarmament. Similarly, in the sixth review of the Global Counter-Terrorism Strategy, Member States expressed concern at the increasing use of information and communications technologies by terrorists, and Security Council resolution 2341 (2017) recognized cybersecurity as one of the streams of effort for the protection of critical infrastructure from terrorist attacks.

In March 2020, the World Health Organization elevated the COVID-19 outbreak to the level of pandemic. In addition to its impact on public health systems, vulnerable populations and the economy, the pandemic also raised the spectre of bioterrorism. Briefing the Security Council, the United Nations Secretary-General warned that *"the weaknesses and lack of preparedness exposed by this pandemic provide a window onto how a bioterrorist attack might unfold – and may increase its risks. Non-state groups could gain access to virulent strains that could pose similar devastation to societies around the globe."*

Pandemics and epidemics, such as COVID-19 and Ebola outbreaks, present an opportunity for and may inspire terrorist groups to perpetrate biological attacks at a time when countries are

facing protracted crises. Indeed, some terrorist and violent extremist groups have called for biological attacks by spreading COVID-19. These crises also test the national and international emergency preparedness and response mechanisms that would be activated following a terrorist attack.

Some of the measures to mitigate pandemics, like travel restrictions, home confinement and telecommuting, place additional pressure and reliance on Information and Communications Technologies and their related infrastructure. This, in turn, increases their vulnerability and attack surface, as manifested in the surge in cyberattacks during the COVID-19 outbreak.

This interactive session will discuss human and infrastructure security within the context of a pandemic, with a particular focus on COVID-19, as well as the connection between public health and security. The session will also consider the challenges Member States face in relation to the rising threat of bio and cyber terrorism and the response strategies that need to be put in place to counter these threats.

Key issues to be addressed:

- *How to address terrorism using weapons of mass destruction in the COVID-19 times?*
- *Does the experience of the pandemic increase the likelihood of the use of disease as a weapon?*
- *Health and Security Interface: where does public health and security systems meet?*
- *How to respond to the threat of cyberterrorism and misuse of the internet for terrorist purposes: challenges and strategies?*
- *How to protect individuals and infrastructures from threats of bioterrorism and use of the internet for terrorist purposes?*