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

Remarks by Mr. Vladimir Voronkov
Under-Secretary-General, United Nations Office of Counter-Terrorism

UNOCT-INTERPOL Launch Event
"Second Edition of the Handbook for Using the Internet and Social Media for Counter-Terrorism Investigations"

22 November 2021, 10.00 a.m.
Conference Room 4 – United Nations, New York

Excellencies,
Ladies and Gentlemen,

It is with great pleasure that I welcome you all to the launch of the second edition of the joint UNOCT-INTERPOL handbook for using the Internet and social media for counter-terrorism investigations.

I would like to express our sincere appreciation to Special Representative Odd Reidar Humlegard and our partners at INTERPOL – and Ambassador Osuga Takeshi for Japan's support to this joint effort.

Today, the majority of the world's population has access to the Internet with attendant growth in digital connectivity and inclusivity, however uneven it might be. People's lives increasingly take place both online and offline.

The General Assembly Declaration for the 75th anniversary of the United Nations points to the unprecedented opportunities and new challenges presented by digital technologies, including their malicious use.

The past 20 months since the onset of the COVID-19 pandemic have only magnified this paradox further.

On the one hand, digital technologies have boosted the healthcare response and enabled governments, businesses, societies and even diplomacy to keep going despite social distancing.

On the other hand, the use of digital technologies for criminal purposes – including by organized criminals and terrorists – has taken new forms and reached new heights.

As these technologies spread, evolve and transform every aspect of our lives, related vulnerabilities will only increase.

Maximizing the benefits and mitigating the risks of digital transformation is a key component of the Secretary-General's report on *Our Common Agenda*.

Building on his *Roadmap for Digital Cooperation*, the Secretary-General called for collective action to reclaim the digital commons, protect the online space and strengthen its governance.

As part of these efforts, we need to deny the digital space to terrorists who have been all too keen to exploit the Internet's tremendous reach and anonymity for their nefarious purposes.

They use the Internet and social media to spread violent extremist ideologies, radicalize people, and incite and plan terrorist attacks; they use virtual assets, mobile payment systems and crowdfunding for terrorism financing; and they use cryptography and the Dark Web to hide.

The ways in which terrorists use the Internet are constantly changing as new capabilities go online and new platforms emerge.

But the online activities of terrorists leave traces that can be followed in a way that allows Member States to detect and bring terrorists to justice, even in the preparatory phase.

Member States therefore are increasingly looking at the Internet as a resource for counter-terrorism investigations. Open-source information and the Dark Web can yield critical leads and evidence.

Ensuring that Member States have the capacity to collect and process such information is recognized as a counter-terrorism priority by the Security Council.

And the General Assembly, in its seventh review of the Global Counter-Terrorism Strategy this past June, requested that UNOCT supports innovative measures and approaches to build the capacity of Member States for the challenges and opportunities that new technologies provide in preventing and countering terrorism.

These efforts are spear-headed by the Global Programme on Cybersecurity and New Technologies of the United Nations Counter-Terrorism Centre withing my Office, working in partnership with Global Counter-Terrorism Coordination Compact entities such as INTERPOL.

In the framework of this Global Programme on Cybersecurity and New Technologies, our effective partnership with INTERPOL will be expanded with the upcoming launch of the joint project “CT TECH”, made possible by a generous contribution of the European Union.

Today, we introduce a second edition of our joint handbook to provide practical support to Member States on how to conduct counter-terrorism investigations online and how to use this information in criminal proceedings, while upholding human rights and the rule of law.

The revised handbook takes stock of latest technological advances and modus operandi of terrorists online.

It looks at gender aspects and identifies good practices for conducting online investigations for counter-terrorism purposes, including to respect freedom of expression and the right to privacy.

It provides practical guidance on how to transform online information into electronic evidence and includes a repository of useful tools and websites for counter-terrorism investigators.

Dear Colleagues,

There should be no impunity for terrorism, offline or online, and we must ensure that the digital space becomes a global common good for humanity, and not a safe haven for terrorists and other criminals.

This handbook will assist Member States in building their online investigation capacities following principles of accountability, competency, objectivity, and legality to uphold the rule of law and human rights.

We look forward to continuing working with INTERPOL, our other partners and generous supporters like Japan and the European Union, to assist requesting Member States in this challenge.

Thank you.