UNDER-SECRETARY-GENERAL FABRIZIO HOCHSCHILD

REMARKS AT THE OPENING OF THE VIRTUAL COUNTER-TERRORISM WEEK

United Nations

6 July 2020

Checked against delivery

What allows us to have this meeting, to talk to one another, is the miracle of digital technology. Digital technology has literally saved countless lives and livelihoods during the pandemic and yet our increased and increasing dependency on it, has also brought to the fore unanticipated risks and dangers. I want to talk briefly about these.

I would like to raise three key points on security threats in the digital domain.

Firstly, our dependency as societies, and individuals on the digital domain has introduced a new domain for conflict and attack. For most of history, we dealt only with the warfare domains of land, sea and more recently, air. Now we have another domain – cyberspace. Not since the invention of manned flight just over a century ago has there been such a significant expansion of a means for violence, conflict and disruption.

With COVID, in recent months, we've seen a significant increase in cybercrime and attacks by those seeking to do harm to citizens around the world. To illustrate this -- in the first quarter of this year, while use of the internet, according to ITU, went up by between 40 and 80 percent, there was a 350% increase in active phishing websites.

One particularly alarming illustration of cybercrime in the time of COVID has been the severe uptick in digital attacks on global hospital systems. Healthcare facilities in several countries, including France, the United States, and Spain, were targets of cyberattacks, while the World Health Organization has also seen a very large increase in cyberattacks.

Secondly, the pandemic has brought with it a significant increase in the use of social media for disinformation, the dissemination of violent extremist content, and the planning of terrorist attacks.

As was said by the distinguished Ambassador of Tunisia, Kais Kabtani, with people spending more time online than ever before, terrorists and other proponents of hatred and division have been provided with a captive global audience, many of whom are feeling afraid, isolated, and unable to trust authorities. Moreover, the strange alien nature of this crisis has been used to spin fear-based conspiracy theories and fuel extremism.

Social media platforms and messaging services have begun to tackle this abuse of their services, but they will not be able handle the burden alone. Heightened cooperation and information sharing is required between Governments and law enforcement as well as the private sector. The Secretary-General launched 'Verify' on 21 May, a campaign aimed at curtailing misinformation on social media.

Thirdly, COVID has reminded us of the need to make sure the adoption of new technologies occurs within the framework of human rights law. The adoption of technologies for surveillance and tracing as well as the restrictions on harmful content, need to be adopted in conformity with international human rights obligations. Where we cut corners and violate human rights or operate outside the rule of law, there is a risk of exacerbating distrust and subsequent extremist activity rather than curtailing it.

With regard to curtailing cyber security threats, important work is underway on the normative side, in particular through the Open Ended Working Group, the Group of Governmental Experts and the Security Council, which are so ably supported by the UN Secretariat, through the Office of Counter Terrorism, through CTED, ODA and others Secretariat entities.

We have seen encouraging voluntary efforts on terrorist and violent extremist narratives, including the Christchurch Call. However, these efforts are not universal, and their reach, though broad in some cases, does not cover all of the world.

We have also to recognize that as important as these initiatives are they are not yet to scale with the challenges we face. The online security threats we face go beyond what these various initiatives are able to curtail and much more work is needed if we are to leave the world as safe as we found it before the advent of digital technology.

In his landmark Roadmap for Digital Cooperation launched last month, our Secretary-General recognized that terrorist groups and violent extremists have exploited the Internet and social media to cause harm in both the digital and physical worlds.

Since last year, in pursuit of the Secretary-General's Roadmap my Office has been coordinating eight thematic multi-stakeholder groups that are working on the important areas identified in the Roadmap, for example, global connectivity, digital human rights, and most importantly, digital trust and security, so as to try and better address the gaps in international digital cooperation.

At a time when many governments have been moving away from international cooperation, the COVID-19 pandemic has served as a stark warning. As our unprecedented dependence and need for digital technologies grows, we must collectively commit and take enhanced action together to ensure a secure,

peaceful, and trustworthy digital future, in which human and other life is protected and respected.

Thank you.