Remarks by Cristina Duarte
Under Secretary-General and Special Adviser on Africa

High-Level Conference on Counter Terrorism
28 June 2021

Excellencies, Ladies and Gentlemen,
All protocols observed.

Let me first thank the UN Office of Counter-Terrorism for inviting me to speak to you today and the opportunity to participate in this important conference.

Ladies and gentlemen,

Advances in information and communications technology have seen the world connected like never before, with information and ideas travelling faster and farther than ever. This impact has been seen the world over, including in Africa where it has been a key enabler of socio-economic development.

The benefits of ICT development in Africa have been incredible. It has completely transformed not only communication on the continent but a wide range of sectors., including health, finance and banking, and even agriculture.

And yet, while the continent pushes for digital transformation and strengthened connectivity, there has been growing concern about the dangers of this technology.

We've seen social media and other digital platforms become low-cost tools used by extremist groups to heighten grievances, spread hate, spur civil unrest, spread propaganda and misinformation, and even to recruit followers.

While its social, economic and even political benefits are clear, we have seen its potential dark sides as well. …

More and more extremist groups such as Al-Shabaab, Boko Haram, ISWAP and ISIL, are using technological advances and expanded Internet access in parts of Africa to finance, train and communicate with potential and current followers.

Africa is no exception to what we are increasingly seeing worldwide, where governments, concerned by the wide reach and blinding speed of these technologies, have taken restrictive measures in order to control potential threats. This year alone has seen social media shutdowns in four African countries.

Shutdowns are usually justified with laudable aims: combatting the spread of hate speech and disinformation; suppressing violence; preventing riots and other forms of civil unrest.

But unbalanced restrictive measures often hurt more than help.

The challenge, unfortunately, is that we fail to understand the nature of social media and other digital technologies. It is often overlooked, for example, that a ban on social media can easily be overcome using cheap and affordable VPN (Virtual Private Network) services that enable users to circumvent government blocks.

In addition, the potential costs of these bans, their potential impact on development, is most of the times disregarded. Negative effects on education, domestic commerce, and entertainment costing millions of dollars and impacting millions of citizens. And that limited understanding also applies to how public

institutions can benefit from using these technologies to communicate their own messages and increase their legitimacy toward the population.

As a result, rather than lessening tensions, shutdowns have the tendency to increase anger, heighten mistrust in government, and give credibility to the very narratives these governments are fighting against.

It is a bit like driving on ice in the winter. When your car starts to skid, the impulse is often to slam on the brakes or to steer harshly in the opposite direction. But, if you do this, your car will invariably spin out of control and crash. Instead, the guidance is to slowly steer *into* the skid and eventually, you will be able to right the car and regain control.

In this instance, steering into the skid means resisting the impulse to shut down access. Instead, a measured approach that addresses the *actual* problem while also uses technology to convey a different message and achieve positive aims is usually more effective.

Therefore, it is important to realize that technology is not the problem.

Growing technological advances and digitalization spurring terrorism and criminality is not the whole puzzle. Instead, it is a piece that fits in a much intricate and much larger puzzle that terrorists and extremist groups use to foment division and conflict.

In a short intervention like this, it will not be possible to delve into the multiple and complex issues behind the factors that make up this puzzle. However, a few key underlying factors can be highlighted, including lack of economic opportunities and service delivery for Africa's predominantly young population, political and social exclusion and marginalization.

Terrorist groups are thriving by amplifying and using these often-genuine grievances, often through social media and digital means, to spread misinformation and recruit members and adherents from among disaffected populations.

For example, is true that extremist groups are using social media to spread propaganda and recruit new members. The stark reality, however, is that much of their messaging is rooted in valid grievances of the people, particularly the failure to provide basic services such as food, energy, education, healthcare, housing, water and sanitation.

In many instances, these failures are more strongly borne by marginalized groups, worsening inequalities along distinctions that have long driven underlying tensions, such as ethnicity, geographic location, and others.

When you look at where violent extremist groups are experiencing the greatest success and growth in Africa, it is not in major cities. Instead, it is in remote areas, often in border areas between two or more states. Why there? Because these are the areas that, due to circumstantial, geographical, demographic or other complexities, are usually the most neglected, politically, economically and socially.

This can be seen in Northern Mali, north-eastern Nigeria, the Kenyan coastal region, and many other areas. Neglected areas suffer disproportionately from insecurity and underdevelopment, which are ultimately exploited by extremist groups through compelling narratives that speak to the grievances of the communities.

It is precisely in these areas where violent extremism is increasingly taking root.

More and more, we are seeing extremist groups exploiting fragility and long-simmering grievances to further their political goals, frequently providing “security”, “justice” and social services such as healthcare, electricity, water and

sanitation, education and infrastructure in the territories under their control in order to gain legitimacy, build credibility and recruit members.

In the Lake Chad Basin, for example, extremist groups like Boko Haram and the Islamic State in West Africa Province (ISWAP) have used lack of public service delivery to help their recruitment and growth, filling gaps in governance by digging wells and providing basic health care and Islamic education.

In Somalia, Al-Shabaab, ISIL and other groups have been able to strengthen their influence and credibility by exploiting local clan grievances, filling governance gaps, and taking advantage of authorities' inability to provide basic services and rule of law in areas under their control.

These are the realities around which extremist groups build their messaging, which they then spread using social media and other digital technologies. The narratives they spread amplify grievances, while highlighting gaps in governance, lack of opportunities and fundamental needs that have been left unmet for far too long.

Digital technologies provide the means of spreading these communications, but more important than the means of communicating is the power of the narrative being communicated. Extremist narratives, grounded in some elements of truth, have been fundamental to their efforts to foment violence, radicalize and recruit, particularly towards the youths who are most often the users of these platforms.

Fighting back should be centered not on fighting the technology, but on fighting against the narrative.

Ladies and gentlemen,

This requires two critical actions. First, of course, is making the narrative untrue. Naturally, if extremist groups are using technology to amplify grievances and spread propaganda regarding government failures and their comparative

successes, one of the most important things government can do is to make this not true.

The paradox facing governments throughout the developing world, including in Africa, is that failure to sufficiently invest in inclusive development historically has led to increased costs related to counterterrorism and security investments today.

Governments need to strengthen equality between groups so that grievances are reduced. Deliver services so that confidence and trust in government is restored. Create an environment of inclusive development that offers opportunities for all, including jobs, so that extremist groups' recruitment calls lose their appeal.

The second action is to understand the technology and use it as a tool to fight back. The internet, including social media, can be a game changer for governments, including rapid and wide-spread crisis communications, strengthened citizen engagement, building public trust, and countering disinformation.

But this requires adapting to rapidly advancing technology and seizing this opportunity to take advantage of new forms of communication.

Excellencies, Ladies and gentlemen,

Even with the growing intersection between digital security and national security, many African countries are not prepared to counter misuse of technology and many lack comprehensive policies and strategies. Joint legislation, increased capacity, political will as well as investments in the infrastructure to share data and intelligence are going to be critical for Africa to deter and counter terrorism activities facilitated by technology.

This effort can however be jeopardized by the deficit of cybersecurity professionals and lack of infrastructure to police the cyber space and to protect critical infrastructure such as telecommunication, banking and utilities. Further complications arise also with introduction of crypto currencies and difficulty in

tracing electronic payment systems, limiting government's ability to trace illegal financial flows that can finance terrorist activities.

Recognizing this threat, The African Union, through Agenda 2063, has identified cybersecurity as a key priority to ensure that emerging technologies are used for the benefit of Africans. The guiding continental framework to this end is the African Union's Cybersecurity Convention (AUCC), adopted in 2014 to legislate important elements of electronic transactions and protection of personal data. However, the convention will only come into force when ratified by 15 member states. So far, it has been ratified by 8 countries.

Ladies and gentlemen,

I want to conclude by emphasizing that Africa's ability to counter-terrorism in all its forms is not just an "African issue". Misuse of technology by terrorist and criminal groups enables them to have uncontrolled access to arms, covert funding, recruits and training materials. It can also facilitate transnational organized crime, including human trafficking and exploitation.

Africa is unfortunately a growing global transit hub for the trafficking of drugs and a range of illicit commodities, with narcotics, pharmaceuticals, stolen motor vehicles and other goods sold and bought online on the surface, deep and dark web.

Cyber-attacks on African Banks, which are increasingly becoming potential targets, can have wider impacts on connected international banking networks, exposing them to billions of dollars in losses due to theft. Service disruptions in critical sectors including African ports and disrupted shipping can create significant delays in the movement of goods, affecting economies beyond African ones.

Therefore, global leadership is critical, and it needs to be preventive not responsive. Because left unchecked, such expansions of technological misuse in Africa will have wider international ramifications.

Africa should not be left alone or behind in countering these threats but needs global partnerships and investments to build its capacities and protect its citizens.

Thank you.