"UN Sanctions and Digital Technologies: Threats and Opportunities"

Remarks delivered by Gerard van Bohemen,
Permanent Representative of New Zealand

I wish to thank Finland and Compliance and Capacity Skills International (CCSI) for hosting this event in follow-up to the High Level Review of UN Sanctions. The compendium from the High Level review of UN Sanctions is a helpful blue-print of best practices that all Council Members should consider closely.

Based on my role as Chair of the 1267/ISIL (Da'esh) and Al-Qaida Sanctions regime, I will touch on three main points: 1) How ISIL (Da'esh) and Al-Qaida misuse digital technologies, 2) What is covered by existing sanctions, and 3) The role of the private sector. Before I begin, I wish to thank the Coordinator of our committee's expert body for his contributions to this briefing.

First, how ISIL (Da'esh) & Al-Qaida misuse digital technology. These groups do so in five key ways:

- One, as a finance mechanism – a recent Financial Action Task Force report from October 2015 identified use of the internet, social media, and internet tools for financing as an emerging trend for terrorist financing. Crowd funding is no longer the exclusive purview of civil society organisations; terrorist organisations and Foreign Terrorist Fighters (FTFs) have discovered the power of this instrument.

- Second, as an operational planning tool and knowledge platform to facilitate attack planning and execution. For example, in 2014, ISIL fighters boasted publically that they had developed an app allowing easy calculation of mortar trajectories on the battlefield. ISIL' videos and chatrooms disseminate tactical advice such as how to design an improvised explosive device (IEDs).

- Third, as a propaganda tool. ISIL has demonstrated a very sophisticated understanding of communications and propaganda strategies, tailoring their communications to particular audiences in a far more advanced manner than other groups have before. It allows the organisation to disseminate its disturbing views and project a fiction of what life is like in ISIL-controlled territory.

- Fourth, as a recruitment tool. On this, we need to be aware that while the internet is frequently used in the recruitment of FTFs, it is, by itself, rarely successful. In the majority of FTF cases, personal contact is what "pushes" an individual self-radicalised over the internet into becoming an FTF.

- Finally, as an internal communications tool. Here, ISIL acts very differently. It is concerned with security, ISIL members carefully guard their communication via internet and digital technology.

Onto my second point, how digital technologies are covered by existing UN sanctions. The Security Council's 1267 Committee administers United Nations sanctions against ISIL (Da'esh), Al-Qaida and associated individuals and entities. All UN Member States are required to implement the measures against listed individuals and entities. Our most recent resolution, resolution 2253 (adopted late last year), dealt with misuse of the internet in a number of ways:

- It condemned ISIL and al-Qaida's use of the internet to incite, recruit, fund or plan terrorist acts.

- It clarified that the assets freeze applies to funds used for the provision of internet hosting and related services used for the support of ISIL and al-Qaida.

- It urged Member States to act cooperatively to counter terrorists' Internet and social media use, including by developing counter narratives, while respecting human rights and fundamental freedoms.

- It tasked the committees' expert body, the Monitoring Team, to assess criminal misuse of the internet by ISIL and Al-Qaida and provide recommendations on any further countermeasures needed. The next regular report of the Monitoring Team, which will contain this assessment and any associated recommendations, is due on 30 June. The Committee will need to discuss and agree proposed action based on any recommendations before it can be actioned.

For the 1267 committee, any Member State can put forward the names of individuals and entities for listing. In particular, they are encouraged to submit listings that would inhibit ISIL's ability to misuse the internet and digital technology. This reiterated previous Council calls for listings of individuals and entities who finance, plan, recruit or otherwise support terrorist acts or activities, including through information and communications technologies, such as the internet, social media, or any other means. Once a listing has been submitted and prepared for circulation to the Committee, it undergoes a 10-day consideration period. If there are no holds or objections placed by any Committee member, the listing is approved and the measures will apply.

Outside of the 1267 committee, in our view few other sanctions committees deal directly with the issue of use of digital technologies by sanctioned individuals. Those that do are often linked back to terrorist acts and work closely with the ISIL and Al-Qaida Committee.

Third, and finally, the role of the private sector. What is clear is that, similar to other areas of sanctions implementation, the full potential of the sanctions measures can only be achieved if all relevant stakeholders work cooperatively and collaboratively. The private sector, in particular, has a pivotal role to play. This has been explicitly recognised by the Council in resolution 2253.

In the last two years, a lot of progress has been achieved in the counter messaging and counter narrative space, with support from the private sector. Further cooperation could help the Council, and its sanctions committees, to develop a deeper understanding of the challenges these companies face and how we can assist.