THE PERMANENT MISSION
OF MALTA TO THE UN NEW YORK

Malta
2023-2024
UNITED NATIONS
SECURITY COUNCIL

Security Council Open Debate on Maintenance of Peace and Security: Cybersecurity, 20 June 2024

Malta Statement delivered by Her Excellency Ambassador Vanessa Frazier
Permanent Representative of Malta to the United Nations, New York

---

President

I begin by thanking the Republic of Korea for organising this open debate on this highly topical and important issue. I also thank the Secretary-General and the briefers for their insightful briefings.

Malicious cyber activities present multifaceted challenges that can have serious impacts on the maintenance of international peace and security. These range from ransomware attacks on government institutions, critical infrastructure, and essential public services, to the unauthorised access and use of electronically stored data.

244, East 48th Street, New York, NY, 10016
T +1(212) 725 2345 **E** malta-un.newyork@gov.mt

www.foreign.gov.mt

We are alarmed by the malicious cyber activities targeting government institutions and democratic processes, often with the direct intent to undermine stability and security and to erode trust in the outcome of democratic elections. The growing reliance on digital technologies by women's human rights defenders and other activists increases their risk of exposure to online harassment and attacks.

Furthermore, human rights and fundamental freedoms, including freedom of expression and assembly, are being increasingly restricted by strict surveillance, internet shutdowns, and bandwidth throttling. At the same time, digital platforms are often exploited to spread dis- and misinformation and hate speech, including misogynistic, homophobic, and radicalising content.

Our collective efforts to promote stability in this domain must be rooted in human rights, both online and offline. Cyber policies must be conflict-sensitive, age-sensitive, and gender-responsive to detect and prevent the harmful impacts of digital security threats, such as technology facilitated gender-based violence. Women's full, equal, safe, and meaningful leadership and participation in cyber decision-making is crucial, especially in conflict and post-conflict contexts.

We reaffirm that international law, in particular the UN Charter, is applicable to activities in cyberspace, as recognised by the UN General Assembly. In the same vein, the framework of responsible state behaviour in cyberspace provides agreed guidelines for member states. This framework should be upheld by all member states, and we support the establishment of a Programme of Action to ensure continued and institutionalised dialogue.

In addition, we call upon all states to exercise diligence, take appropriate measures in line with the norms of the UN framework for responsible state behaviour in cyberspace, and refrain from participating in or aiding malicious cyber activities originating from their territories.

State-sponsored malicious cyber actors exploit ransomware and digital thefts to generate illicit revenues. These include attacks against critical infrastructures as well as financial institutions and cryptocurrency firms. Cyber attacks and crimes know no borders, and no country is immune to them.

Reports estimate that, in 2023 alone, malicious cyber activities by DPRK-sponsored hackers have generated the equivalent of one billion dollars. The regime utilises these revenues to fund its illegal WMD program, which threatens peace and security in the Peninsula and beyond. These activities have been well documented in the reports of 1718 Committee Panel of Experts, which played an invaluable role in investigating these crimes.

To conclude, President, the Security Council can play an important role in addressing the issue of cyber security. Its efforts can and must be complementary to other cybersecurity fora based in the General Assembly, including its Open-Ended Working Group.

The Council can serve as a powerful platform to reinforce agreed principles and enhance further discussions. It should promote an open, secure, accessible, and peaceful cyberspace. We will continue to support its renewed engagement on this topic.

I thank you.