

## **Statement by Ambassador James Roscoe, UK Acting Deputy Permanent Representative to the UN, at the Security Council Arria formula meeting on Cyber Stability, Conflict Prevention and Capacity Building**

**Friday, 22 May**

Mr President,

I thank Estonia for its initiative to bring cyber security to the Security Council. I welcome the briefings we have listened to, and the opportunity to consider this issue in an open and inclusive Arria format.

As the Security Council meets today, it is a reminder of how so many lives rely on digital connectivity, especially during this global pandemic - as you said yourself, Foreign Minister, in education, in medicine, for keeping in touch with our families. And our services too - energy, transport, and public utilities - are underpinned by cyber-technology. But unfortunately, we face threats in the digital space. The British Foreign Secretary recently called for an end to cyber attacks by hostile actors who are using the coronavirus pandemic as an opportunity to carry out harmful cyber activity. The UK National Cyber Security Centre has identified, amongst other activity, a surge in websites imitating those of official organisations connected to the COVID-19 outbreak, such as the World Health Organisation. It is unacceptable that malicious cyber actors are targeting those working to overcome the pandemic around the world.

Hostile actors must understand that irresponsible behaviour in cyberspace will carry a cost. This deliberately harmful cyber activity knows no international boundaries, so neither should our efforts to resist and deter such attacks.

Mr President,

In 2013 and 2015, the General Assembly endorsed our shared commitment to uphold the application of international law to activities in cyberspace, just as it applies to activities in any other domain. As our Foreign Secretary made clear, now, more than ever, international law and the voluntary and non-binding norms of responsible state behaviour which sit alongside it must be respected. These form the basis of the international stability framework for Responsible State Behaviour in cyberspace, along with confidence building measures, and are crucially underpinned by capacity building.

Three consensus reports of previous UN Groups of Governmental Experts provide recommendations, which every State should implement to deliver this international stability framework. In 2015, the General Assembly called on all UN Member States "to be guided in their use of information and communications technologies by the Group of Experts 2015 report". Now is the time to make that a reality. Ongoing discussions, both the open and inclusive Open Ended Working Group, and the valuable expert-based format of the GGE, are critical to achieving this.

The United Kingdom believes that positive action by all States to implement the international stability framework can reduce the risk of conflict; that's why we are here in a Security Council format today. We have been at the forefront of demonstrating that there are consequences attached to malicious activity. The UK can, and does attribute malicious cyber acts to States where we believe it is in our interests to do so, and to further our commitment to clarity and stability in cyberspace. We share our analysis of the threats and our experience, to increase the capabilities and commitment of countries globally to do the same. We are one of the most active cyber donors in the world, investing over \$44 million in international cyber work with partners in more than 100 countries across six continents since 2012.

But no country can do this alone. There is a vast community supporting States. From regional organisations, such as the OSCE, who help States to implement CBMs, to the principle-driven capacity building of the Global Forum for Cyber Expertise (GFCE.)

We all have a role to play in the implementation of our framework, and all states and stakeholders must draw on this community to take their positive steps. It is only through our shared commitment to do so that we can effectively support the maintenance of international peace and security in cyberspace.

Mr President, we all know what being a good global citizen in cyber looks like. We all know the security and real risks to people when malicious actors act irresponsibly. So I hope all the States assembled here today will recommit themselves to responsible state behaviour in cyberspace.

Thank you, Mr President.

Kind regards,

Communications Team | UK Mission to the UN

Follow the UK Mission to the UN on twitter for the latest news @UKUN\_NewYork

This email is intended for the addressee(s) only. All messages sent and received by the Foreign & Commonwealth Office may be monitored in line with relevant [UK legislation](#)