UK STATEMENT – EXISTING AND POTENTIAL THREATS

Chair. Thank you for the opportunity for all of us to give the national statements we came here to make. Before proceedings I want to make clear that the UK does not support the idea put forward by our Russian colleague that there are opponents in this OEWG process.

We all want this process to succeed and we hope we can move towards that from this point. In December the UK said that ‘working together to understand the evolving nature of the threat of malicious cyber activity is crucial to setting the context in which we develop practical measures for international cooperation’.

Our threat context has changed and we must note it.

The UK can say clearly that we stand for the responsible use of any State cyber capabilities. Addressing the real-world impact of hostile activity against critical national infrastructure remains a number one priority. We should be in no doubt that in times of high tension hostile activity against critical national infrastructure poses escalatory risk.

Ahead of Russia’s March 2014 annexation of the Ukrainian territory of Crimea, and in the years immediately following, state-sponsored cyber actors embarked on a campaign of disruptive attacks against Ukrainian critical national infrastructure.

In a familiar pattern, in February this year we saw activity against the Ukrainian financial sector which we attributed to Russia.

Last week we attributed a concerted global campaign of malign cyber activity targeting critical national infrastructure in Europe, the Americas and Asia to Russia.

And we also sanctioned an additional Russian organisation for its 2017 activity interfering with safety override systems in industrial control systems.

These malign activities must stop.

We add to these, concerns the danger of ‘spill over’ activity – the cross-border impact arising from reckless malicious activity.

In 2017 Russia unleashed the destructive NotPetya cyber capability on the Ukrainian financial, energy and government sectors. It spread well beyond its initial targets. NotPetya was a deliberate attack, but its impact on the UK and other countries was unintended. It was reckless.

We should be clear irresponsible and reckless activity resulting in spill over impact – particularly against a State’s critical national infrastructures – can be escalatory.

Additionally in December we spoke – in the context of Ransomware - of the importance of implementing norm C - the ‘reasonable steps’ a State may take to address malicious activity emanating from within their territory.

The UK takes this opportunity make clear that it does not support any unlawful activity in cyber space. Individuals who undertake such activity from the UK can be charged with offences under the Computer Misuse Act. This applies to activity relating to this conflict as much as it does to any other unlawful cyber activity.
So-called ‘hacktivists’ introduce risks to themselves where they undertake illegal activity. And they pose a risk of unintended escalation, particularly where activity occurs around critical national infrastructure. States should therefore be alert to significant activity in support of either side of any conflict.

I note our Russian colleague’s comments on cutting off countries. It is important to be clear what action has been taken and why.

- Many messaging services and platforms have been clear that they aim to continue serving Russian customers.
- But several digital services are not operating in Russia because they have been blocked or limited by the Russian government.
- And where technology companies have withdrawn, the majority of these have made clear that they have done so on the basis of commercial risk and not political positioning. Very few have made any political statement. But they have done so on the basis of financial issues, regulatory issues or other concerns. These are legitimate business concerns.

With regard to the importance of the free flow of information which was raised. We fully agree and will look at this topic under our norms intervention. Similarly - Interference in internal affairs – we believe we can have a substantive discussion of this issue under the upcoming session on the application of existing international law where there is already an legal obligation which we believe is of relevance.

Finally I would note it is not true to say no one has thought about measures to countermand these issues raised previously. We believe that these measures are indeed encapsulated in the framework we are here to discuss.

This is the context which inspires the practical, action-oriented measures I hope to speak about in our sessions this week.

Chair, improving cyber resilience is central to reducing cyber-attacks and their real world impact. Strengthening the resilience of critical infrastructure must be a top priority for States. Strengthening the relationships between government departments, regulators, and private sector operators is key to ensuring the latest threats, risks and vulnerabilities are understood mitigated effectively. States can provide technically accurate, timely and actionable cyber security advice and guidance to businesses and organisations to enable them to properly manage their cyber risks.

States should, where possible, make publicly available their approaches to cyber security and resilience, including how they relate to critical infrastructure protection. The UK routinely publishes this information including guides on how to effectively detect, respond to and resolve cyber incidents, and crucially where organisations can find support from certified Cyber Incident Response companies assessed against clear published standards.

And there are a range of organisations of CERTS that allow for the sharing of information on existing and potential threats in real time. I point towards the submission to this process of the Forum of Incident Response and Security Teams (FIRST) as one such example. We look forward to an opportunity to hear them speak about that in due course.