Threats – UK statement

Chair, 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.
Hostile activity against critical national infrastructure and government will always be one of States' key concerns. Over the last 12 months the UKs National Cyber security Centre dealt with 777 significant incidents– up from 723 the previous year – with around 20% of organisations supported linked to the health sector and vaccines.

The real-world impact of such activity has been heightened as we have seen healthcare and public services disrupted, and food and energy supplies affected. Where we once focussed primarily on the threat to governments and defence, we must now recognise the real-world impact of irresponsible activity on broader economy and society. That change must be matched in our response.

The increasing scale and severity of ransomware attacks is one element which heightens the risk to essential services or critical national infrastructure. In the UK, education has been among the top sectors targeted, we have seen local Councils suffer significant disruption to public services, whilst a ransomware attempt against the University of Oxford's Covid-19 vaccine researchers had the potential to cause significant disruption to the UK's pandemic response. Such malicious activity affects not only our governments but our peoples.

International cooperation against cybercrime is the focus of another UN process, which we must not duplicate. But this activity highlights the need to urgently focus on implementation on existing norms which hold solutions to parts of this challenge. In particular those addressing critical national infrastructure are key here, as are those related to 'reasonable steps' a State may take to address malicious activity emanating from within their territory.

This OEWG can and should ensure that coordinated capacity building serves as a force multiplier in the fight to minimize the ransomware threat, whilst also offering a response to states whenever they do not address the activities of cybercriminals within their territory.

In the last 12 months, the compromise of the software company SolarWinds and the exploitation of Microsoft Exchange Servers have again highlighted the threat from supply chain attacks. The UK considers these intrusions targeting less-secure elements in the supply chain of economic, government and national security institutions extremely serious. The national security interest of States is not served by reckless use of capabilities which, in the case of Microsoft Exchange Server left tens of thousands of organisations of no national security interest needlessly and disproportionately impacted in the US alone.

And we are further concerned by the increase in the use of ICTs in ways that are not in line with States human rights commitments. We will propose concrete actions on this issue under the upcoming norms discussion.

Supporting States to develop the capacities and structures required at the national level to prevent, detect and respond to threats is a crucial element of this OEWG's work. Alongside facilitating this through supporting needs assessments and the development of national strategies, the UK will also address the issue of incident management processes.

Finally chair, we note the inclusion of data security in the group’s mandate. This is not a term the UK uses or fully understands, so we will listen carefully to what our Chinese colleagues have to say before we respond on this topic.