Madam Chair, thank you for your questions. The UK’s position is that this chapter should encourage States to share their best practice and policies for the prevention of cybercrime. The best approaches will be those that are gender sensitive and which recognise the important role of non-government actors in these efforts.

On question 32, the UK submission proposed specific reference to online gender based violence, and we consider the chapter on preventive measures should specifically recognise the disproportionate impacts of cybercrime on women and girls, and children. Although cybercrime can affect all elements of society, some types of cybercrime affect some groups more than others.

We have already spoken in this Committee about child sexual abuse material and the action we need to take. Another example is the non-consensual sharing of intimate images. This wicked crime does affect men as well as women. But, according to data from the UK’s Revenge Porn Telephone Helpline, between 2015 and 2020, for every one male victim who lodged a report, 67 women also lodged reports.

The UK believes that understanding the gender dimensions of some of these cybercrimes is at the heart of responding to them, and preventing them from happening in the first place. Prevention efforts should take the experiences of these groups into account, in order to create interventions that will maximise our ability to reduce this type of offending.

On question 33, member states are of course free to take action to make their critical infrastructure more resilient to cyber-attacks. However, the UK agrees with the distinguished delegate from Singapore and many others that this topic is outside the scope of our Convention, which is fundamentally a criminal justice instrument.

On question 34, the UK support measures that raise awareness and knowledge of steps that can be taken to address the broader issue of cyber resilience. We see three key aspects to this. First, the nature of the risk needs to be understood. Second, action needs to be taken to ensure that systems are as secure as possible to prevent and resist cyber crime. Third, recognising some cyber crimes will still happen, States need to encourage potential victims to be resilient enough to minimise their impact and be able to recover.
We do not believe the Convention should designate the areas where cooperative preventive measures are required. States should be able to decide which areas make most sense in response to their own circumstances. Such cooperation can happen in many different areas. Resilience is a shared endeavour between the government and all parts of society. This is the approach to cyber resilience taken by the UK, which we think works well. To ensure the greatest success, the convention should encourage and promote good practices in cooperative working between government, law enforcement agencies, academia, civil society and the private sector.

On question 35, the UK does not believe that the convention should stipulate which national authority should be responsible for preventing cybercrime. States know best what will work for them. Being too prescriptive will only slow down and increase costs to States when we come to implement this treaty.

On question 36, the Convention could include a provision that calls on States to encourage private sector organisations within their jurisdiction to employ risk-based approaches to improve their resilience and to detect, respond to and recover from the offences in this Convention. This Convention should not purport to create responsibilities or obligations for the private sector.

On question 37, the convention should encourage States to do more to promote, and raise awareness of, the sorts of practical steps that can make a real difference to prevent cybercrimes from occurring. These efforts must draw on the expertise of and access to the public that non-state actors including business, academia and civil society have. Awareness raising, and more specifically, behavior-change campaigns are nothing new – much is known about what works and what does not. Up to date evidence and best practice approaches should inform our efforts to help keep people and businesses safe from cybercrime.