

U.S. Remarks on Criminalization Chapter

Thank you very much to the Chair for these able compilations which highlight the strong commonality of proposals. We are pleased to see nearly universal consensus on the need to criminalize core cyber-dependent crimes like illegal access and data interference.

We would like to see the Committee reach agreement on the cyber-dependent crimes we will include in this chapter before we turn to the more complicated discussion of whether to also include cyber-enabled crimes. This seems like an achievable goal based on the submissions and comments so far.

The United States supports including some discrete cyber-enabled crimes in this treaty if that is where consensus leads us, where the use of the computer significantly increases the scale, scope and speed of the offense and which are not being addressed in other fora. We recommended some of these cyber-enabled crimes in our own submission, based on our own experience with cybercrime trends and the needs of cybercrime prosecutors. We look forward to feedback to our proposals and further discussion about the ideas of others.

As we begin to deliberate on the offenses to set forth in this treaty, we must be careful not to treat traditional crimes as a “cybercrime” merely because a computer was involved in their planning or execution.

We would also encourage Member States to think about how other chapters of this treaty might impact our approach to this one. If we use this treaty to empower countries to collect and share electronic evidence for any crime, subject to dual criminality as needed – which is what many have proposed in their submissions on procedural measures and law enforcement – we can focus the criminalization chapter just on the core cyber-dependent crimes repeated again and again in the national submissions as well as those limited cyber-enabled crimes that consensus determines are fundamentally changed by the use of a computer system, like computer-related offenses involving child sexual exploitation.

In this gathering, we are seeking to maintain the open, interoperable, secure and reliable internet while protecting it from cybercriminals who abuse it for their own gain. There are member states whose aim is the opposite. We must be clear eyed about proposals from the Russian Federation in particular – it has clearly demonstrated its wanton disregard for international law including the UN Charter in waging war against Ukraine and it continues to use cyberattacks to advance its

its dangerous and destabilizing foreign policy, including Moscow's territorial ambitions. Therefore, it is clear that it does not intend to negotiate in good faith. We will engage with other Member states to achieve a treaty of benefit to the global community.