United States remarks for March 2022 session of the OEWG, as prepared

On norms

- 2021 was a capstone year for the framework of responsible behavior in cyberspace. The GGE and OEWG produced robust reports and all UN member states committed to be guided by those reports. This consensus by UN member states represents a global political commitment to the framework.

- Over the course of two decades of negotiations, States recognized that existing international law provides a sufficient legal framework for state behavior in cyberspace. States also concluded that non-binding voluntary peacetime norms of state behavior and CBMs complement international law and complete the framework for responsible State behavior.

- The framework’s set of voluntary peacetime norms, in particular, have captured the international community’s attention.

- These non-legally binding norms serve to define a standard of behavior. When widely followed, they enhance cyber stability.

- Since the norms were first adopted and affirmed by consensus in UNGA in 2015, we have sought to deepen understanding of their purpose and encourage states to adhere to them – not just by supporting a resolution, but in their actions.

- The 2021 GGE report, in particular, provides meaningful new guidance on each of the existing norms.

- It has served us well to build on existing consensus and principles while deepening our shared understanding of that consensus.
• As we confront new and emerging threats, our existing norms can provide guidance.

• These norms were designed to be technology-neutral, broadly applicable, and flexible, and have so far proven to be sufficiently comprehensive to address emerging challenges.

• For example, recent concerns about election-related threats and threats to healthcare systems led the 2021 GGE to acknowledge that states may consider such systems as critical infrastructure, and therefore relevant to several GGE norms that address protections for critical infrastructure.

• Similarly, the relatively recent issue of ransomware incidents affecting critical infrastructure in a manner that could impact national security may be addressed in part through cooperation among states to address criminal use of ICTs as well as assistance in mitigating malicious ICT activity aimed at critical infrastructure. Related concerns about some states wittingly or unwittingly serving as safe havens for criminal actors may be addressed through reference to the existing norm admonishing states not to knowingly let their territories be used for internationally wrongful acts.

• However, there is room for the OEWG to provide more guidance on some of the norms. The 2021 OEWG report is silent on the topic of attribution, which is addressed in norm 13(b). In our view, the OEWG should provide additional guidance on this important topic, starting with acknowledging that States may choose to publicly attribute state-sponsored malicious cyber activity, or to share attribution conclusions through bilateral or multilateral channels.
• The group could also acknowledge that publicly attributing state-sponsored malicious cyber activities can shape expectations about what will not be tolerated and help build international consensus. We would also see value in acknowledging that when a state is in a position to attribute a particular cyber incident as an internationally wrongful act to another State, the victim State has all of the rights and remedies against the responsible State permitted to it under international law.

• The OEWG could also consider how capacity-building could improve States’ ability to attribute ICT incidents accurately.

• In addition, we believe the OEWG needs to address the issue of Internet Freedom.

• This issue has taken on new relevance this year, as we have seen numerous reports of Internet outages in Ukraine as Russia is engaging in its illegal war, which limits the people of Ukraine’s ability to receive and impart vital information. In addition, Russia’s censorship agency has blocked major social media platforms and news sites, and restricted access in Russia to international news outlets in order to mislead the Russian people and the world about what it is doing in Ukraine.

• Any further actions by Russia to shut off Internet access or to block international platforms will only further deny the Russian people access to information, show that Russia is doubling down on authoritarianism and repression domestically, and isolate Russia internationally.

• These repressive actions impede or prevent people from exercising freedoms of expression, peaceful assembly, and
association online. Such measures also disrupt access to essential services such as healthcare and emergency services.

- The United States believes that the OEWG should call upon governments worldwide to refrain from adopting or implementing laws and policies that may negatively affect the enjoyment of human rights online, including through Internet shutdowns.

- Blocking or degrading access to Internet resources cuts off connectivity for citizens, civil society, and human rights defenders in Ukraine, severing critical channels for sharing and learning information about the conflict online.