U.S. National Statement

Before I turn to our work this week, I first want to express our solidarity with the Ukrainian people. The United States stands resolutely with the government and people of Ukraine and condemns in the strongest terms Russia's premeditated, unprovoked, and unjustified attack on Ukraine. We call on Russia to cease its aggression against Ukraine and its flagrant violations of international law.

We gather here to build a meaningful tool for international cooperation against the scourge of cybercrime. From the outset of this process, we have sought to foster a spirit of consensus and cooperation—and we remain committed to working cooperatively with all Member States who are here to work in good faith toward a legally-binding international tool to combat cybercrime.

But the events of the last week have made it clear that the Russian Federation does not share our goals. The Russian Federation's invasion of Ukraine is, as Ambassador Thomas-Greenfield said last week, "tantamount to an attack on the UN."

As we sit here today, Russia appears to have aggressively used cyber, in addition to physical, means of attacking and destabilizing its neighbor. The Russian government's repeated violations of international law, including its ongoing invasion of Ukraine, make clear that Russia has no standing to negotiate in good faith toward a consensus instrument that helps the world combat malicious cyber activity.

The Russian Federation cannot present itself as a defender of the sovereignty of nations in these discussions while at this very moment it violates the sovereign territory of Ukraine. We can hardly address the Russian proposals for cooperation in this sphere while Russia continues

its audacious and illegal efforts in Ukraine. Until the current crisis in Ukraine is resolved peacefully, we will treat proposals by the Russian Federation with extreme skepticism as not being offered in good faith. Based on its unprovoked and unjustified attack on Ukraine, we can only assume that Russia's true goal in the ad hoc committee is to negotiate a legal instrument by which all other states abide but which it will ignore. We call on all member states to do the same and remain clear-eyed about the true motivations at play here.

Luckily, this process belongs to the whole of the United Nations membership, not merely the Russian Federation. We look forward to making progress with other Member States over the upcoming two weeks.

I would like to turn now to our thoughts on how we can move forward towards a fair and practical UN instrument that respects rights and all Member States can join. We believe an effective instrument should be grounded in existing best practices to provide immediate benefit to law enforcement. It must also protect human rights and preserve an open, interoperable, secure, and reliable internet.

As we all know, there are long-standing efforts to combat cybercrime already underway through existing international legal instruments, formal and informal cooperation, and robust capacity-building and technical assistance initiatives. These are critical efforts that we must preserve and promote, and the United States remains committed to strengthening and implementing our existing toolset.

Critically, a new instrument should be tailored to meet the actual challenges we face from cybercrime. The first and most important way to do that is through discerning and meaningful criminalization. The United States expects a UN cybercrime instrument, like all UN anti-crime

instruments, to call for domestic legislation to criminalize core conduct involving computers and provide procedural legal authority that permits law enforcement to preserve, collect, and share electronic evidence – consistent with due process guarantees, privacy interests, civil liberties, and human rights.

We would support an instrument that covers both cyber-dependent crimes, which target a computer or data, and a certain limited number of cyber-enabled crimes whose scope, speed, or scale are significantly increased due to the use of a computer. Though it is tempting to think of each new technology as novel and unique, we should be focusing on crimes committed with a computing device, whether a traditional "computer," mobile phone, or "Internet of Things" device. Member States should also be judicious in the breadth of cyber-enabled crime we seek to address. We should make sure the treaty captures essential cybercrime activities, and we should also be careful not to treat traditional crimes as a "cybercrime" merely because a computer was involved in their planning or execution. This is a complicated balance to strike and not one we should expect to resolve during this session. We look forward to further inputs from Member States and additional negotiations on the breadth of criminalization in future sessions.

We also expect this instrument to ensure appropriate domestic authorities which are necessary for investigating crimes in the modern era. A new instrument should call for the generally agreed procedural tools for electronic evidence: search and seizure, preservation, and real-time interception authorities. As with every UN anti-crime instrument, these tools should also include appropriate limits and safeguards to protect rights and prevent abuse. States need modern electronic evidence frameworks that are consistent with due process and human rights in order to effectively combat cybercrime and share evidence with international partners.

Sharing evidence with international partners is, of course, a core reason to build a UN cybercrime instrument. We expect the new instrument to provide tools to increase international cooperation, including through mutual legal assistance, extradition, and law enforcement cooperation. It should also allow for broad mutual legal assistance obtaining electronic evidence pertaining to a criminal offense regardless of whether the criminal offense was committed with a computer system. These provisions should include the appropriate safeguards and protections as we find in existing UN anti-crime instruments, which have been successfully implemented by the overwhelming majority of UN Member States.

Finally, the United States expects the UN cybercrime instrument to promote avenues for capacity-building and technical assistance, particularly for developing and less-developed countries. For most countries, international cooperation does not fail from lack of will but from limitations either in domestic law or in the expertise of law enforcement agencies. One of the most vital tools that a UN instrument can provide is additional resources for technical assistance.

There are two additional values that must guide us in this enterprise. One is humility: we must recognize that we do not know all there is to know about combating cybercrime and seek guidance from experts and other key stakeholders. This issue is too complex and multifaceted for governments to tackle it alone. The participation of multistakeholders can raise public awareness about the threats of cybercrime; ensure the work of Member States is undertaken in a transparent manner; and address substantive matters related to privacy, civil liberties, and human rights. An effective instrument also will depend on the contributions of experts in the field of combating cybercrime. We therefore welcome the Chair's proposals for regular consultations with multistakeholders to inform our negotiating sessions and the robust participation of multistakeholders in this process moving forward.

The second value that must guide our efforts is prudence: It is easy to get swept up in the newness and dynamism of cyber issues and all too tempting to address every trend or challenge now that we are gathered together. But we are tasked with a much more practical and discrete assignment: To provide criminal justice tools to our law enforcement who are facing a substantial and immediate threat from cybercrime. We can best meet the needs of law enforcement and fulfill our mandate by focusing on the criminal justice challenges of crimes committed with computers and expressly excluding from our work the broader and more politically sensitive debates about internet governance; security in cyberspace, including countering terrorism; and issues of cybersecurity. Valuable ongoing efforts on these other issues are being conducted in the UN and other intergovernmental and multistakeholder fora. It is important that we do not duplicate or undermine that focused work – both to avoid conflicts of obligations and so as not to detract from our objective to produce a targeted, practical instrument to fight cybercrime. Attempting to address every cyber-related issue in this criminal justice instrument risks miring these negotiations in unfocused and tangential debates that would do little to combat cybercrime and only slow our progress toward a useful instrument.

We welcome the Chair's proposal for a work plan that clearly outlines which chapters we will tackle in each session and solicits inputs from both Member States and multistakeholders in stages in line with that chapter schedule. We recognize that some states may have inputs of both texts or requested articles or elements to provide sooner, but we appreciate that the Chair's proposed work plan expects and encourages additional text and element contributions from Member States at later dates as we work through the chapter structure.