Joint Statement on Ransomware Attacks Against Healthcare Facilities

(The following is a joint statement delivered by the U.S. Deputy National Security Advisor Anne Neuberger, on behalf of Albania, Argentina, Australia, Austria, Bahrain, Belgium, Bulgaria, Canada, Colombia, Croatia, Costa Rica, Cyprus, the Czech Republic, Denmark, Dominican Republic, Ecuador, Estonia, the European Union, Finland, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Jordan, Latvia, Lithuania, Luxembourg, Malta, Morocco, the Netherlands, Norway, Philippines, Poland, Portugal, Republic of Korea, Republic of Moldova, Romania, Sierra Leone, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, Ukraine, Uruguay, the United Kingdom, the United States, Vanuatu, and Vietnam.)

Albania, Argentina, Australia, Austria, Bahrain, Belgium, Bulgaria, Canada, Colombia, Croatia, Costa Rica, Cyprus, the Czech Republic, Denmark, Dominican Republic, Ecuador, Estonia, the European Union, Finland, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Jordan, Latvia, Lithuania, Luxembourg, Malta, Morocco, the Netherlands, Norway, Philippines, Poland, Portugal, Republic of Korea, Republic of Moldova, Romania, Sierra Leone, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, Ukraine, Uruguay, the United Kingdom, Vanuatu, Vietnam and the United States are deeply concerned with the frequency, scale, and severity of ransomware attacks against critical infrastructure, in particular hospitals and other healthcare facilities.

These attacks pose direct threats to public safety and endanger human lives by delaying critical healthcare services, cause significant economic harm, and can pose a threat to international peace and security.

When hospitals and healthcare providers are targeted by ransomware attacks, the attacks have caused ambulances to be diverted, lifesaving surgeries to be halted, critical emergency care to be delayed, and blood donations to be suspended.

We must call on all Member States to collectively work together to strengthen the cybersecurity and resilience of our critical infrastructure and work to confront and disrupt the ransomware threat.

The General Assembly has repeatedly endorsed by consensus the UN framework of responsible state behavior in cyberspace, which makes clear that international law applies in cyberspace and that States are expected to uphold voluntary norms of State behavior during peacetime.

Consistent with relevant norms, States should not knowingly allow their territory to be used for internationally wrongful acts using Information and Communications Technologies (ICTs), which could include acts by ransomware actors operating within their jurisdiction.

States also should respond to appropriate requests to mitigate malicious cyber activity aimed at the critical infrastructure of another State that emanates from their territory.

When States act inconsistently with the framework, and knowingly allow ransomware actors to operate with impunity from their territories, responsible States should call out such irresponsible and destabilizing behavior and hold irresponsible actors to account.

The increasing threat of ransomware is detrimental to all of us.

Together with the international community, we will continue our work to uphold the international framework of responsible State behavior in cyberspace and address the ransomware threat comprehensively by pursuing ransomware actors, targeting the malicious software they use and its dissemination, countering the illicit finance that supports their activities, securing critical infrastructure, providing technical assistance, and, as appropriate, coordinating among nations.

We are deeply committed to fighting cybercrime and to building capacity of UN members to join this fight, including via the 68-member International Counter Ransomware Initiative.

Thank you.