CYBER AND DIGITAL SECURITY

1. We confirm our joint commitment to promoting an international stability framework for cyberspace based on the application of international law, agreed voluntary norms of responsible state behaviour, and confidence building measures, supported by co-ordinated capacity building programmes. We reaffirm that the UN Charter applies in its entirety to state actions in cyberspace. The law of state responsibility applies to cyber operations in peacetime, including the availability of the doctrine of countermeasures in response to international wrongful acts.

2. We recognise that an increasing number of states are developing operational cyber capabilities. We emphasise their obligation to ensure their use is governed in accordance with international law. This does not encourage aggression, or contradict our common commitment to maintaining a peaceful cyberspace environment, rather, it fosters the understanding that, just like in the physical domains, states' activities in cyberspace do not occur in a vacuum – states have rights – but they also have obligations.

3. To this end, we will:

    - Engage in a new annual policy **strategic dialogue** on cyber threats, bringing together Government and Agencies;

    - Continue to offer our cyber reserves and expertise to help build resilience within **NATO**, and commit to joint action on building a role for NATO in improving the cyber defence capability of Allies and Partners;

    - Develop a new bilateral cooperation framework for engagement with Private Sector **critical infrastructure** owners to implement resilient cyber security solutions for their products and services, focusing particularly on companies in which we have a shared interest;

    - Identify cross-sector CNI interdependencies and our most **critical assets, systems, and networks** as well as current and potential forums for collaboration on the security and resilience of such assets, including a bilateral exchange on risk and resilience;

    - Support a variety of approaches, such as security by design, risk management practices, market-relevant security assessment for consumer **Internet of Things** products and associated services, including by seeking alignment on recommendations and sharing best practices;

    - Work together to **raise the cost of malicious cyber activity** by criminals and state actors, including through promoting the use of the EU Cyber Tool box and coordinated messaging; and

- Explore closer collaboration on **Open Source and Open Source Intelligence** to inform domestic and international policy, including sanctions, cyber, and hybrid threats, such as disinformation and propaganda.