UN GENERAL ASSEMBLY, 80TH SESSION
FIRST COMMITTEE

THEMATIC DEBATE ON OTHER DISARMAMENT MEASURES

STATEMENT BY THE UNITED KINGDOM

New York, October 2025

Chair,

The UK reiterates the importance of maintaining a free, open, peaceful and secure cyberspace that enhances collective security and supports global development and economic growth.

This requires all states to uphold and implement the existing UN Framework for Responsible State Behaviour in Cyberspace and existing international law, including the UN Charter, the Law of State Responsibility, international human rights law and international humanitarian law.

Cyber operations are deployed in conflicts with real-world impacts on civilians and critical infrastructure. In Ukraine, Russia's campaign of aggression includes attempts to target Critical National Infrastructure and vital public services. This is part of a wider campaign of irresponsible and indiscriminate cyber-attacks, intent on causing destruction and harm. The UK remains concerned by the growing irresponsible use of cyber capabilities by certain states and state backed groups.

The Open-Ended Working Group on ICTs concluded its mandate this year, submitting its final report to the General Assembly, in which all states agreed to establish a UN Global Mechanism on international cyber security. We look forward to engaging actively in the next steps.

In April 2025, the UK and France launched a Code of Practice for States under the multistakeholder Pall Mall Process, to guide the responsible development, transfer, and use of advanced cyber intrusion tools. We urge all States to engage in good faith and align national practices with the Code's principles.

The integration of AI in the military domain will transform global security dynamics. We should approach adoption safely, responsibly and in compliance with international law.

The Secretary General's report on AI in the military domain offers an opportunity to build collective understanding on AI's applications and implications - so we can make the most of the opportunities and address associated risks.

The UK commitment to secure and responsible AI in the military context is set out in our Defence AI Strategy and AI Ethics Principles. We work closely with international partners, including through our world-leading AI Security Institute, to ensure that the transformative power of AI is harnessed in a responsible way. We welcome the resolution proposed by the Netherlands and South Korea which we are pleased to co-sponsor, and their continued leadership in this area.

Threat awareness and cyber security capacity building are essential pillars of the consensus UN framework on responsible state behaviour in cyberspace. The UK remains committed to working inclusively with its partners, member states and relevant international organisations to promote responsible behaviour in the cyber domain.

* * *