

REPUBLIC OF KOREA-UK STRATEGIC CYBER PARTNERSHIP

STATEMENT OF INTENT

1. In line with the **2022 ROK-UK Bilateral Framework for Closer Cooperation** and the **2023 Downing Street Accord**, cooperation on cyber is an essential pillar of the Republic of Korea-UK relationship. The Governments of the Republic of Korea and the United Kingdom (hereinafter referred to as the “Participants”) are committed to a cyberspace environment that is open, free, peaceful and secure, adheres to international law and maximises opportunities for economic growth.
2. In the year of the 140th anniversary of diplomatic relations between the United Kingdom and Korea, the strategic direction of the Participants is to further deepen and fulfil the potential of our vibrant, modern relationship in the cyber domain.
3. As agreed by their leaders on 22 November 2023, the Participants hereby strengthen their cyber cooperation to form a Strategic Cyber Partnership.
4. The Participants reaffirm the benefits of close collaboration, including on information sharing, developing technical standards, international law and norms, protecting critical national infrastructure, and the development and deployment of cyber and core technologies.
5. The Participants will use their available capabilities to deter the full range of cyber threats facing the Republic of Korea and the United Kingdom.

SCOPE

6. The Republic of Korea-UK Strategic Cyber Partnership (hereinafter referred to as the “Partnership”) will provide an adaptable framework to pursue our goals. The Partnership will serve to intensify co-operation and delivery around shared opportunities and challenges with respect to cyberspace. It may support other specific bilateral initiatives by mutual consent, in addition to providing strategic direction on existing collaboration.
7. The Partnership will be separate from, but complementary to, the ROK-UK Digital Partnership.
8. The framework will remain flexible in order to respond to any emerging issues relevant to the bilateral relationship. In the first instance, co-operation will be intensified around three pillars:
 - i. (Pillar 1) Strengthen our cyber ecosystems and resilience.
 - ii. (Pillar 2) Advance shared international interests.
 - iii. (Pillar 3) Detect, disrupt and deter malicious cyber threats.
9. In support of Pillar 1, the Participants will:
 - a. Build and develop ties between the government, private sector, and academia to improve cyber resilience, including through seeking to enrol South Korean companies in the UK NCSC’s Industry 100 programme.
 - b. Encourage bilateral industry partnerships and endeavour to enable market access opportunities for the Participants’ cybersecurity products and services.
 - c. Cooperate in the research and development of core technologies to protect critical national infrastructure.

- d. Continue to share best practice on approaches to the cyber security of smart city (connected place) technologies.
- e. Actively participate in cyber exercises hosted by the Republic of Korea and the United Kingdom to enhance cybersecurity capabilities, including Exercise Defence Cyber Marvel 3 to be organised by the British Army Cyber Association in February 2024, Cyber Conflict Exercise to be organised by the National Intelligence Service in September 2024.
- f. Cooperate on making policy and institutional improvements for personnel training, e.g., cybersecurity expert exchanges and educational support.

10. In support of Pillar 2, the Participants will:

- a. Work together to promote responsible cyber behaviour in relevant multilateral and multi-stakeholder processes.
- b. Share information on the threats posed by commercial cyber proliferation.
- c. Seek to identify opportunities to work together on international cyber security capacity building initiatives.
- d. Work together to support an open, free, peaceful and secure cyberspace in relevant international fora.

11. In support of Pillar 3, the Participants will:

- a. Closely share information and actively cooperate to prepare policy measures to respond to malicious activities in cyberspace.
- b. Cooperate in developing and implementing a diverse set of tools to deter malicious cyber activities in cyberspace.
- c. Collaborate to advance joint efforts to work with partners in the Indo-Pacific region and beyond to deter malicious cyber activity.
- d. Work together to disrupt and deter DPRK malicious cyber capabilities and activities that contribute to its WMD programs. Concurrently seek to drive up the economic and reputational cost of DPRK cyber actors' operations. Cooperate to jointly respond to DPRK cyber-attacks and to other illicit DPRK cyber operations, including but not limited to revenue-generating activities.
- e. Establish a joint analysis group to mitigate international cyber threats, such as ransomware, commercial spyware.

MUTUAL SUPPORT

12. When either of the Participants faces destructive, disruptive or otherwise destabilising malicious cyber incidents, the Participants intend to cooperate through official channels to share information and provide support.

GOVERNANCE

13. The Partnership will be governed through regular discussions between the ROK National Security Office (NSO) and the UK National Security Secretariat (NSS), with input from other relevant governmental departments where required, to advance the full spectrum of cyber co-operation.

14. To support the discussions between NSO and NSS, the ROK-UK Cyber Dialogue will continue to be co-chaired by principals in the Republic of Korea Ministry of Foreign Affairs (MOFA) and the UK Foreign, Commonwealth and Development Office (FCDO) with the participation of other respective departments and agencies with relevant policy interests. The Cyber Dialogue will continue to be convened annually, or as otherwise decided by MOFA and the FCDO.

15. Between formal meetings, activity will be led on a day-to-day basis by officials in respective governments, in line with routine policy ownership and collaboration.

PLAN OF ACTION

16. The Partnership will be supplemented by an underlying Action Plan. The Action Plan will detail the practical areas of cooperation and collaboration that the Participants will aim to pursue within the first 2 years of the Partnership. The Action Plan will be updated by way of mutual consent between the Participants on an as needs basis.

NON-BINDING

17. This document only serves as a record for the Participants' intentions and does not constitute and is not intended to create any legally binding obligations under domestic or international law and will not be deemed to constitute or create any legally binding obligations or enforceable obligation, express or implied.

Prime Minister Rishi Sunak

President Yoon Suk Yeol