

**STRATEGIC CYBERSECURITY COOPERATION FRAMEWORK
BETWEEN THE REPUBLIC OF KOREA
AND THE UNITED STATES OF AMERICA**

In commemoration of the 70th anniversary of the United States (U.S.) and the Republic of Korea (ROK) Alliance, we intend to make robust and resilient national cybersecurity a high policy and strategic priority, including responding to the upsurge in national security threats while contributing to peace and prosperity in cyberspace.

Recognizing the depth and robustness of the longstanding strategic alliance between the Republic of Korea and the United States of America, and the importance of continuing that in cyberspace;

Sharing in the vision that the Republic of Korea and the United States of America intend to defend national security and respect for our common values, including liberal democracy, while contributing to economic prosperity in cyberspace;

Underscoring the importance of promoting an open, interoperable, secure, and reliable Internet and a stable cyberspace;

Reaffirming our intent to respect our obligations under international law, including the UN Charter, international humanitarian law, and international human rights law, in conducting activities in cyberspace, and to respect and promote established voluntary norms of responsible peacetime state behavior in cyberspace;

Recognizing the alliance applies to cyberspace, the United States and the Republic of Korea intend to begin discussions regarding how the Mutual Defense Treaty would apply and under what circumstances;

Reaffirming our commitment to work together on a voluntary basis to hold states accountable when they act contrary to the framework of responsible peacetime state behavior in cyberspace, including by taking measures that are transparent and consistent with international law. We also reaffirm the applicability of international law to peacetime state behavior in cyberspace, respect for internationally recognized voluntary norms of responsible peacetime state behavior, and the development and implementation of confidence building measures;

Reaffirming the commitment to deepen bilateral cooperation on regional and international cyber policy, including cooperation on deterring malicious cyber activity, improving the cybersecurity of critical infrastructure, combatting cybercrime and associated money laundering, securing cryptocurrency and blockchain applications, capacity building, cyber exercises, information sharing, military-to-military cyber cooperation, and other international security issues in cyberspace, as stated in the Joint Statement during the U.S.-ROK Summit of May 2022; and

Recognizing the benefits of close-knit cooperation and coordination in the areas of intelligence sharing, implementation of laws, development of core cybersecurity

technologies, partnership with the private sector, and raising of specialized cybersecurity talent.

AREAS OF CYBERSECURITY COOPERATION

The Republic of Korea and the United States of America intend to extend our robust cooperation to cyberspace. In this regard, the United States and the ROK intend to promote cooperation and build trust in cybersecurity technology, policy, and strategy, including the sharing of intelligence. Each country intends to further develop its capabilities to assist national authorities in protecting critical infrastructure, such as the energy and financial services sector, including preparing to defend against malicious cyber activities. Both countries intend to make every effort to enhance stability in cyberspace and reduce the risk of misunderstanding, miscalculation, and conflict through compliance with their respective obligations under international law and by respecting and promoting the internationally recognized voluntary norms of responsible peacetime state behavior in cyberspace. The United States and the ROK intend to cooperate/affirm their cooperation in the following areas and other areas as mutually coordinated:

1. To cooperate in developing and implementing a diverse set of tools, including defensive and threat mitigation measures, to deny and deter malicious actors operating in cyberspace.
2. To continue to share information from diverse sources and cooperate to detect, deter, and disrupt malicious activities in cyberspace, including but not limited to money laundering and cryptocurrency theft.
3. To collaborate in international forums, including the United Nations, and with allies and partners to promote the framework for responsible peacetime state behavior in cyberspace that consists of international law, voluntary and non-binding norms, and confidence building measures, and hold accountable irresponsible states that engage in disruptive, destructive, or otherwise destabilizing activity in cyberspace.
4. To actively participate in cyber exercises hosted by the United States and the ROK to enhance cybersecurity capabilities, and cooperate in the research and development of core technologies to protect critical national infrastructure.
5. To cooperate on making policy and institutional improvements for personnel training, e.g., cybersecurity expert exchanges and educational support, and enhancing the cooperation between private sectors.
6. To build and further develop existing ties between the government, private sector, and academia to foster cyber resilience in areas including, but not limited to cybersecurity incident management, and the sharing of cyber threat information in real time.
7. To enhance cooperation in cyber capacity building to facilitate all states having the necessary capacity to promote an open, interoperable, reliable, and secure internet and a stable cyberspace, including the framework for responsible peacetime state behavior in cyberspace.

PRINCIPLES FOR COOPERATION

The United States and the ROK intend to actively cooperate on the following to respond to malicious cyber activities that undermine global peace and security based on mutual trust:

1. Use available capabilities to deter, deny, defend, and respond to the full range of cyber threats, including through political, diplomatic, economic, law enforcement, military, and technical means;
2. Continue sharing information regarding malicious cyber activities, exchange national approaches and response measures, and enhance possible mechanisms for cooperation in order to counter state and non-state actors conducting malicious cyber activities; and
3. Carry out coordinated action and/or parallel response measures, as appropriate, through close bilateral consultation and information sharing in the event of a significant cyber incident affecting the national interests, or critical infrastructure of the United States, the ROK, and/or other partners.

MECHANISMS FOR COOPERATION

1. As close partners on cyber issues, the United States and the ROK have multiple channels and mechanisms for coordination and cooperation at various levels. Both countries intend to continue to coordinate on cybersecurity activities through multiple mechanisms, including the channel between the U.S. National Security Council and the ROK National Security Office, the U.S.-ROK Cyber Dialogue, the U.S.-ROK Working Group on DPRK Cyber Threats, the U.S.-ROK Cyber Cooperation Working Group, and other interagency mechanisms to include cyber-related working groups led by law enforcement or intelligence agencies, to confront a range of cyber threats from various actors.
2. Both countries also intend to continue sharing technical and operational cyber threat information, cooperate on cyber incidents of mutual interest as appropriate, exchange best practices in cyber crisis management, and mutually participate in practice, research, and training through the U.S. Cybersecurity and Infrastructure Security Agency's Joint Cyber Defense Collaborative (JCDC), as well as other parts of CISA and the ROK National Intelligence Service (NIS), Korea Internet & Security Agency (KISA) CERT, ROK National Cyber Security Center (NCSC) and the National Cyber Risk Management Unit (NCRMU).

DISCLAIMER OF LEGAL EFFECT

This Strategic Cybersecurity Cooperation Framework is not intended to give rise to rights or obligations under international or domestic law.

President Joseph R. Biden

President Yoon Suk Yeol