Abstract

The Biden Administration's Cyber Security Policies and Implications: Focusing on Cyber Deterrence

Il-Seok Oh

(Institute for National Security Strategy)

The Biden administration faces critical cyber security challenges posed by various cyber attacks, including the SolarWinds hack, the 2021 Colonial Pipeline ransomware attack, and cyber crimes associated with the 2022 Russia-Ukraine War. In response to such attacks, the Biden administration declared "America is Back" and strived to strengthen liberal democratic values and secure competitiveness in cyberspace by implementing aggressive cyber security policies and retaliatory deterrence strategies.

Washington aims to enhance its cyber "deterrence by denial" strategy by establishing cyber security governance, advancing supply chain security, realigning cyber security agencies and activities, and improving legislation. The Biden administration also pursues various policies related to "deterrence by retaliation" through summits and diplomatic efforts, criticisms and warnings against adversaries, cyber economic sanctions, export controls, law enforcement, military intelligence sharing and joint exercises, and preemptive responses based on norms. The administration will also likely enhance its attribution capabilities, as cyber attribution is a prerequisite to concrete steps for deterrence by retaliation. Hence, the U.S., under its "defend forward" strategy, will likely conduct cyber attributions and carry out deterrence by retaliation measures in the form of kinetic attacks or cyber operations against China, Russia, Iran, or North Korea, if necessary.

The South Korean government needs to establish a national cyber strategy that strikes a balance between deterrence by denial and deterrence by retaliation, and propose concrete countermeasures. Furthermore, the

government should modify specific laws and regulations to support deterrence by retaliation measures, including cyber economic sanctions, condemnation statements and international recommendations, export controls, joint cyber military exercises, and law enforcement.

Keywords

cyber deterrence, deterrence by denial,
deterrence by retaliation, economic sanctions, condemnation statements, export control, defend forward, attribution