# Integrating information warfare into U.S.-ROK defense strategy

**By Michael Raska**

For 60 years, South Korea's defense strategy has remained relatively constant — maintaining deterrence and robust defense posture in order to prevent another major outbreak of war on the Korean Peninsula. Its three mutually reinforcing strategic pillars — defensive deterrence, the U.S.-ROK (Republic of Korea) alliance and forward active defense — have defined the baseline of South Korea's national security, the structure of its forces and its operational conduct.

However, in the last decade, South Korea's security dilemmas have become progressively more "hybrid" and multifaceted. Traditional conventional threats, scenarios and contingencies linked to high intensity conventional wars vis-à-vis North Korea, have been converging with a range of asymmetric and nonlinear security challenges, including nuclear threats, ballistic missiles and also information and cyberwarfare.

According to Gen. James Thurman, the commander of U.S. forces in South Korea, North Korea has acquired "significant" IW-related military capabilities. Notwithstanding its continuing political, socio-economic and technological isolation, North Korea's military has shifted its focus toward asymmetric negation, probing any vulnerabilities of the U.S.-ROK alliance in order to counter its qualitative technological and military advantages.

In addition to its nuclear and ballistic missile programs, these also include hacking, encryption and virus insertion capabilities. These can be used in the many crisis scenarios that the U.S.-ROK alliance currently trains for: from a full-scale conventional war to low-intensity conflicts, asymmetric scenarios and other nonlinear contingencies.

Indeed, both North and South Korea engage in three information conflicts simultaneously — a war for information to obtain information and intelligence about each other's means, capabilities and strategies; a war against information aimed at protecting their information systems, while disrupting or destroying the other side's information infrastructure; and a war through information reflected in the misinformation and deception operations to shape their broader internal and external strategic narratives.

In the first category of war for information, for example, the South Korean National Intelligence Service and the Defense Security Command reported in 2009 that a suspected North Korean hacker unit (Unit 110) operating under the North Korean Army General Staff's Reconnaissance Bureau intercepted confidential defense strategy plans, including OPLAN 5027 detailing U.S.-ROK responses to potential North Korean provocations.

The incident happened as an officer with the ROK-U.S. Combined Forces Command used an unsecured USB memory stick plugged into his PC while switching from a highly secure private intranet to the public Internet.

Michael Raska

While the OPLAN 5027 is currently under review (OPLAN 5015) with the ROK military planning to take over the war time operational control from the United States Forces Korea in 2015, its compromise may raise a question as to what extent could North Korea access and potentially disrupt selected U.S.-ROK operational plans in times of war or crisis, including ROK Army mobilization, U.S. Noncombatant Evacuation Operations, and essentially the staging, onward movement, and synchronization of deep, close and rear defenses.

In the same year, North Korean hackers reportedly stole information from the South Korean Chemical Accidents Response Information System developed by the National Institute of Environmental Research under the Ministry of Environment after infiltrating the ROK Third Army headquarters' computer network and using a password to access CARIS' Center for Chemical Safety Management.

In the category of war against information, North Korea has attempted to disrupt South Korea's highly developed digital information infrastructure using cyberattacks to shut down major websites, disrupt online services of major banks, and probe South Korea's readiness to mitigate cyberattacks.

Most cited cases in this tier include the 2009 distributed denial-of-service attacks against four dozen targets in South Korea and the United States and the 2011 DDoS attacks targeting South Korean government websites as well as the network of the U.S. Forces Korea for 10 days — a.k.a. the "10 Days of Rain."

According to analysis by McAfee Labs, the combination of clearly defined targets, highly destructive malware code, multiple encryption algorithms, and multi-tiered botnet architecture preconfigured for specific duration, has led to a conclusion that the attack was set up by North Korea to test and observe how rapidly the attack would be discovered, reverse engineered, and mitigated. At the end of the "10 Days of Rain" DDoS attacks, the botnets were configured to self-destruct.

Finally, in the category of war through information, North Korea has relied on information warfare to alter the perceptions of its strategic plans. For example, prior to its recent rocket launch in December 2012 and subsequent nuclear test in February 2013, North Korea manipulated news stories as part of a deliberate deception campaign to hide its real intentions.

In the case of the rocket launch, Pyongyang announced several days beforehand that there were technical problems with the rocket. At that time, U.S. satellites observed the North Koreans taking apart the three-stage rocket, and moving the parts away from the launch pad. North Korea, however, launched the rocket without any delay, catching U.S.-ROK military and intelligence agencies off guard. Subsequent reports indicate that North Korea manipulated the launch so that U.S. intelligence satellites would not be overhead.

Following the sinking of the Cheonan warship and subsequent shelling of Yeonpyeongdo Island in 2010, the South Korean military has established a psy-ops unit to diffuse news and information into North Korea — whether through radio transmissions, balloon leaflets, DVDs and possibly USB memory sticks. Since then, it has sent thousands of leaflets and transmitted broadcast into North Korea using mobile broadcast vehicles and six relay stations. South Korea has also established a new cyberwarfare command designed to counter North Korean cyberthreats.

With changing strategic realities on the Korean Peninsula, however, information warfare will have greater ramifications for the U.S.-ROK defense strategy. In order for the U.S.-ROK alliance to effectively cope with the emerging information war threats, while leveraging its strategic opportunities, the alliance should therefore intensify its efforts in conceptualizing, planning and integrating information warfare into joint U.S.-ROK defense planning, training and operations.

In this context, South Korea should devise a new defense strategy that allows greater flexibility and adaptability to shifts in strategic environment and with military forces having the flexibility and robustness to operate in divergent scenarios. This means pursuing military innovation and breaking away from South Korea's long-standing, static, defensive posture emphasizing conflict and war avoidance, path dependence and overreliance on the U.S.

---

*Michael Raska is a research fellow at the Institute of Defense and Strategic Studies, a constituent unit of the S. Rajaratnam School of International Studies, Nanyang Technological University, in Singapore.*