RINSA FORUM
Korea National Defense University
Research Institute for National Security Affairs
http://rinsa.kndu.ac.kr, http://www.kudu.mnd.mil
vol. 93 | 2024. 08. 31.

The Russia-DPRK Summit and ROK-US Security Cooperation

Jihwan Hwang
Professor, Department of International Relations, University of Seoul

I. Russia–DPRK Treaty on Comprehensive Strategic Partnership

The "Treaty on Comprehensive Strategic Partnership" signed by North Korea and Russia on June 19th represents a significant threat with profound implications for the security environment on the Korean Peninsula. Kim Jong Un has asserted that this treaty elevates the Russia-DPRK relationship to "a new higher level of alliance." A key element of the treaty is Article 4, which stipulates that if either party is subjected to a state of war due to an armed invasion by one or more states, the other party shall provide military and other assistance without delay, utilizing all means at its disposal. This provision aligns with the laws of the DPRK and the Russian Federation and Article 51 of the UN Charter, which recognizes the inherent right of individual or collective self-defense if a member of the United Nations is attacked.

While Article 4 assumes a state of war, Article 3 implies security cooperation measures in times of crisis. If a direct threat of armed invasion arises against either

party, both sides shall immediately activate bilateral negotiation channels. This is to adjust their positions and discuss feasible, practical measures to ensure mutual assistance in eliminating the prevailing threat, upon the request of either side. Articles 5 and 6 of the treaty reflect North Korea's recent external security environment. Article 5 stipulates that each party is obligated not to conclude any agreements with third countries that would encroach upon the other party's sovereignty, security, territorial integrity, or rights to freely choose and develop their political, social, economic, and cultural systems, as well as other core interests. They also agree not to participate in such actions. Article 6 states that both parties will actively cooperate to implement policies aimed at establishing a just and multipolar new world order. This aligns with North Korea's stance on the "new Cold War" and the "multipolar" order, indicating a move towards creating a new multipolar world order that includes the rising influence of Russia and China.

Articles 7 and 8 are particularly significant at a time when Russia-DPRK security cooperation is increasing. Article 7 stipulates that, with the aim of maintaining international peace and security, the two sides shall discuss and cooperate on global and regional developments that could pose a direct or indirect challenge to their common interests and security. This cooperation will take place within the framework of international bodies, including the UN and its specialized agencies. Article 7 also covers security cooperation measures during peacetime within international organizations, including the UN, and is interpreted to encompass all actions within the UN Security Council, including the lifting or reduction of economic sanctions against North Korea.

Article 8 is one of the most important provisions for North Korea's effort to build up its military capability. It stipulates that both sides shall establish mechanisms for taking joint measures aimed at strengthening defense capabilities to prevent war and ensure regional and global peace and security. This suggests that joint military-industrial cooperation between North Korea and Russia is likely to accelerate in the future. Notably, North Korea reportedly received Russian assistance in launching a military reconnaissance satellite in November of last year. This satellite launch can be seen as an effort to overcome North Korea's previously significant disadvantage in military intelligence.

If defense cooperation between the two countries expands, Russia will play a key role not only in reconnaissance satellites but also in various aspects of North Korea's defense industry development. After the summit between Kim Jong Un and Vladimir Putin, the possibility of Russia providing precision-guided weapons was mentioned. From North Korea's perspective, Russian air defense systems could be of utmost importance. Should Russia provide advanced air defense systems like the S-400 to North Korea, or offer technological and military support for North Korea's air defense network, it could significantly impact the security environment on the Korean Peninsula. In addition to the S-400, other Russian air defense systems of interest to North Korea might include the Buk (medium-range) and the Tor or Pantsir (short-range).

However, given Russia's ongoing war with Ukraine, there are doubts about its ability to provide such systems directly to North Korea, and questions have been raised about the performance and responsiveness of Russia's air defense capabilities. Nevertheless, there remains a significant possibility that Russia could offer technical support or components for North Korea's own air defense network. Additionally, North Korea is likely to be interested in Russian strategic submarine technology and new fighter aircraft.

II. The Future of Russia–DPRK Security Cooperation

There are several considerations regarding the long-term effects and functions of the security alliance between Russia and North Korea. First, it is uncertain whether the treaty will remain effective after the end of the Ukraine War. Historically, the Russia-DPRK relationship has experienced significant fluctuations depending on changes in the international situation, as demonstrated in the early 1990s. The new treaty specifies in Article 22 that "the Treaty on Friendship, Good-Neighborliness, and Cooperation between the Democratic People's Republic of Korea and the Russian Federation, adopted on February 9, 2000, shall be terminated from the date this treaty comes into effect." The "Treaty of Friendship, Cooperation, and Mutual Assistance" signed by North Korea and the Soviet Union in 1961 included a provision for automatic military intervention in similar situations, which was officially abolished in 1996. The 2000 treaty, on the other hand, only included provisions for immediate contact in such situations. Just as the 2000 treaty reflected the relationship between the two countries after the dissolution of the Soviet Union in 1991, the new treaty reflects the relationship between the two countries after the Ukraine war.

For the new security alliance to endure beyond the Ukraine War, a significant level of alliance institutionalization would be required. Currently, there is a lack of institutionalization comparable to that seen in the ROK-US alliance treaty. In this context, the Russia-DPRK treaty includes various efforts aimed at institutionalizing the bilateral security relationship.

Articles 9 through 21 of the treaty address cooperation across diverse areas such as the economy, society, technology, and law. It is evident that over two-thirds of the treaty's content focuses on non-traditional security areas, reflecting efforts to ensure its practicality and sustainability. The bilateral relationship has experienced instability over the past 30 years, influenced by the changing conditions and needs of each country. Since the early 1990s, Russia has been relatively passive regarding Korean Peninsula issues. On the North Korean nuclear issue, Russia has often acted as a veto-wielding state rather than an active mediator. Although the war in Ukraine has significantly reshaped the relationship between the two countries, it remains uncertain whether their close ties will persist after the conflict ends. In this light, North Korea appears to be leveraging the treaty to institutionalize its relationship with Russia.

The future of the North Korea-Russia relationship may not be as promising as it initially seems, mirroring the evolving dynamics between North Korea and China. The noticeable improvement in China-DPRK relations began after Kim Jong Un held five summits with Xi Jinping, following Kim's meeting with U.S. President Trump in 2018. Before 2018, under Xi Jinping's leadership, no such summits had taken place. Relations between North Korea and China had been strained after North Korea's third nuclear test in 2013, particularly due to UN Security Council sanctions against North Korea, which China chose not to veto. Recent reports of tensions in China-DPRK relations underscore the instability in North Korea's foreign relations. This raises questions about whether the new treaty between North Korea and Russia would have been concluded without the Ukraine war. Additionally, the treaty's effectiveness in the future remains uncertain, especially considering that President Putin, who turns 72 this year, may not remain in power indefinitely. Excluding the impact of the Ukraine war, the structural basis of the bilateral relationship between North Korea and Russia appears quite fragile.

In fact, Kim Jong Un seems to be leveraging the Russia card to draw China into an anti-U.S. alliance on the Korean Peninsula. Kim has repeatedly emphasized the establishment of a new Cold War order and a multipolar system, seeking to create a new security environment on the Peninsula with a North Korea-China-Russia bloc countering the U.S.-South Korea-Japan security cooperation. Article 6 of the new Russia-DPRK treaty also aims at establishing a multipolar world order. Therefore, it appears more accurate to view the treaty as part of North Korea's long-term strategy to involve China through its alliance with Russia, rather than as an attempt to isolate China. While the provision for military assistance in Article 4 of the treaty is significant, it is crucial to consider the broader changes in the global order and the structural aspects of the bilateral relationship when assessing the treaty's implications. Additionally, potential changes in the security environment on the Korean Peninsula following the U.S. presidential election in November should also be closely monitored.

III. ROK–US Alliance Response and the Future of the Korean Peninsula

The Russia-DPRK alliance treaty is likely to negatively impact the security of the Korean Peninsula by fostering enhanced military cooperation between the two countries and bolstering North Korea's military capabilities. Currently, the ongoing war in Ukraine limits South Korea's ability to effectively counteract Russia-DPRK military cooperation. However, in the long term, it is essential to strengthen defense and security diplomacy to counterbalance and mitigate the effects of the Russia-DPRK security partnership. On the other hand, reinforcing military cooperation within the ROK-US alliance is crucial. Continued efforts to enhance U.S. extended deterrence, as outlined in the Washington Declaration and the U.S.-ROK Guidelines for Nuclear Deterrence and Nuclear Operations on the Korean Peninsula (Guidelines document), are vital. Additionally, improving crisis management capabilities is essential to prevent accidental incidents and ensure stability on the Korean Peninsula.

Most notably, the Washington Declaration from last year and the Guidelines document agreed upon by the United States and South Korea have significant implications for enhancing the credibility of U.S. extended deterrence on the Korean Peninsula. The Guidelines document, finalized during the recent ROK-US summit, aims to further specify and institutionalize the Washington Declaration, seeking to strengthen U.S. extended deterrence in response to recent developments in North Korea's nuclear capabilities and the new treaty between Russia and North Korea. Although the Guidelines document has not been publicly released, it is believed that its core content refines and institutionalizes the conventional-nuclear integration (CNI) outlined in the Washington Declaration.

The Washington Declaration established a new Nuclear Consultative Group (NCG) to bolster extended deterrence and enhance the visibility of strategic assets on the Korean Peninsula, including the visit of a U.S. nuclear ballistic missile submarine to South Korea. Additionally, the ROK-US alliance will work on enabling joint execution and planning for South Korea's conventional support to U.S. nuclear operations in a contingency. The Guidelines document underscores

that the NCG has significantly strengthened ROK-US cooperation on extended deterrence and facilitated joint U.S.-ROK nuclear and strategic planning in response to North Korea's advancing nuclear threat. The NCG has played a crucial role in enabling joint planning and execution for South Korea's conventional support to U.S. nuclear operations in a contingency. Specifically, the Guidelines document highlights the importance of a solid foundation for enhancing ROK-US extended deterrence cooperation in an integrated manner, providing guidance to alliance policy and military authorities to maintain and strengthen a credible and effective nuclear deterrence policy and posture.

However, the issue of defining South Korea's role in nuclear and strategic planning under CNI remains unresolved. The joint statement on the Guidelines document defines CNI as "South Korean conventional support for U.S. nuclear operations during contingencies through the integration of U.S. nuclear and conventional forces." As a component of 'integrated deterrence,' CNI is presumed to include various elements such as nuclear consulting, nuclear planning, and nuclear implementation. This process will need to advance the institutionalization of U.S. extended deterrence.

Vipin Narang, former Acting Assistant Secretary of Defense for Space Policy, recently assessed in an interview that the role of the ROK-US Nuclear Consultative Group has evolved and become more institutionalized in response to North Korea's advancements in nuclear and missile capabilities. He emphasized that this evolution does not mean that South Korea and the U.S. are equal partners in the operational aspects of U.S. nuclear missions. Rather, it signifies that South Korea's ability to coordinate conventional support for U.S. nuclear operations has been strengthened, and that South Korea can now contribute input during the stages of U.S. nuclear planning and implementation. Addressing recent discussions about assigning specific U.S. nuclear assets to the Korean Peninsula for both wartime and peacetime scenarios, Narang explained that the commitment is not about assigning specific weapons to particular missions or goals. Instead, it represents a pledge to utilize nuclear forces in all contingencies involving nuclear or strategic attacks on South Korea. Concerning the proposal to permanently deploy U.S. strategic assets on the Korean Peninsula, he clarified that it involves the U.S. commitment to regularly rotate strategic assets, emphasizing that the core feature of the Guidelines document is to maximize the flexibility of strategic asset utilization for deterrence against North Korea.

The Washington Declaration and the Guidelines document mark significant progress in institutionalizing U.S. extended deterrence on the Korean Peninsula, effectively addressing the growing North Korean nuclear threat and the strengthening of Russia-DPRK security cooperation. However, to ensure that U.S. extended deterrence remains robust, it is crucial to enhance not only deterrence capabilities against intended and planned provocations by North Korea but also against accidental situations. For instance, North Korea's 'Nuclear Force Policy Act' outlines conditions for the use of nuclear weapons and explicitly permits preemptive nuclear strikes, thereby escalating the risk of nuclear conflict on the Korean Peninsula. This nuclear strategy introduces significant risks during military crises, as any increase in military tensions could lead North Korea to heighten its vigilance against the ROK-US alliance, increasing the likelihood of accidental nuclear conflict. While the Washington Declaration and the Guidelines document effectively bolster deterrence against North Korea's deliberate provocations, they do not fully address the risks of accidental conflict stemming from North Korea's advanced nuclear capabilities. Therefore, it is essential to develop additional measures to mitigate the risks associated with accidental escalation and ensure comprehensive deterrence.

Ultimately, to effectively address the crisis potential posed by North Korean nuclear weapons, it is essential to strengthen deterrence and response capabilities against North Korea's military threats and provocations, as outlined in the Washington Declaration and the Guidelines document. At the same time, efforts to pursue North Korean denuclearization and disarm its nuclear capabilities must continue. The new Russia-DPRK alliance treaty, coupled with the ongoing conflicts between the U.S. and both Russia and China, is shaping a new Cold War dynamic on the Korean Peninsula. The opposition from Russia and China has hindered the imposition of additional sanctions on North Korea and diminished the effectiveness of existing sanctions. In this context, integrated deterrence efforts must extend beyond military dimensions, such as extended deterrence, to encompass geopolitical and diplomatic strategies aimed at reshaping the security environment around the Korean Peninsula.

Understanding K-RMF and Its Impact on Defense Contractors

Kwangsoo Cho (Primary author)
Student (Ph.D. course), School of Cybersecurity, Korea University

Seungjoo Kim
Professor, School of Cybersecurity, Korea University

1. Introduction of RMF

Network and information technologies have begun to integrate into military weapon systems to enable effective command and control, such as allowing commanders to quickly assess battlefield status and make informed decisions. In the past, conducting a cyberattack required a malicious actor to have direct physical access to a weapon system, such as through a USB port or debugging port. However, as weapon systems have become more interconnected, attackers can now execute cyberattacks remotely, increasing the window of opportunity for such attacks. Consequently, the importance of defense cybersecurity in protecting weapon systems is growing.

The U.S. federal government, including the Department of Defense (DoD), has a long history of assessing the security of systems delivered to the federal government to protect them from cyberattacks. This security assessment process began with the Trusted Computer System Evaluation Criteria (TCSEC), published in the 1960s, and has evolved through Certification and Accreditation (C&A) to the current Risk Management Framework (RMF). These processes are primarily centered on the National Institute of Standards and Technology's (NIST) Special Publication 800-37, although they vary somewhat depending on the agency, such as the DoD and the Department of Homeland Security.

NIST introduces the Risk Management Framework (RMF) as follows: "The Risk Management Framework (RMF) provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle." In essence, it guides organizations on how to properly integrate risk management activities into their existing system development or acquisition processes. According to NIST standards, RMF comprises several components: risk management activities, security (and privacy) controls, various documentation templates and guidance, and a roles and responsibilities matrix. At the core of these components is the risk management process.

The RMF risk management process begins with the "Prepare" step and consists of a total of seven steps that follow a cyclical structure, continuously repeated. The "Prepare" step serves as a foundational phase that helps the organization execute the remaining steps smoothly. Therefore, organizations must sequentially and repeatedly perform the steps from "Categorize" to "Monitor." Figure 1 below succinctly illustrates the RMF risk management process.

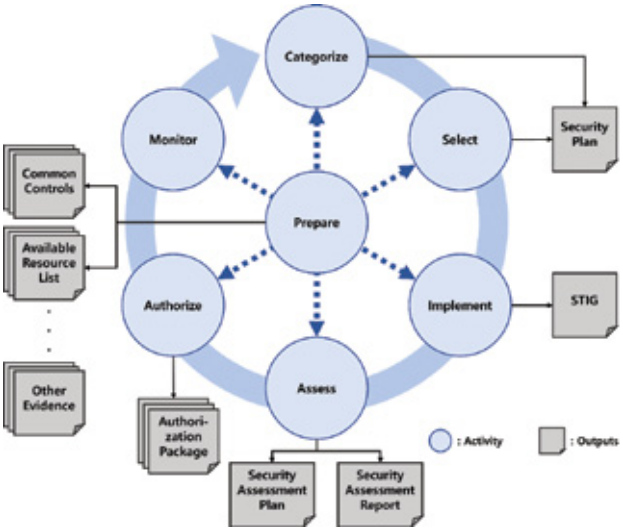

Figure 1. An Overview of 7-Step Risk Management Process in RMF

According to NIST's RMF standard, the purpose of each step in the RMF process shown in Figure 1 above is:

- 0. Prepare Step: Carry out essential activities at the organization, mission and business process, and information system levels of the organization to help prepare the organization to manage its security and privacy risks using the Risk Management Framework.
- 1. Categorize Step: Inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the nation.
- 2. Select Step: Select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the nation.
- 3. Implement Step: Implement the controls in the security and privacy plans for the system and for the organization and to document in a baseline configuration, the specific details of the control implementation.
- 4. Assess Step: Determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.
- 5. Authorize Step: Provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) is acceptable.
- 6. Monitor Step: Maintain an ongoing situational awareness

about the security and privacy posture of the information system and the organization in support of risk management decisions.

Organizations seeking to implement the RMF must carry out the step-by-step activities in alignment with the aforementioned objectives. It is crucial to note that the RMF risk management process should be fully integrated with the existing system development and acquisition processes within the organization, rather than being treated as a separate activity.

2. The Birth of K-RMF and Comparison with US RMF

The U.S. DoD is concerned about risks associated with both U.S. military weapon systems and interconnected allied weapon systems. For instance, according to the DoD's 2015 "The DoD Cyber Strategy," the Department declared its commitment to actively support the enhancement of cybersecurity capabilities among its allies. This initiative aims to mitigate the risks that might arise from allied nations' weapon systems interconnected with U.S. weapon systems. As part of this effort, the U.S. DoD has required its allies to develop and implement frameworks equivalent to the U.S. RMF for their weapon systems that interconnect with U.S. weapon systems. South Korea was no exception to these requirements, leading the South Korean Ministry of National Defense to develop the K-RMF (Korea-RMF) framework.

The K-RMF framework is overall very similar to the NIST RMF, though there are some detailed differences, as it was developed by benchmarking the NIST RMF. When comparing the NIST RMF and K-RMF, two major differences stand out.

The first major difference lies in the steps of the risk management process. According to the latest version of the NIST RMF, the risk management process consists of seven stages, as explained in Chapter 1. However, the K-RMF comprises six stages, excluding the "Prepare" step. Initially, the NIST RMF also consisted of six stages, similar to the K-RMF, but the "Prepare" step was included in recent updates.

The "Prepare" step is designed to perform preliminary and ongoing activities necessary for effectively integrating risk management activities into the existing system development or acquisition lifecycle. This step is not considered one of the primary stages of the RMF's risk management process but serves as a foundational phase to support the successful execution of the remaining six steps. Initially, NIST developed the RMF standard with only six stages, excluding the "Prepare" step. However, when applying this six-step RMF to various organizations, it was observed that the risk management process was often conducted separately from the existing system development or acquisition processes, contrary to its intended purpose. Based on this experience, NIST introduced the "Prepare" step to support and reinforce the remaining six main steps.

The second major difference lies in the security controls. The list of security controls referenced in the NIST RMF, specifically NIST SP 800-53 Rev.5, comprises 1,189 security controls (including control enhancements) divided into 20 families. In contrast, the K-RMF security controls list published by the South Korean Defense Counterintelligence Command consists of 761 security controls divided into 17 families. Notably, the privacy controls included in the NIST RMF are absent from the K-RMF security controls list. Table 1 below compares the families of security controls between the NIST RMF and the K-RMF security controls list.

Security Control Family	NIST RMF	K-RMF
AC: Access Control	O	O
AT: Awareness and Training	O	O
AU: Audit and Accountability	O	O
CA: Assessment, Authorization, and Monitoring	O	-
CM: Configuration Management	O	O
CP: Contingency Planning	O	O
IA: Identification and Authentication	O	O
IR: Incident Response	O	O
MA: Maintenance	O	O
MP: Media Protection	O	O
PE: Physical and Environmental Protection	O	O
PL: Planning (PA: Security Planning and Assessment)	O	O
PM: Program Management	O	-
PS: Personnel Security	O	O
PT: PII Processing and Transparency	O	-
RA: Risk Assessment	O	-
SA: System and Services Acquisition	O	O
SC: System and Communications Protection	O	O
SI: System and Information Integrity	O	O
SR: Supply Chain Risk Management	O	O
CR: Cryptography Management	O (Included in SC)	O

Table 1. Security Control Family Differences between NIST RMF and K-RMF

As briefly introduced in Table 1, the NIST RMF's security controls encompass those of the K-RMF. Unlike the NIST RMF, which is designed for a wide range of organizations, including the military, federal government, and private enterprises, the K-RMF is specifically limited to the defense sector. Consequently, security controls deemed irrelevant to weapon systems have been excluded, resulting in a smaller number of security controls in the K-RMF compared to the NIST RMF. Additionally, while there may be differences in the terminology used for security control IDs and titles, no new security control items were developed with the establishment of the K-RMF. Therefore, all security controls described in the K-RMF are included in the NIST RMF.

As such, while most aspects are similar, there are some differences between the NIST RMF and K-RMF. These differences arise from the variations in laws, policies, and security requirements between the two countries.

3. How does the K-RMF Affect Defense Contractors?

As previously mentioned, the U.S. has required allied nations to develop and implement frameworks equivalent to the DoD's RMF-based acquisition system. Specifically, for South Korea, the U.S. mandated the application of RMF to AKJCCS, a command-and-control system interconnected with the United States. In response to this requirement, South Korea developed the K-RMF. According to the K-RMF instruction, while the specific implementation timelines vary depending on the type of weapon systems, most are ultimately required to be acquired in accordance with the K-RMF. The first systems to be evaluated and acquired under the K-RMF are command-and-control systems directly interconnected with the U.S., such as AKJCCS and JFOS-K.

At each stage of the RMF's risk management process, organizations (in the case of the K-RMF, the military) must produce specific outputs. As shown in Figure 1, various outputs are produced over the six stages of the risk management process. Among these, the "Authorization Package" is particularly important for deciding on system acquisition. The "Authorization Package" consists of several documents: the Security (and Privacy) Plan, the Security (and Privacy) Assessment Report, and the Plan of Action & Milestones. The acquiring organization (i.e., the military) reviews the submitted "Authorization Package" to determine if the system has been developed correctly. In addition to the "Authorization Package," both the military and the development contractor must prepare various key documents, such as the Security Technical Implementation Guide (STIG), to ensure the proper operation of the developed system. Table 2 below provides an overview of the key outputs for each step of the RMF's risk management process.

Risk Management Step	Key Outputs	Main Contributor
Categorize	Security Plan	Army
Select		
Implement	Security Technical Implementation Guide (STIG)	Developer
Assess	Security Assessment Plan & Report	Army
Authorize	Authorization to Operate	Army
Monitor	Monitoring Strategy, Security Posture Report	Army

Table 2. The overview of key outputs of the RMF's risk management steps

To ensure that risk management activities are adequately performed and accountability is maintained, the NIST RMF and the DoD RMF-based Acquisition Lifecycle Guidance (hereafter referred to as DoD RMF A&A) describe the responsibilities and roles required for software development and acquisition projects. Since the NIST RMF is general enough to be utilized by both military and commercial organizations, this article will focus on the DoD RMF A&A, which is more specific to the military environment. According to the DoD RMF A&A, there are various roles, each with five levels of responsibility for risk management activities within the RMF. Tables 3 and 4 below illustrate the responsibilities and roles as outlined in the DoD RMF A&A.

Key	Description
(R)esponsible	Role that executes one or more process activities. There may be multiple "R" roles for a process activity; however, there must be at least one.
(A)ccountable	Role ultimately accountable for the work. Individual with final decision authority, or depending on the product, signatory authority.
(S)upportive	Role that is allocated to those who help to complete the task.
(C)onsulted	Role that needs to be consulted before a final decision can be rendered. Two-way communication is assumed.
(I)nformed	Role that is informed when a decision is made or an action is taken. One-way communication is assumed.

Table 3. The Responsibilities in the US DoD's RMF-based System Acquisition Lifecycle (RASCI Key)

Key	Description
Program Manager (PM)	Responsible for ensuring the program meets statutory and regulatory requirements for cybersecurity and for incorporating cybersecurity requirements into the program from conceptual development through design and sustainment/disposal.
Information System Security Manager (ISSM)	Responsible for ensuring all products, services, and PIT have completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an IS or PIT system.
Authorizing Official (AO)	Responsible for authorizing the system's operation based on achieving and maintaining an acceptable risk posture.
Information Owner (IO)	Acts as statutory or operational authority for specified information; responsible for establishing the controls for data generation, classification, collection, processing, dissemination, and disposal.
Developer or System Integrator (D/SI)	Role may be performed in-house, by another government entity, or by a contractor/system integrator. The developer should understand relevant threats and be able to assess mission needs and capability gaps against likely adversary threat capabilities. Development will be conducted in accordance with security controls related to assurance, system development, and security best practices to reduce vulnerabilities and to design, build, and test security in the system early and cost effectively.
...	

Table 4. The Roles in the DoD RMF A&A

Based on Table 3 and 4 above, the DoD describes which roles are responsible for each risk management activity in the DoD RMF A&A. For example, the activity "Categorize the system" has four roles with "R" responsibility: PM, IO, ISSM, and Defense Intelligence Agency Threat Analysis Center (Intel). And AO is Accountable, User Representative (UR) and Systems Security Engineering (SSE) are Consulted. The mapping of all three of these activities, roles, and responsibilities is called the "RASCI Matrix", and the D/SI role, referring to the defense contractor, is assigned "R" for four activities. The following Table 5 shows these activities.

Acquisition Phase	Activity	D/SI's RASCI
Engineering & Manufacturing Development (EMD)	Characterize the attack surface and begin to assess cybersecurity in planning and performing component and system integration testing	R
	Complete the detailed build-to design of the system, ensuring that cybersecurity requirements are included	R
	Conduct systems engineering, including technical planning as defined in the approved SEP, and verify compliance with the functional, allocated, and product baselines	R
	Ensure that cybersecurity requirements are mapped and allocated to the hardware and software design	R
	...	

Table 5. Four Activities for which the D/SI is assigned as Responsible

According to Table 5, the D/SI role is not only responsible for designing and manufacturing products according to given requirements but also for conducting security analyses of the system to be developed, such as "Characterize the attack surface." In this regard, the U.S. DoD's "Cybersecurity Strategy Outline and Guidance" requires comprehensive analyses, including Trusted System and Networks (TSN) analysis and threat modeling, to be presented as the basis for planning and implementation steps. To meet these requirements, defense contractors need to faithfully perform security analysis activities, such as threat modeling, during development and present the results as evidence.

In response to the emergence of the RMF, overseas defense contractors have developed threat modeling and cybersecurity management tools to meet these requirements and are using them in the development of actual weapon systems. Examples include Lockheed-Martin's Cyber Resiliency Level and STRIDE-LM, BAE Systems' Epiphany, and Boeing's Security Monitoring Infrastructure System. Additionally, the U.S. DoD, through the MITRE Corporation, developed and applied the Threat Assessment and Remediation Analysis (TARA) threat modeling methodology for weapon systems. As cybersecurity evaluation systems such as RMF are applied, overseas defense contractors are making significant efforts to develop technologies and automation tools for threat modeling and risk analysis.

4. Conclusion

This article began with an overview of the RMF and explained its impact on defense contractors. As mentioned at the end of Chapter 3, efforts are being made overseas to develop systematic threat modeling methods and automation tools to respond to the RMF. While the concept of threat modeling is simple, it requires a great deal of effort and expertise, resulting in varying outcomes depending on the performer's capabilities. Overseas, efforts are being made to develop systematic methods and automation tools to minimize this variability.

Due to the nature of military weapon systems, their design details and functional requirements are classified. Additionally, according to domestic studies such as "Korean Security Risk Management Framework for the Application of Defense Acquisition System" by Woo-Sung Yang et al., it is challenging to apply the U.S. RMF to the Korean military due to differences in laws, policies, and the level of security awareness. Therefore, it is not appropriate to use threat modeling and cybersecurity management tools developed by overseas defense contractors.

Recently, several studies have been conducted in Korea on how to use the results of threat modeling in RMF. For example, the paper "A Study on Constructing an RMF Optimized for Korean National Defense for Weapon System Development" by Jung Keun Ahn et al., along with various other industry-academia studies, are exploring this topic. Based on these studies, Korean defense contractors need to conduct various case studies to become familiar with threat modeling and RMF, thereby building their know-how. In the future, leveraging the accumulated knowledge and experience from these case studies, it will be possible to research and develop threat modeling methods and automation tools suitable for the Korean weapon system acquisition process.

RINSA

RINSA, KNDU
1040, Hwangsanbeol-ro, Yangchon-myeon, Nonsan-si
Chungcheongnam-do, 33021, Rep. of KOREA
Tel : +82-41-831-6414
Publisher : Ki Hoon Lim
Editor : Park Young-June