KONRAD ADENAUER STIFTUNG

SPACE SECURITY

New Frontiers

Risk Factors in Space and How to Manage Them

1. Introduction

With regard to the recent Ukraine war, an intriguing photo has been posted online. The photo features a GPS receiver installed on a Sukhoi Su-34, the main fighter-bomber of the Russian Air Force. Su-34 is one of the country's important weapon systems, just like F-15K in South Korea. Meanwhile, Russia is known to have sent jamming signals so that Ukraine cannot use GPS signals. In other words, ironically, Russia is utilizing the GPS signals, space assets operated by its potential enemy and at the same time interfering them.

One of the latest trends in space security is utilization of open-source intelligence (OSINT) such as commercial satellites. Russian flagship Moskva, which sank on April 14 after being hit by Neptune anti-ship missiles of Ukrainian military, is a case in point. At that time whether the Russian warship was really attacked drew significant attention. Some civilians discovered the fire at the Moskva using a Sentinel satellite. The Sentinel is a satellite system led by the European Space Agency (ESA), featuring a range of sensors including radar (Sentinel-1), optics (Sentinel-2), radiometer/marine spectrometer/altimeter (Sentinel-3)[1], collectively also known as the Copernicus Program. The program, which is directed by the European Commission in partnership with ESA, is the world's largest single Earth observations program.

The increasing use-cases of space assets reflect the rise in the dependency on space assets. As our life is closely linked to space, any threat to each space asset may endanger our security. For instance, GPS jamming incidents may result in aviation accidents.[2] Furthermore, it may cause national security issues, such as a power grid failure caused by solar storm.[3] With space emerging as a new battlefield, interest in space-related national security threats has been on the rise. In other words, space security has become one of emerging security issues.

Emerging security refers to a phenomenon where a microscopic individual safety issue grows into a collective safety issue or a collective security issue, and eventually a macroscopic general security issue.[4] Emerging security issues are characterized by the amplification of an ordinary, microscopic safety issue into a macroscopic national security issue under certain conditions.

Non-national security issues cannot be put on the back burner only because such issues have not resulted in a dispute and a war between countries, in other words, only because such issues are within the boundary of traditional security issues. Therefore, it is crucial to analyze emerging security related risks and come up with countermeasures.

This paper will take a look at risk factors of space security based on risk management principles and discuss how to manage them. First of all, it will explain the concept of risk management for space security and introduce typical risk events. And then this paper will introduce key participants managing such risks and their organizations, and countermeasures. Lastly, it will discuss the possibility of working with Europe on risk management for space security.

2. Concept and Risk Events

2.1. Concept

Risk can be described by multiplying the likelihood of a risk event by the impact of the event concerned as follows[5]:

Risk = Likelihood of a risk event × Impact of the risk event (1)

A variety of events may constitute risk events, from tumbling over a stone to aircraft crash depending on the extent of the impact. As you may see in Fig. 1, an event with higher likelihood and bigger impact is prioritized among others.

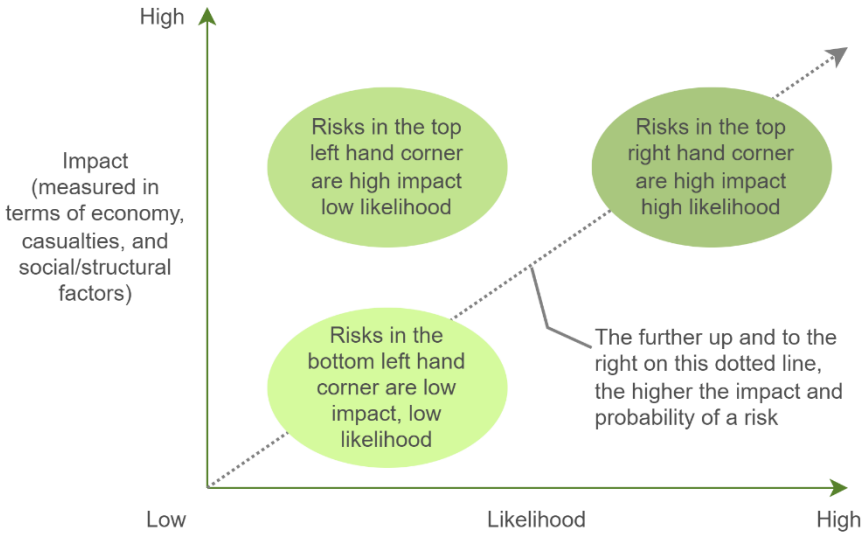

Fig. 1 Diagram showing how the national security risk assessment judgements were made: a risk in the top right-hand corner is one that is relatively more likely and relatively more impactful.

Also, risk events having impact on space security can be analyzed in the same way. For instance, a risk event in terms of space security refers to an event where the enemy attacks strategic assets of our military using satellite data. In this case, the likelihood of a risk event is calculated as follows:

Likelihood of a risk event = Likelihood of being observed × Likelihood of being identified as a target (2)

Simply observing an event may not bring about any result. Nevertheless, it can be a risk event with a huge impact since it offers an opportunity to identify our weakness and attack us depending on data processing capabilities. Being deployed at low altitude, conventional reconnaissance satellites have shorter orbital cycles as well as shorter observation time. In this case, the likelihood is calculated by dividing the hours available to observe by 24 hours.

Likelihood of being observed = Hours available to observe in a day / 24 hrs (3)

For instance, the likelihood of a satellite that can be observed for an hour a day is a 24th. Assuming that the likelihood of being identified as a target is constant, the likelihood calculated based on an orbital cycle has a great impact on the likelihood of risk events. Also, assuming that the impact of risk events is constant, the risk depends on the likelihood of being observed.

Satellite networks like Space X's Starlink, which has recently been deployed, offset the drawback of shorter observation time. Space X plans to launch over 40,000 satellites to provide seamless internet services to the world. In case of launching an optical satellite or a radar imaging satellite with the same concept, the observation time comes close to 24 hours while the likelihood of a risk event also comes close to 1, which means that the risk is significantly high.

The National Security Risk Assessment (NSRA) is designed to assess risks threatening the national security and prioritize them.[6] Based on such prioritization, national assets can be efficiently allocated to manage those risks appropriately. Even though space security also matters to national security, unlimited investment is practically impossible. So, it is necessary to make proper investments and eventually maintain risks under acceptable level. Fig. 2 shows a general circumstance of risk management. On the graph, the x-axis represents level of risk and the y-axis total cost. The higher the level of risk, the higher the risk cost (red line). On the other hand, the lower the level of risk, the higher the management cost (blue line). For instance, when the acceptable level of risk is about 0.7, the optimal point with the lowest total cost is where the risk is 0.5.

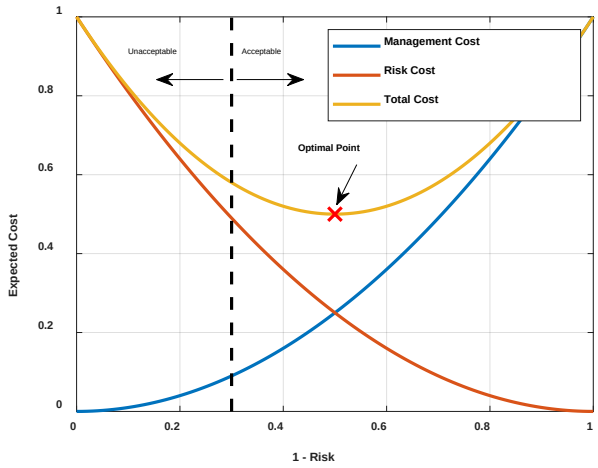

Fig. 2 Optimization for resource distribution

2.2. Risk Events

2.2.1. Space Weather

The U.K. identifies and assesses risk events using the NSRA every year.[6] Space-related risk events registered in the National Risk Register 2022 include severe space weather events, such as solar flare, solar proton event, and coronal mass ejection (CME). The damage afflicted by each event is as follows:

① Solar flare – A phenomenon that releases a huge amount of energy from one specific spot within a few minutes (or a few hours). The energy released during a flare could reach the Earth within a few minutes, causing radio blackouts.

② Solar proton event – A phenomenon where the high-energy protons in the solar atmosphere reach the Earth at enormous speed (within a few hours) in the event of a solar flare. The high-energy protons may damage satellites.
③ Coronal mass ejection (CME) – A phenomenon where a large mass of solar particles is ejected from the solar atmosphere within a short period of time. Such particles move slowly. CME reaches the Earth within a few hours or a few days, causing a geomagnetic storm and consequently a regional breakdown of a power grid, etc.

2.2.2. Space Debris

Since Russia sent Sputnik into orbit in 1957, about 7,900 satellites have been launched. About 3,000 satellites will be added by 2026, during which a significant amount of space debris will be generated. Space debris includes artificial space objects that have failed to fulfill the intended functions due to a failed reentry, equipment failure and others, and remained in orbit. Space debris also includes explosion debris, tools lost during spacewalk, etc. Such space objects, artificial or natural, may fall to the Earth, causing damage.

As of May 2022, 25,474 artificial space objects larger than 10 centimeters in diameter are orbiting the Earth. Since then, 26,997 space objects are known to have fallen towards the Earth.[13] Smaller objects are likely to collide with other objects in space while bigger objects are likely to fall to the Earth as well as collide in space. Over the past 50 years or so, the total mass of artificial space debris that has not been burned up during the reentry and has fallen to the ground or into the water is estimated to be 5,400 tons. However, most of them are likely to splash down into the sea which covers two-thirds of the Earth's surface, so they are unlikely to cause direct damage.

2.2.3. Counterspace Warfare

Weapons in counterspace warfare are categorized into kinetic physical attack, non-kinetic physical attack, electronic attack and cyber-attack.[7] Each has the following feature:

① Kinetic physical – An attack attempting to damage or destroy a satellite through high-speed collision with other objects. This form of attack is organized into three categories: direct-ascent anti-satellite weapons (ASAT), co-orbital ASAT and ground station attack. Direct-ascent ASAT is the typical land-based kinetic energy weapon in which a kill vehicle separated from its rocket booster launched from the ground locates and destroys a satellite target using embedded sensors and a thruster.
② Non-kinetic physical – An attack attempting to physically damage a satellite by shooting high-powered lasers or microwaves into specific satellite components. Particularly, this form of attack can cause permanent damage (aka partial blinding) to the optics of a satellite or temporary loss of sight (aka dazzling) for the satellite.
③ Electronic – An attack attempting to disturb the uplink or downlink between a satellite and a ground station. This type of attack is effective in damaging commercial broadcasting satellites with inadequate electronic protection. However, electronic attacks against military satellites with enhanced electronic protection require more advanced technologies.
④ Cyber – An attack targeting the data transmitted between a satellite and a ground station, and equipment that uses, transmits and controls such data. Cyber-attacks against satellites involve monitoring of data traffic patterns, data interception, injection of fake or tainted data, etc. Having low barriers to entry, cyber-attacks can be performed by individuals as seen in the Ukraine war.

Risk factors of space security facing South Korea will be prioritized depending on North Korea's space warfare capabilities. North Korea is deemed to be incapable of operating direct-ascent or co-orbital ASATs as well as non-kinetic energy attacks except EMP threats. On the other hand, North Korea has demonstrated its jamming-based electronic

warfare and cyber warfare capabilities.

In April 2020, North Korea has announced its plan to weaponize the latest GPS jammers. According to multiple sources, the regime is conducting jamming operations across the Korean Peninsula as of January 2021. Its operations are mostly targeting the radio frequency range and GPS signals used in the private sector, so threats to the military sector have not yet been identified.[7] In response, South Korea is developing an advanced global navigation satellite system (GNSS) as a ground system. The development of such a system was triggered by the spoofing attacks assumed to have been conducted by North Korea between 2010 and 2016.

Cyber warfare is mostly conducted by North Korean agencies including Unit 121, Unit 180, Unit 91 and Lab 110.[9] Among them, Unit 121 established by the then North Korean leader Kim Jong-il in 1998 is the largest in scale. The over 6,000-strong unit carries out cyber-attacks against overseas infrastructure, such as telecommunication, electric power, aviation. Unit 180, which is deemed to have been established upon the direction of North Korean leader Kim Jong-un, aims to finance the development of nuclear weapons and ballistic missiles. It is alleged that Unit 180 has been involved in the hacking of a large sum of NEM tokens from Japanese cryptocurrency exchange Coincheck. No attack against space assets has been identified so far. As cyber warfare capabilities continue to become more advanced, however, the threats to space assets and ground stations are likely to grow.[7]

3. Risk Management

Risk management for space security with regard to space weather, space debris, and counterspace warfare involve different participants, such as Ministry of Science and ICT, Ministry of National Defense, ROK Joint Chiefs of Staff, military headquarters, National Meteorological Satellite Center (NMSC) of the Korea Meteorological Administration (KMA), Korea Space Weather Research Center (KSWRC) of the Korea Astronomy and Space Science Institute (KASI), Center for Space Situation Awareness of the KASI, ROK Air Force Headquarters Space Center, Korean Air and Space Operations Center (KAOC) of ROK Air Force Operations Command (AFOC).

The ROK Air Force has its own space center under the headquarters. Having been fully operational since September 2021, the Space Center is focusing on cooperation and interaction for advancement of space capabilities, and establishment and implementation of space policies with external organizations, such as Korea Aerospace Research Institute (KARI) and Korea Astronomy & Space Science Institute (KASI), as well as higher commands, such as Ministry of National Defense and Joint Chiefs of Staff. The ROK Air Force Headquarters Space Center, which is comprised of three departments – the Space Policy Branch, the Space Asset Development Branch and the Space Intelligence Center, is committed to advancing and refining the Air Force's space strategies and space operations concept. The ROK Army and Navy are less involved in space security. But they are competing with the Air Force to become a key participant, as seen in the "Pegasus Project" of the ROK Army.

3.1. Space Weather

Space weather events with higher risks rarely occur, but a single occurrence may cause extensive damage and implications, which requires development of technologies for early detection in the orbit of a satellite, status analysis and communication, and response. Most of all, various research has been conducted to analyze and predict the three essential elements of space environment, solar radiation (R), high-energy particles (S) and variations in Earth's magnetic field (G), using ground and satellite observation data.

The National Meteorological Satellite Center (NMSC) of the Korea Meteorological Administration (KMA) and the Korea Space Weather Research Center (KSWRC) of the Korea Astronomy and Space Science Institute (KASI) as key participants from the public sector are striving to deal with risks arising from the variations in space weather. First, the NMSC is constantly monitoring space weather conditions in order to support the stable operation of satellites and prevent damage caused by solar activities.[8] Currently, the Korean Space Weather Monitor (KSEM) mounted on the Cheollian 2A satellite is the country's first system observing space weather at the geostationary orbit. The KSEM is comprised of three different sensors: particle detectors, magnetometer and charging monitor. The data observed by the KSEM is used for real-time monitoring and early detection of space weather events of concern, and for stable operation of satellites. The KSWRC is a research center conducting integrated research activities, such as basic research on the solar and space environment, and development of applied technologies and services. The Solar and Space Weather Group initiated its activities with the observation of sunspots in 1987 and has since developed and operated various equipment for monitoring space environment. In particular, the group has worked with NASA to establish and operate the Korea Solar Dynamics Observatory (SDO) Data Center and the ground station for the Van Allen Probes (VAP), satellites observing the Earth's radiation belts.

In the military sector, the space weather team at the Weather Group of the ROK Air Force is a key participant. The team forecasts space weather for the next three days on a daily basis and, in the event of an erupting sunspot, analyzes the impact on navigation and communication equipment to share the outcome with relevant departments. It invests in related research and mainly focuses on studying the causes of variations of the ionosphere over the Korean Peninsula and countermeasures, etc.[12]

In the field of space weather, the team has long cooperated with the KASI and built the VHF ionospheric radar observatory within the Weather Group of the ROK Air Force in 2010. The radar is used to analyze and predict the variations in the mid-latitude ionosphere that may cause satellite and military communication failure.

3.2. Space Debris

At the moment, the only way to respond to falling space objects or impact disasters is to monitor and track satellites, space debris and others in a consistent manner. Once a space object is identified as a potential hazard to Earth, an estimated time and location of the impact should be provided for precaution. When a space object is identified as approaching an active satellite, the satellite should perform a collision avoidance maneuver to avoid the impact.

In accordance with Article 15 of the Space Development Promotion Act, the government has come up with the First Master Plan for Space Hazard Response (2014-2023) to protect the safety and property of the public from space hazards, and thereby formulated detailed action plans every year.[11] It has also designated the KASI as "National Space Situational Awareness Organization" to advance policies and technologies required for space situational awareness.

In 2020, the ROK Air Force established a satellite surveillance unit in order to monitor and track over 2,000 satellites over the Korean Peninsula. The Air Force introduced the military's first space surveillance system called the Electro-Optical Satellite Surveillance System (EOSS) in January 2022. The EOSS is designed to acquire information by monitoring espionage activities of satellites passing over the Korean Peninsula, and tracking space objects. To this end, the Air Force has built observatories across the country to establish an integrated network.

3.3. Counterspace Warfare

As mentioned earlier, there are different ways of attacks that may put space infrastructure at risk. So far, the space operations unit at the Korean Air and Space Operations Center (KAOC) of ROK Air Force Operations Command (AFOC) is the only organization that is directly engaged in counterspace warfare. Staff of the United States Space Force (USSF) is dispatched to the unit to support countermeasures such as raising of the satellite output power in the event of attacks like GPS jamming.

The Air Force has unveiled its roadmap towards 2050 in the Master Plan for Development of Air Force Space Capabilities (also known as the Space Odyssey 2050). According to the Air Force, the space operations unit will be expanded to Space Operations Squadron by 2025, Space Operations Group by 2030, and eventually Space Command by 2050.[10]

Considering that the support for land and maritime operations is necessary, joint efforts for space operations are all the more important. In this respect, the Army and the Navy are pessimistic about the Air Force-led establishment of a space command and a space force. In particular, the Army unveiled the Pegasus Project with its vision beyond 2030s in June 2021. The Army believes that it must play a central role in enhancing space capabilities as it has the highest demand for space assets, such as satellite-based location data and communication data, among the three armed forces in Korea. Meanwhile, the Navy is striving to establish maritime-based space operations including the Aegis Ballistic Missile Defense System, and to come up with measures to build up its military capability.

4. Cooperation with Europe

The Committee of Peaceful Use of Outer Space (COPUOS) has played a leading role in developing a treaty on international order in space and relevant principles and has discussed all the issues. Following over a decade long discussions, the COPUOS finally reached an agreement on the 21 Guidelines for the Long-Term Sustainability of Outer Space Activities (LTS Guidelines) designed to reduce the risk of collision in space and promote equal access to space in June 2018. Those guidelines are comprised of four different areas: policies and regulations, safety in space operations, international cooperation and capacity building, and science and technology R&D.[14] Based on those guidelines, this paper will discuss in which areas South Korea need to cooperate with Europe.

4.1. Space Weather

Among the LTS Guidelines, B6 and B7 guidelines are designed to share space weather data and weather forecasts collected by each country, develop space weather models and tools, and put together cases for mitigating space weather related risks.

Multiple cooperative initiatives on space weather have already been launched. First of all, the College of Applied Sciences at Kyung Hee University signed an international research agreement with the European Space Agency (ESA) in 2016 and since then has conducted research and development on the KSEM which was mounted on the Cheollian 2A satellite and launched in 2018. The KSEM has been designed to observe high-energy particles, magnetic fields and satellite charging effects at the geostationary orbit. The KMA has worked with the European Organization for the Exploitation of Meteorological Satellites (EUMETSAT) on development of meteorological satellite technologies since 2021. Established in 1986, the international organization has 30 countries in Europe. In accordance with an agreement, both organizations have cooperated to develop a hyperspectral infrared detector which helps monitor greenhouse gases and water vapor, major causes of global warming, by measuring temperature and humidity in the atmosphere. They have also worked together to share satellite-based technologies for forest fire detection and verify GHGs in the atmosphere. In 2018, the KARI, the KMA and the Centre National d'Etudes Spatiales (CNES) of France exchanged a letter of intent on establishment of a space weather observatory.

Further cooperation is likely to be required for development of space weather models going forward. And it is believed that the country needs to benchmark Europe's measures to mitigate hazards caused by variations in space weather and thereby further advance its response system against space weather events.

4.2. Space Debris

B9, one of the LTS Guidelines is designed to mitigate the risks caused by reentry of space objects. In accordance with B9, any predictions regarding the reentry must be shared with countries having risks of impact or the international society. Other guidelines, D1 and D2, stipulate that each government must support research and development on measures to maintain sustainability, including space debris management and impact avoidance.

The more observational equipment, the more precisely we can monitor space objects. But there is a limit to the amount (and size) of such equipment we can expand due to technical complexity and enormous installation costs, etc. This is why major advanced countries have built their own observation systems depending on their objectives and at the same time have made up for shortfalls through networks with other key countries. South Korea has just been equipped with observational equipment for space situational awareness, which makes it reasonable to cooperate with Europe which has a higher level of capabilities in that field. Europe has come up with a comprehensive plan through the ESA and operated its own space situational awareness program in solidarity with others.

For instance, the Optical Ground Station (OGS) is capable of observe a space object with a minimum diameter of 10 cm.

Development of measures and technologies aimed to reduce space debris requires cooperation. The fact that such measures or technologies may be diverted for military purposes is a well-known challenge. Discussion on the LTS Guidelines have not reached a consensus on active removal and intentional destruction of space objects.[14] Therefore, it is believed that cooperation in such fields needs to be discussed following the establishment of international standards.

4.3. Counterspace Warfare

Cooperative measures aimed to mitigate the risks of counterspace warfare include the Horizon 2020 Program, the EU's largest research funding program which has been conducted from 2014 to 2020. Multiple research institutes in Korea have participated in this program. Cooperative cases regarding counterspace warfare are as follow:

The Electronics and Telecommunication Research Institute (ETRI) of Korea has participated in the total of seven projects during the program period (2014-2020).[15] Among them, one project falls into the field of space. Titled with "Standardization of GNSS threat reporting and receiver testing through international knowledge exchange, experimentation and exploitation," the project was aimed to conduct research on standards for the reporting and analysis of hazards such as GPS jamming GPS, and international standards for the performance and utilization of GPS receivers under hazard situations.

Korea University has participated in three projects in total.[15] Among them, two projects fall into the field of space. Both projects are associated with the Copernicus Program and their objectives are to develop technologies designed to integrate satellite data acquired by the Program with other data. They have already helped observe forests around the world, detect water pollution in lakes and coastal areas, and create disaster maps.

As mentioned in the introduction above, such open source data can be utilized for military purposes as well. In reality, the properties of space technologies make it challenging to distinguish military technologies from civilian ones. Aside from technologies for mitigating the risks of physical attacks, measures against electronic attacks and cyber-attacks are likely to be subject to cooperation of the private sector.

5. Conclusion

This paper identifies hazard events regarding space security based on risk management principles and looks into how to manage such hazard events, such as space weather, space debris and counterspace warfare. Hazard events with regard to space weather include solar flare, solar proton event and coronal mass ejection-led communication failure. For space debris, hazard events include collision in space, impact on the surface of the Earth. For counterspace warfare, hazard events include physical attacks, electronic attacks, and cyber-attacks against space assets. In South Korea, multiple participants are committed to alleviating those hazards. Lastly, the paper examines the possibility of cooperating with Europe on risk management for space security. A significant level of cooperation has been under way, mostly in the private sector. It is imperative that the country keep working with Europe on risk management for space security within the LTS Guidelines going forward.

Reference

[1] https://www.copernicus.eu/en, Accessed 25 May 2022.

[2] W. Bellamy III, "Are GPS Jamming Incidents a Growing Problem for Aviation?", Aviation Today, (2017).

[3] D. Wallace, "A Large Solar Storm Could Knock Out the Internet and Power Grid — an Electrical Engineer Explains How," Astronomy, (2022).

[4] Sangbae Kim, "Emerging Security and Meta-governance: Theoretical Understanding of the New Security Paradigm", Korean Political Science Review, 50(1), 75-104, (2016).

[5] MIL-STD-882E, "System Safety," U.S. Department of Defense, (2000).

[6] National Risk Register, HM Government, (2020).

[7] Space Threat Assessment 2021, Center for Strategic & International Studies, (2021).

[8] https://blog.naver.com/kma_131/222355907127

[9] Yonhap News, "Unit 121, Unit 180, Unit 91 and Lab 110... North Korea's Cyber Forces in Operation", (2018).

[10] Seoul Economic Daily, "South Korean Space Command Derailed During the Participatory Government...Set to be Launched as an Independent Space Force After 17 Years, (2022).

[11] https://www.nssao.or.kr/html/2, Accessed 25 May 2022.

[12] Yonhap News, "Competition in Space is Heating Up as Countries Launch Space Forces One After Another", (2020). Accessed 25 May 2022.

[13] https://www.nssao.or.kr/html/35, Accessed 25 May 2022.

[14] S. Shin, "The significance of a U.N. Guideline for Long-Term Sustainability of Outer Space Activities," Journal of Aerospace System Engineering, 13(5), 49-56, (2019).

[15] Kyung-Mo Sung, Soeun Kim, Jin Gyu Jang and Juwon Kim, "Plan to Strengthen Korea-EU International Cooperation in Science and Technology: Focusing on the Cooperation Strategy for Horizon Europe", Policy Research 2021-42, Science and Technology Policy Institute, (2021).

Author Dooyoul Lee graduated from the Air Force Academy in aeronautical engineering and obtained a doctorate in mechanical engineering from Northwestern University in the United States and is currently a professor of defense science at the Korea National Defense University. He is researching on topics related to engineering risk analysis and is interested in predicting rare events by using artificial intelligence technologies such as Bayesian networks and deep neural networks. Over the past three years, 10 SCIE-listed journal papers and 8 KCI-listed journals have been published.

Dooyoul Lee
Professor of Defense Science
Korea National Defense University

Konrad-Adenauer-Stiftung Korea Office
kaskorea@kas.de
www.kas.de/korea