

Korean Security Briefing _ vol.2

3. The smart industry

Growing industries from smart unmanned stores to metaverse are in the spotlight.

Diagnose policies promoted this year, related to smart stores, smart cities, UAM, geospatial data, and metaverse.

The government has selected smart city policies as a key national task, investing 10trillion won in the 'smart city' project by 2025. Also, it is applying digital technology to solving urban problems, including construction of a national model city, with the goal of creating 150,000 jobs. In particular, through K-City NetWork, various projects such as the domestic smart city industry, national pilot city, smart challenge, smart city regulation special system, smart city regeneration, smart city integrated platform, and innovative talent development project are underway.

'Smart City', which has been regarded as simply a change in the city, is now beyond it. 'Smart City' is changing and growing to develop new transportation, operate stores without people, or engage in various activities in virtual spaces.

The evolution of unmanned stores requires the efforts of the government and companies

As interests in non-contact and non-face-to-face increase due to COVID-19, unmanned stores that were applied to convenience stores and PC rooms are rapidly spreading. Recently, it is evolving into a complete smart store that can be operated automatically without human intervention in the entire process, and that can automatically detect accidents and crimes.

From 2019 to 2021, industries that can quickly convert to unmanned stores such as convenience stores and PC rooms were the main targets, but this year, it is expanding to meal kit stores, stationery stores, photo studios, and recently smart stores selling cars and mobile phones have also emerged. The reasons for the rapid increase in smart stores can be summarized in three main categories: "working population concentrated in metropolitan area," "increasing minimum wage and operating costs," and "rapid development and introduction of artificial intelligence."

①As working population is concentrated in the metropolitan area, it became difficult to find a person to work in the provinces. In addition, the number of store users has decreased, which made operating stores in the evening or late-night hours with resident workers as a burden to store owners.

②The Ministry of Employment and Labor announced in August 2022 that the minimum wage of 2023 is 9,620 won per hour. This is a 5.0% increase from 9,160 won of 2022. In convenience operating costs, labor costs take up 70%, increasing burden on store owners. Moreover, 30.4%(as of July 2022) of the operators of CU, GS25, and 7-Eleven, which are three major domestic convenience stores, had profits lower than the minimum wage.

③Rapid growth of artificial intelligence (AI) training data and the improvement of computing power to handle data led to development of models that can efficiently and quickly process large amounts of

data. In particular, technologies such as face recognition and object recognition using artificial intelligence are applied to fully smart stores, drawing attention to development of related technologies.

The biggest advantage of smart stores is 'non-face-to-face'. As interest in non-contact and non-face-to-face has increased due to COVID-19, interest in smart stores is increasing in various industries, starting with unmanned stores. Security industry is also expanding its scope in related markets with solutions such as non-face-to-face access security, and intelligent CCTV. The trend is expected to continue in 2023.

The number of unmanned stores in four major convenience stores (GS25, CU, 7-Eleven, and E-Mart 24) was 2,783 at the end of June 2022. This is 14 times increase from 2019 when there were only 200 stores. As smart stores spread, demand for security solutions such as CCTV and access control and related technologies such as artificial intelligence (AI) vision and kiosks is also expected to increase, and the ecosystem of the unmanned store industry is expected to grow rapidly.

Although smart (unmanned) store market and related industries are growing rapidly, there are many problems that need to be solved through policy. CCTV video information cannot be used properly under the Personal Information Protection Act. However, the industry believes that if consumers recognize the convenience of using personal information in smart stores and agree to providing personal information, smart stores will expand at a faster rate and more technologies and services will emerge. In addition, industry hopes that policies will develop around anonymization and de-identification of video information, strengthening safety for transmission and storage, and expanding the scope of video information use.

It is also necessary to establish technology and product standards that can be applied to smart stores and formulate development support policies. Since technology development costs a lot, smart technology developers should be able to grow by expanding the government's budget and securing sales channels for developed products and services. In addition, if small business owners who feel the economic burden of introducing smart find out which technologies and products they really need and let related small and medium-sized companies develop them, a win-win stage can be set up for everyone. Finally, it is also necessary to make efforts to safely operate unmanned stores by setting up channels where private companies and public institutions such as the police can communicate closely.

Next Generation Advanced Transportation System, Urban Air Mobility (UAM)

Urban Air Mobility (UAM) refers to next-generation advanced transportation system that safely and conveniently transports people and cargo in an urban environment based on electrically powered low-noise aircraft and vertical take-off landing areas.

Many companies around the world are participating in UAM gas development and service construction, and Korea is also striving to commercialize UAM. In May 2020, the Korea Urban Air Transport (K-UAM) Roadmap was announced. In March 2021, a technology roadmap containing mid-to-long term research development strategies and tasks of domestic UAM was prepared. And in September of the same year, K-UAM Operation Concept 1.0 was published. In November 2021, the

UAM demonstration was conducted at Gimpo Airport to confirm possibility of UAM services in terms of airframe, operation service, and traffic management.

In December 2021, the Ministry of Land, Infrastructure and Transport and 37 organizations in the urban air transportation sector held the "UAM Team Korea 3rd Main Consultative Meeting" and discussed △ the operation plan of Korean Grand Challenge △ Expansion of UAM Team Korea participating organizations.

First of all, the Ministry of Land, Infrastructure and Transport has set a goal of commercializing the K-UAM roadmap for the first time in 2025. Before commercialization, it is processing grand challenge, which is demonstration project for ①safety verification, ②establishing appropriate safety standards, ③Industry testing and support for demonstration.

Urban Air Transportation (UAM), local governments also actively participate.

UAM, which expands air transportation to urban transportation systems, is a representative future industry that will revolutionize transportation and industry. Research and demonstration systems are being developed worldwide, and local governments are also actively working to introduce it.

Incheon City signed a memorandum of understanding with the Korea Aerospace Industries Convergence Institute and Vessel Aerospace for the urban air traffic agreement. Vessel Aerospace, which has experience in developing two-seater aircraft (KLA-100) through the agreement, develops and demonstrates urban air transportation aircraft. Aerospace Industries Convergence Institute supports urban air transport platform demonstration projects. In order to take the lead in introducing the urban air transport system, the Incheon Metropolitan Government enacted the "Ordinance on the Establishment of the Urban Air Transport System" in 2020 and is analyzing the risk of low-altitude airspace (sky road).

In March, Gwangju Metropolitan City (hereinafter referred to as Gwangju City) formed a research · planning task force (T/F team) involving experts from all walks of life to respond to the rapidly changing drone industry and set up a roadmap for drone · urban air transportation (UAM) industry. Gwangju City has selected drone industry as one of the 11 representative industries in 2019, and intensively fostered the industry. It established ordinances and a five-year basic plan to lay the foundation for development of local drone industry. Gwangju City plans to link · utilize various artificial intelligence and metaverse resources, and to create competitive drone · urban air transportation industry ecosystem by converging with the future car industry that shares core technologies such as batteries and motors.

Jeju Island announced that it will nurture Jeju-type urban air transportation as a future eco-friendly industry, and that it aims to commercialize urban air transportation by 2025. Jeju Island is planning to expand its scope to public services such as logistics and emergency medical care and replace transportation in the future, starting with non-urban · low-density tourism air taxis in consideration of safety, public acceptance, and profit realization. In particular, if an emergency occurs on the sea, islands, or Mt.Halla, which is difficult to access by car, it can be used as a new emergency transport system in addition to emergency medical helicopters. Logistics problems caused by island characteristics can also be solved and can be used as an eco-friendly means of tourism.

"Special Purpose Oil-Free Drone Industrial Ecosystem Creation Project" by Wonju City finally passed the Ministry of Public Administration and Security's local fiscal central investment review. With the acceptance of this screening, Wonju City aims to invest 29 billion won in the Buron General Industrial Complex, including national and provincial expenses, to start construction in August 2023, complete it in December 2024, and build test equipment at the same time.

In October, Namwon City held a briefing session on the launch of the "Research Service on the Creation of Aviation Industry Clusters." Through this, Namwon city is planning △ Analysis of domestic and overseas drone industries trends, conditions, situations, and actual conditions in Namwon-si △ Strategies for creating an Aviation Industry (Drone/UAM) Cluster by Attracting Drone/Aircraft Institution △ Research on policies linked to 4th industrial revolution with big data through drones · seek ways to activate light aircraft for the aviation leisure and tourism industries. △ Establishing an annual promotion plan for drone (including UAM) industry in Namwon City, establishing infrastructure related to drones and UAM in the future, and public offering by the government.

In October, Daegu City signed a business agreement with SK Telecom to create a UAM leading city and formed a consortium of "K-UAM Dream Team." The "K-UAM Dream Team" consortium and Daegu City plan to expand to regional aviation mobility services connecting Daegu downtown with Daegu Gyeongbuk Integrated New Airport by 2030 through UAM commercial service and demonstration-model city-commercialization plan.

Expanding the use of Geospatial data

Geospatial data includes map and all information that can be expressed on maps. It provides basic information and standards for determining behavior or attitudes in daily life or specific situations.

Geospatial data is essential for efficient management and development of the country. Politically, geospatial data can be used to determine and maintain social areas such as national boundaries, administrative districts, constituencies, and tax zones. In addition to this location information, attribute data such as the number of residents, election votes, and tax details can be built and managed in database, so that necessary information can be used in the right place and national land management can be efficiently performed.

Economic losses can be minimized by selecting the optimal location for roads, railways, ports, and aviation facilities using geospatial data on topography and geography of the country. In addition, by establishing a development plan that makes the most of the country's tourism resources, it can be used as a motor force of economic growth in the country by invigorating tourism. In order to build such geospatial data, a lot of manpower is required in various fields such as surveying and data processing, system construction, geospatial data analysis, and software development. Therefore, various jobs can be created to revitalize people's economic activities, thereby growing country's domestic market. In this way, it is possible to efficiently manage and develop the country and secure national external competitiveness.

The upcoming future society is expected to change from “knowledge and information society” to “smart society”. The smart geospatial data society will be able to recreate reality almost as it is by collecting, processing, and utilizing geospatial data using various mobile devices and IT infrastructure built across the country.

According to 2021 geospatial data industry survey of the Ministry of Land, Infrastructure and Transport, sales in the domestic geospatial data industry grew 4.6% year-on-year to 9.7691 trillion won, and the number of workers increased 3.6%.

Private companies can also use geospatial data

On March 17, the Enforcement Decree of the Framework Act on National Geospatial data was revised and security review regulations were enacted, which included allowing private companies to receive high-precision geospatial data established by the government. Until now, high-precision aerial photographs or three-dimensional geospatial data built by management agencies such as central administrative agencies or local governments were limited to data under security management regulations, so private companies could not be provided for business purposes.

However, as the enforcement ordinance has been revised and security review regulations have been enacted, high-precision and three-dimensional geospatial data built by the government in new private industries such as autonomous driving, augmented reality, and virtual reality (AR·VR) can be used for projects such as developing new services.

① Geospatial data that is restricted from disclosure is information that may harm public safety if disclosed, so the head of the management agency has specified the provision criteria to review security management matters such as preventing information leakage from private companies. However, if the geospatial data to be provided includes information on military facilities or national security facilities, the head of the management agency must provide security treatment, such as deleting the information.

② The head of the designated standards management of security review agency stipulated that security review agency can be designated from among institutions or associations that conduct a professional · systematic review of geospatial data security management of private companies. In such cases, institutions or associations shall meet the designated criteria such as technical personnel, confidential approval, and dedicated organization, necessary in performing the review work.

In July, the Ministry of Land, Infrastructure and Transport announced that it will open the list of geospatial data held by 240 institutions (including central ministries, local governments and public institutions) to the public. Since 2016, the Ministry of Land, Infrastructure and Transport has opened a list of various information related to geospatial data such as data holding institutions, documentation guidelines, renewal cycles, and application fields. The list of geospatial data opened this time was 102,178, an increase of 16,979 (19.9%) from 85,199 in 2021.

The Ministry of Land, Infrastructure and Transport continues to make efforts by signing a business agreement so that geospatial data held by various institutions can be opened to the private sector

and used jointly. Through this, it plans to open 102,178 geospatial data held by the public and 603 data (including highly utilized real estate data and environment data) held by NS Center, and to continue to collect · expand various geospatial data.

Metaverse has emerged as a trend in all fields.

Metaverse is a combination of Greek Meta, which means "processing" and "abstract," with Universe, which means "real world." Metaverse seems similar to virtual reality, but it is one step further from it since it uses avatars in virtual reality to engage in real-life social · cultural activities.

Metaverse began to draw attention as online platforms such as teleconferencing were activated due to COVID-19 pandemic. With the prolonged pandemic, there were needs from people to experience the lack of offline activities similarly in the online space, and it was Metaverse that emerged as a tool to meet these needs.

The Yoon Suk Yeol government, which was launched in May 2022, also cited "activating ecosystem: including enactment of Metaverse · Cloud, and Metaverse Special Act," as one of the major national tasks. In "realization of digital economy through public · private cooperation.", the new government plans to enter the top five global metaverse market share (21st in 2021) by 2027 through revitalizing the metaverse economy.

To this end, it proposed a policy to create a foundation for trust through blockchain (2022~) and to revitalize the ecosystem by enacting a special law on and discovering metaverse services that support daily and economic activities. It also plans to lay the foundation for user protection in new digital industries such as metaverse, digital platforms, mobility, and to establish cooperative self-regulation systems such as digital community ethics, and to reorganize the Location Information Act to promote the mobility industry and protect users.

In addition, Its goal is to apply · expand metaverse throughout the industry including △Developing technologies to actualize realistic media such as metaverse, fostering front · rear industries such as equipment and devices △ Reviewing the establishment of a remote training platform incorporating new technologies such as metaverse or VR and linking it to smart vocational training platform (STEP) △ Simplifying pre-evaluation of training institutions and courses for SMEs or self-employed people, and supporting the spread of training by incorporating new education methods such as project learning (PBL) with new technologies such as metaverse. △ Supporting content production, fostering human resources, and expanding investment in cultural technology to lead new markets such as metaverse, realistic content, and OTT. △ Customized learning using AI learning system and metaverse reduces private education and intensively supports resolving learning deficits caused by COVID-19. △ Strengthening the Capacity of Digital Unification Education Using Metaverse

ETRI Develops Standard Guidelines for Metaverse Ecosystem

The Korea Electronics and Telecommunications Research Institute (ETRI) announced in April that it will start developing an ICT convergence standard framework in the field of 'metaverse', a virtual convergence space that is emerging as a new center of the future digital society.

With the expansion of non-face-to-face services due to COVID-19, Metaverse is in the spotlight as a next-generation ICT industry that allows daily life and economic activities beyond the limitations of time and space. However, for Metaverse to be connected to actual industries and services, it is necessary to find related convergence services and develop standards to support them along with a clear definition of technology elements.

ETRI's Metaverse Standard Framework began development to support researchers to develop and utilize technologies or standards by defining standards necessary to analyze and implement newly created Metaverse convergence services and utilization scenarios. The standard framework is a guide to discovering new convergence services created based on future ICT advanced technologies and presenting the standards necessary to implement services.

It predicts ecosystem structure of future industries through △service modeling for industrial ecosystems, △identification of currently developed standards, and △analysis of standards (potential standards) that require further development, and preemptively presents blueprints for standards required by markets and services.

Self-driving technology is applied to everyday life

Automobiles are by far the first thing to come to mind when it comes to autonomous driving, but recently, they are expanding into various fields such as autonomous robots and drones. Ministry of the Interior and Safety demonstrated the address-based autonomous robot delivery service at Eco Delta City Smart Village in Busan on 11th of November.

When a person orders through "Smart Village Robot Delivery Internet Service" piloted by KAIST, the convenience store owner who received the order from the Internet service checks it and notifies the robot of the start of delivery after loading the product. The robot then automatically informs when it arrives at the site to the person who made orders. When the person presses OK, the robot's luggage compartment door opens and receives the item.

The demonstration venue is a complex where you can meet future life and new technologies in advance, with a total of 56 households residing. Three types of robots, patrol · cleaning · delivery, are on demonstration by subdividing addresses to road names and building numbers and by establishing robots' movement paths.

Ministry of the Interior and Safety has been conducting service pilot projects and verifying the operating environment in four regions nationwide, including KAIST Daejeon Campus, Konkuk University Seoul Campus, and Yonsei University Incheon Campus.

Since November, the Seoul Metropolitan Government has introduced "Traffic Safety Smart Alert App," a specialized system for children's traffic safety using autonomous communication technology. Traffic safety smart notification is an application that combines "Vehicle to Everything" technology, which is used as an autonomous driving technology, with the advantage of strengthening walking safety through advanced technology in everyday life.

This app collects and analyzes data such as users' current location, movement direction, and speed in real time by transmitting them to 5G cloud system. It analyzes various collected information and sends warning messages with sound and vibration to help prevent accidents if the risk of collision is predicted. In addition, the app is linked to artificial intelligence-based smart CCTV to detect the risk of collision of pedestrians who do not have the app installed. CCTV checks pedestrians and vehicles to calculate their location, direction of movement, and speed, and immediately notifies drivers using the app of the risk of collision when a dangerous situation is predicted.

2023 Cyber Threat Forecast Keywords: National Background Hacking Organization, Ransomware, Zero Day Vulnerability, Ransomware, PhaaS, IIoT, Mobile, Virtual Asset

In the new year, attacks by state-backed hacking organizations will increase more frequently, and attacks by variant ransomware will still show off their influence following this year. East Security (CEO Jeong Jin-il), a security company, selected "Top 5 Settlement and Retrospective of Major Cyber Threat Trends in 2022" and Top 5 Prospects of Cyber Threats in 2023.

East Security cited the top five cyber threat prospects for 2023 as ① Escalated Cybersecurity Threats by Hacking Organizations Behind the Country, ② Continuous distribution of ransomware variants and evolution into APT attacks, ③ Concerns over personal information theft attacks due to widespread use of digital identification and electronic document services, ④ Diversification of cyberattacks targeting virtual assets, and ⑤ Increasing attacks exploiting Zero-Day and N-Day vulnerabilities.

First of all, in the "high cybersecurity threat of hacking organizations behind the state," attacks by state-backed hacking organizations are expected to become frequent as the war began in February this year when Russia invaded Ukrainian territory and conflicts between countries intensified.

Along with continuing hacking attacks in the sector of national defense and security, hacking attacks targeting the aerospace industry and mobile communication, which are used in missile launch and defense technologies, are expected to increase significantly. In addition, it is analyzed that deepening conflicts between countries will trigger conflicts within hacking groups composed of multinational members, and information leakage will occur frequently. Global security threats are expected to increase in the new year, with attacks by state-backed professional APT groups and attacks using leaked information prevalent together.

The second is "continuous distribution of ransomware variants and evolution into APT attacks", and ransomware is expected to be used as a means to generate high profits for hackers next year as this year.

It is concerned that ransomware that attempts to bypass security systems will increase as produce relatively less known programming languages such as GO, RUST, and Dlang. In addition, the latest Zero-Day vulnerabilities are expected to penetrate the internal network and evolve into APT attacks such as file encryption, information theft, and additional malicious code distribution, and the scale of damage is expected to expand.

As the threat of ransomware is expected to accelerate and evolve into more creative forms, companies and institutions need to identify the latest ransomware trends and prepare customized countermeasures.

Third, there is a growing concern about "personal information theft attacks due to universalization of digital ID cards and electronic document services." Mobile issuance services for resident registration cards and driver's licenses have been implemented since July 2022, and mobile services will gradually expand. In particular, a service that allows sensitive documents such as resident registration copies, health insurance payment confirmations, and copies of medical records to be issued in the form of electronic documents has further strengthened the convenience of the public. In line with this trend, attackers also began distributing malicious apps disguised as identity pass apps and mobile ID apps in the second half of the year. Attacks aimed at stealing digital IDs and electronic documents are expected to increase significantly in the new year.

The fourth is "diversification of cyberattacks targeting virtual assets." The increase of platforms that help generate NFTs and the increase of participants in virtual asset investments is creating greater attack opportunities. Virtual asset theft is attracting attention as in poor countries foreign currency gives "low cost and high efficiency" profits, and it is expected that more and more professional hacking organizations are aiming to earn foreign currency through virtual asset theft.

Not only hacking attacks on members using social engineering techniques, but also attempts to steal virtual assets through various attack methods are expected to become frequent.

Lastly, attention is being paid to the increase in attacks that exploit Zero-Day and N-Day vulnerabilities. Since COVID-19, many companies have introduced remote work systems and Dark Web has been activated, increasing the number of newly discovered Zero-Day vulnerabilities.

More and more APT organizations are using Zero Day for attacks, and as the value of Zero Day vulnerabilities in dark web increases, many attackers are jumping into discovering Zero Day. As supply and demand increase at the same time, the zero-day market is activated, and attacks are also increasing.

In the case of N-Day vulnerabilities, interest is relatively low because they have been released for a certain period of time. And as solutions used by companies became diverse, it is difficult to check open vulnerabilities and patches for every solution. Attacks using N-Day vulnerabilities that exploit these points are also expected to increase.

EQST (Experts, Qualified Security Team, EQST), a group of white hacker experts on the life care platform SK Shields (CEO Park Jin-hyo), held a media seminar to share security threat prospects and response strategies in 2023, preparing for the new year.

In this seminar, major cybersecurity threats that are likely to occur next year were selected based on cases and research of hacking accidents experienced by SK Shields this year. In addition, the results of

examining cases of accidents by industry that occurred this year and analyzing major vulnerability statistics were also disclosed.

In 2022, security infringement accidents occurred the most in manufacturing and public sectors in Korea, and 'ransomware' was cited as the main cyber threat. GWISIN ransomware targeting only domestic companies has emerged and introduced advanced strategies such as triple threats, and a service-type ransomware LockBit 3.0 (RaS) (Ransomware as a Service) is prevalent and social damage from ransomware has increased due to the leakage of internal information from companies.

In March, hacking group LAPSUS\$ launched an attack on global IT companies and manufacturing industries to leak confidential data, and in July, a server attack on medical image information management system used by domestic medical institutions was found, putting medical institutions on alert. In October, there were a number of attacks that abused the disability of the public messenger service, which became a representative example of abusing social issues to target more.

According to statistics on infringement accidents by industry, infringement accidents targeting the manufacturing industry accounted for the highest proportion with 18%. Overseas, the proportion of attacks on public institutions and governments recorded 21% in the aftermath of the Russia-Ukraine war.

As for the statistics of accidents, infringement accidents through malicious code infection were the highest at 32%. This was mainly due to the influence of GWISIN ransomware and the active distribution of malicious code using previously known vulnerabilities such as Log4j vulnerabilities. In addition, the proportion of phishing and scams increased 4% compared to the first half of the year to 20%, and as phishing attacks that abused social issues are increasing, URLs with unclear sources should be blocked.

Among the major security threats for next year, ransomware is expected to become more diversified, intelligent, and sophisticated. Since the emergence of domestic target ransomware, new types of ransomware such as ransomware aimed only at data destruction, or ransomware aimed only at vulnerabilities in database servers, have been increasing. With the outbreak of ransomware attack groups, related damage is expected to increase as the attack method for survival is newly modulating.

Phishing attack, one of the traditional methods of attack, is expected to meet a new type of phishing platform and intensify the attack. Starting from phishing sales site called "Caffeine" found on the dark web, PhaaS (Phishing-as-a-Service) is expected to be popular. There is also a form of creating phishing sites through dark web, which is very dangerous since it can identify targets or impersonate individual services. Techniques such as bypassing spam mail using AI filtering technology have also been found, requiring systematic countermeasures against phishing attacks.

As super apps that can use various services in one app are recently activated, attention should be paid to attacks targeting mobile. In the process of combining multiple functions into one app, the security verification process may be omitted, or loopholes in authority management may occur, and hacking attacks aimed at this may occur. It is predicted that zero-click attacks, an attack that can be infected

even if you do not click the link included in email or text messages will also increase for mobile devices. Zero-click attack is a new attack method in which malicious code disguised as an image file is planted in text messages and malicious code is executed just by reading the text message.

It is also necessary to prepare for the threat of unmanned and automated devices that have spread throughout the industry since COVID-19. Unmanned industrial · manufacturing facilities with Industrial Internet of Things (IIoT) use various equipment, but they are often subject to cyberattacks such as personal information leakage or ransomware as they often use operating systems that has poor asset management and are vulnerable to security threats. In addition, attacks targeting virtual assets are expected to become more active with the advent of Decentralized Finance (DeFi, decentralized finance).