sustainability

Article

Measures to Ensure the Sustainability of Information Systems in the COVID-19 Environment

Hyukjin Kwon [1], Youngjoo Shin [2], Jaeyeong Jeong [3,4], Kookjin Kim [3,4] and Dongkyoo Shin [3,4,*]

[1] Department of Defense Science Convergence, Seoul National University of Science and Technology, Seoul 01811, Republic of Korea
[2] Korea Institute for Defense Analyses, Seoul 02455, Republic of Korea
[3] Department of Computer Engineering, Sejong University, Seoul 05006, Republic of Korea
[4] Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul 05006, Republic of Korea
* Correspondence: shindk@sejong.ac.kr

Abstract: National defense requires uninterrupted decision-making, even under direct or indirect impacts of non-traditional threats such as infectious diseases. Since all work utilizes information systems, it is very important to ensure the sustainability and availability of information systems. In particular, in terms of security management, defense work is being performed by dividing the network into a national defense network and a commercial Internet network. This study suggests a work execution plan for sustainability that takes into account the efficiency of work performed on the Internet and the effectiveness of security through effective defense information system operation. It is necessary to minimize the network contact points between the national defense network and the commercial Internet and to select high-priority tasks from various tasks and operate them efficiently. For this purpose, actual cases were investigated for an institution, "Organization A", and characteristics were presented. Through the targeted tasks and operation plans presented in this paper to improve the effectiveness of defense tasks and ensure security, it will be possible to increase the sustainability and availability of task performance even under non-traditional threats such as infectious diseases.

Keywords: sustainability; defense security; COVID-19; non-traditional threat; BCP; VDI; close network; military network

check for updates

Citation: Kwon, H.; Shin, Y.; Jeong, J.; Kim, K.; Shin, D. Measures to Ensure the Sustainability of Information Systems in the COVID-19 Environment. *Sustainability* **2023**, *15*, 35. https://doi.org/10.3390/su15010035

Academic Editor: Zlatko Nedelko

Received: 2 November 2022
Revised: 10 December 2022
Accepted: 16 December 2022
Published: 20 December 2022

1. Introduction

The importance of comprehensive national security against non-traditional threats such as disasters and infectious diseases continues to be emphasized. Even if system operators are quarantined and facilities are closed due to an infectious disease, it is necessary to maintain business continuity without interruption. Providing an environment and system so that non-face-to-face work that can minimize the work gap can be carried out stably is emerging as a key issue [1–3]. The military started information system conversion training as COVID-19 became a major threat, but it is necessary to establish an implementation system with clear priorities and goals [4].

In addition, countermeasures against information leakage and service failure should be devised when performing work in a non-face-to-face situation. Working from home in a defense environment has a number of problems, unlike those in the private sector. Because the national defense operates a closed network, it is impossible to access the defense network from the home or outside space. In addition, it is unclear what tasks can be performed by telecommuting due to the security of defense work [5–7].

As the connection points with the internal network increase, it is also necessary to prepare countermeasures against leakage of confidential information from insiders or unauthorized outsiders and service failures due to hacking [8–11]. The Ministry of National

Defense is conducting response training according to COVID-19, but the non-face-to-face work performance system has not been finalized. Of course, not all work has to be done remotely. It is necessary to have a structure of what the priorities are, what the goals are, and how to do them.

In the context of the spread of COVID-19, two problems were identified with South Korea's defense network: One is that when an epidemic such as COVID-19 occurs, existing countermeasures have limitations in effectively guaranteeing the sustainability of the defense information system. The other is that it is difficult to maintain the continuity and sustainability of defense missions because it is impossible to implement safe telecommuting in the closed network-based South Korean defense network environment. In the situation of the spread of infectious diseases such as COVID-19, there have been cases where the information systems of private and public institutions could not perform services normally. This has made it necessary to study ways to ensure the sustainability of the defense information system so that it can continue to perform defense missions in the face of infectious diseases [12–14].

The goal of this study is to derive a plan to maintain the sustainability of defense information systems against non-traditional threats such as infectious diseases. There is a demand created by infectious diseases for a method to support remote non-face-to-face work performance. In this study, sustainability is defined as the ability of an information system to continuously provide services even in the event of the spread of infectious diseases such as COVID-19 and traditional natural disasters. Maintaining 24-h availability and sustainability of defense information systems supporting military operations is paramount. Therefore, various measures must be devised to ensure the sustainability of the defense information system in any harsh environment. This is because, in a situation such as South Korea facing an adversary, if decision-making is delayed even by a second, it will be difficult to respond in a timely manner to a missile attack from an adversary.

Existing papers describe a safe telecommuting system in an environment connected to the commercial Internet. However, we present a telecommuting system that guarantees work continuity and reliability so that there is no mistake in decision-making by meeting stronger security requirements than civilians in the defense network consisting of a closed network. In addition, other papers presented a conceptual diagram of the system for telecommuting [15,16], but we decided to apply the system as an experimental project in the actual organization A and designed an actual system diagram for this. Moreover, this study proposes a network configuration that logically connects a closed network and the commercial Internet by using VDI, VPN, and DMZ technologies in combination. Unlike other studies presented on a conceptual level, it is designed in a practical way based on actual experimental projects.

This study proposes a safe and efficient non-face-to-face work environment in situations such as COVID-19 to ensure the continuity and sustainability of defense work. In addition, the network configuration proposed in this study can logically and safely connect the Internet and the closed network while achieving a physical separation effect, which will contribute to the safe interworking of heterogeneous networks.

2. Related Work

2.1. Non-Traditional Threat Study

The Delphi method targeting experts selected cyberattacks (cybercrimes such as hacking, national cyber warfare) as the number one threat factor [17]. When non-face-to-face work is activated due to COVID-19, this trend will increase. In such a non-face-to-face work environment, network-based stability and reliability must be guaranteed, and a lot of time and effort are required to implement it.

2.2. Infectious Disease Threat Research

The difficulty of electrification due to operational problems in the supply chain was viewed as a problem to be resolved by Lee et al., 2020 [18]. Oh (2020) [19] emphasized the importance of securing the reliability and safety of cyberspace due to the increase in non-face-to-face contact. Since the number of connection points increases and the complexity increases exponentially, managing the work environment in the conventional way in terms of cyber security reduces work efficiency and may cause new security problems such as information leakage. The situation in which cyber considerations and operational efficiency and effectiveness must be considered at the same time will continue. Redundancy of all systems and dual control is the best way. However, there are practically difficult problems such as budget and manpower. Therefore, it is necessary to pay attention and effort to how to optimize it to achieve the desired effect.

2.3. Case Study

2.3.1. Financial Institution Case

Financial institutions must comply with the information protection control in accordance with the Electronic Financial Supervision Regulations of the Financial Supervisory Service [20,21]. Based on the environment of the institution, the emergency response system is operated according to the establishment and application of independent remote non-face-to-face system access control and the BCP. We establish a remote non-face-to-face (telecommuting) operation plan, define emergency situation standards as shown in Tables 1 and 2 in disability, disaster, strike, and terrorism, and operate telecommuting by situation.

Table 1. Criteria for social distancing.

Division	Level 2~3	Division
Telecommuting rate	25%	Separate notice
System access target	Inaccessible (biometrics)	Accessible (QR authentication)
Account access target	Pre-approval	Telecommuting target all

Table 2. Criteria for closing workplaces.

Division	No Closure	Floor Closure	Building Closure
Telecommuting rate	25%	Entire target floor	Entire target building
System access target	Inaccessible (biometrics)	Closed floor accessible (QR authentication)	Closed building accessible (QR authentication)
Account access target	Pre-approval (Payment terminal)	Telecommuting target all	

In terms of system and technology, security measures were devised by applying additional authentication methods such as user authentication and encryption to prevent illegal remote access. mOTP was additionally applied to the authentication method of ID and password. By allowing access only to domestic IPs, foreign IPs are blocked, and access is allowed only to public IPs registered in advance. On the PC at home, the USB type external storage medium was blocked, and the local printer was blocked. The external terminal for remote access and the system for internal business perform section encryption communication. In the communication section, encrypted communication of SSL VPN (virtual private network) is applied, and in the internal entry section, a firewall is operated to block unintentional access.

2.3.2. Public Institutions

In a situation where infectious diseases such as COVID-19 are spreading, we have established a non-face-to-face work system and are shifting to telecommuting and teleworking. A BCP was established to respond to infectious disease situations and an emergency response system was operated [22]. In order to reduce the density of people in offices, it is mandatory to implement shift telework at an appropriate ratio for each department. Telecommuters create conditions for telecommuting by making work-related calls and installing GVPN network environments. In addition, the smart work centers are established and operated based on the smart work activation promotion strategy of the Ministry of Public Administration and Security [23].

Guidelines for non-face-to-face work performance have been established, and they provide safe remote work and video conferencing implementation guidelines and checklists for security [24,25]. Remote work is performed as shown in Figure 1 through the cloud-based government remote work service (GVPN + G-Cloud). Some institutions perform remote, non-face-to-face work in a cloud-based VDI environment. The Ministry of Public Administration and Security performs work in a remote workspace through the establishment of a smart work center [26].

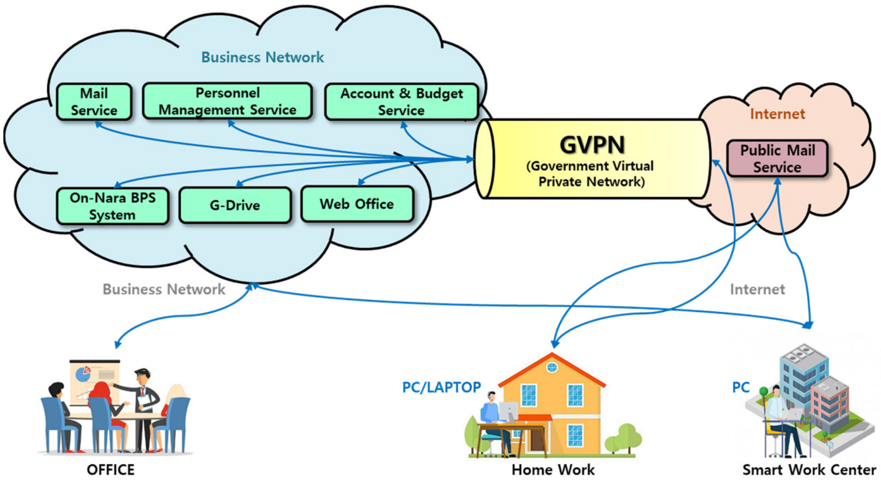

Figure 1. Systems and technologies in public institutions.

2.4. Implications

From the perspective of the work process, a systematic manual is needed to establish an active response plan for the disruption factors of the military information system in preparation for disasters, including the spread of infectious diseases. For example, the BCP of public institutions and enterprises. In order to be effective, such a business continuity plan must include the training cycle, scenario, priority target, and improvement plan for training results. In terms of related regulations, it is necessary to overcome the restrictions on the performance of essential personnel of the military information system in a situation where the duration of an infectious disease such as COVID-19 is prolonged. It is necessary to expand institutional infrastructure such as defense regulations and guidelines for the conversion of non-face-to-face tasks, such as remote work measures to convert to non-face-to-face tasks. From the perspective of personnel, organization, and education, it is necessary to secure a systematic response strategy through the establishment of a military-only organization to systematically and preemptively respond to infectious disease crisis situations. From a system and technology perspective, it is necessary to take a good look at the case of teleworking by the U.S. military and the transition to teleworking by major national and public institutions that followed the existing network separation policy. Our military also needs to come up with a system environment and security measures for remote non-face-to-face work, for example, a biometric-authentication-based remote access system. In addition, it is necessary to apply the non-face-to-face work performance method in Korea and domestically by reflecting the characteristics of the relevant institution and work rather than by comparing the advantages and disadvantages of each institution.

3. Defense Environment Status

It is necessary to support the systematic management and response of the defense information system to operate under the spread of infectious diseases. This is because a lot of confusion and difficulties arise when a real situation occurs. In case of self-quarantine of key personnel due to direct or indirect contact with an infectious disease, normal work performance is restricted. Relevant organizations operating the defense information system are conducting limited training such as system conversion, but there is no basis for this and it is being conducted unplanned. It is necessary to have a system environment for remote non-face-to-face business performance. The remote work environment through the commercial Internet should take measures to ensure security. Currently, only the indirect interworking method is allowed in the directive as shown in Table 3 for the interworking method between the Internet and the national defense network.

Table 3. Interworking method between the Internet and the defense network under the current guidelines.

- ○ Defense Security Service Ordinance Article 134 (Interworking with Information and Communications Network)
  - Mandatory indirect interworking through interlocking equipment is mandatory for collaboration between users with different security clearance levels.
- ○ Defense Cyber Security Ordinance (Defense Information System Protection Standards and Protection Requirements)
  - Indirect and direct linkage is possible if the confidential grades are the same (Defense Network ↔ Defense Network/Battlefield Network ↔ Battlefield Network), and the criteria are presented so that only indirect linkage is possible if the users' clearance levels are different (Battlefield Network ↔ Defense Network).

Clear standards for the new linkage method (using VDI technology) according to the development of ICT are insufficient. The standard is unclear to classify the interworking method using VDI technology into direct and indirect methods. There is no clear difference between the direct linkage method and the indirect linkage method in the Defense Security Work Order and the Defense Cyber Order. The standard for classifying the interlocking method is ambiguous. The indirect interworking method is a method of interworking systems with different security (secret) levels by maintaining the characteristics of physical separation of networks [27]. The interworking method using VDI technology is not described in the Ordinance and Ministry of Defense guidelines.

4. Non-Face-to-Face Business Execution Plan

4.1. Basic Requirements

In case of an infectious disease situation or emergency, it is necessary to ensure the continuity of work without restrictions on time and place. In addition, it is necessary to define the tasks to be performed externally, distinguish between users and tasks that can operate in a commercial Internet environment, identify which tasks must be performed flexibly in real time, and consider the work performed by each user (decision maker, researcher, manager, etc.). Technical and security aspects must also be considered at the same time. Secure connection must be ensured to the national defense network and commercial Internet, e.g., through logical network separation using VDI technology. Moreover, it is necessary to establish measures to prevent data leakage and security accidents.

4.2. Defense Non-Face-to-Face Task Execution System

4.2.1. Composition

The configuration diagram of the Internet-based remote non-face-to-face work plan is shown in Figure 2 [28]. The procedure for a remote worker connected to the Internet to access the information system located in the national defense network is as follows:

1. A remote worker connected to the commercial Internet uses the VPN client installed on the remote PC to connect to the VPN server operating in the DMZ section.

2. The VPN server authenticates the VPN user for secure network connection for remote work (two-factor authentication can be applied for strong security).
3. After the secure network is connected through VPN, the virtualization server requests authentication to the authentication server to confirm the authorized remote worker.
4. The virtualization server requests a virtual desktop from the management server to provide an environment that can perform remote work in a virtual space to a user who is properly authenticated as a remote worker.
5. The management server allocates pre-registered privileges and appropriate work environment to the virtual desktop to the authenticated user.
6. The remote worker uses the assigned virtual desktop to access the closed network and safely perform the authorized work.

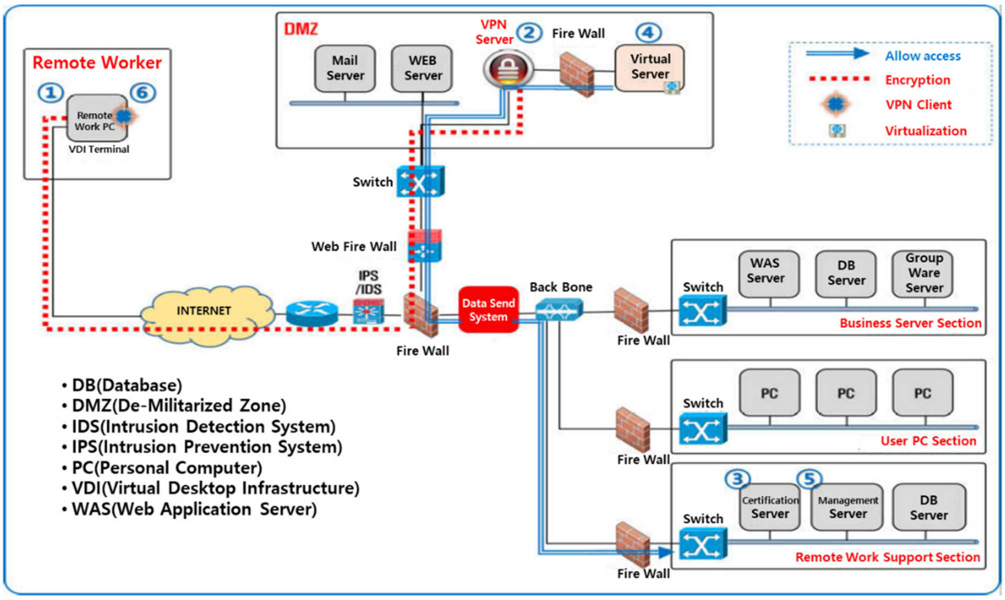

Figure 2. Non-face-to-face work system network configuration diagram in a heterogeneous network.

4.2.2. VDI Technology Applied

The network interworking method through VDI technology is known as the most reasonable and safe method applicable to remote work. By installing a virtualized VDI in the DMZ and performing remote access via VPN, the characteristics of physical network separation can be maintained, and network efficiency can be guaranteed due to near real-time data delay. VDI technology does not exist physically, but it is a technology that can create another computer that runs inside a computer that actually works. The cloud server creates a VM by allocating promised resources (CPU, memory, etc.) to the authenticated user using VDI technology and creates a virtual desktop by running OS and programs on the VM according to the user's request. Based on the cloud, it configures the same virtual PC environment as a general PC on the VDI server and provides virtual desktop services that can be used from various devices through the network. Currently, VDI-related technologies include architectural technologies that virtualize networking, computing, and resources into a single location so that they can be further controlled by software and the development of various operating systems and HW technologies related to DaaS. VDI technology is being actively introduced as a way to increase the availability and security of work. Through these VDI and DaaS technologies, it is possible to overcome the time and space constraints of a physical PC and provide a terminal use environment to users. Desktop management such as patching, backup, and upgrade is performed centrally, making it easy to manage and maintain. Unlike a physical PC that directly stores and manages data, the security is improved by storing and managing individual data in the cloud storage instead of storing it in the PC. It is easy to secure business continuity by promptly providing a new desktop in the event of a failure or disaster. By overcoming the constraints of time and space, the desired information can be accessed at anytime and anywhere, expanding work mobility. VDI technology is classified into text, image, and video according to the properties of the screen. Depending on the classified attributes, text may be compressed without loss, images may be compressed in JPEG Turbo format, and videos may be compressed in H.264 or MPEG-2 format to reduce CPU usage and network traffic. The data usage between video transmission for VDI solutions used commercially was measured and compared as shown in Figure 3. The size of the bandwidth used in the case of remotely playing and watching videos through VDI of companies T and V, which are used commercially, was measured. In the case of Company V, a bandwidth of 4.9 MBps was required to transmit a 480p (SHD)-level video. In order to transmit 720p (HD)- and 1080p (FHD)-level video, a bandwidth of 9.3 MBps was required. In the case of Company T, a bandwidth of 1.94 MBps was required to transmit an SHD-level video. To transmit HD- and FHD-level video, bandwidths of 2.24 MBps and 3.2 MBps were required. Depending on the characteristics of the solutions, there may be differences in video specificity, but, in general, a bandwidth of 10 MBps is required for seamless remote viewing of FHD video. In particular, in the case of company T, the transmission speed of other companies was improved by applying a protocol developed in-house to specialize in high-definition video. In a general PC work environment that does not require high bandwidth such as video, VDI can be applied with relatively few network resources.

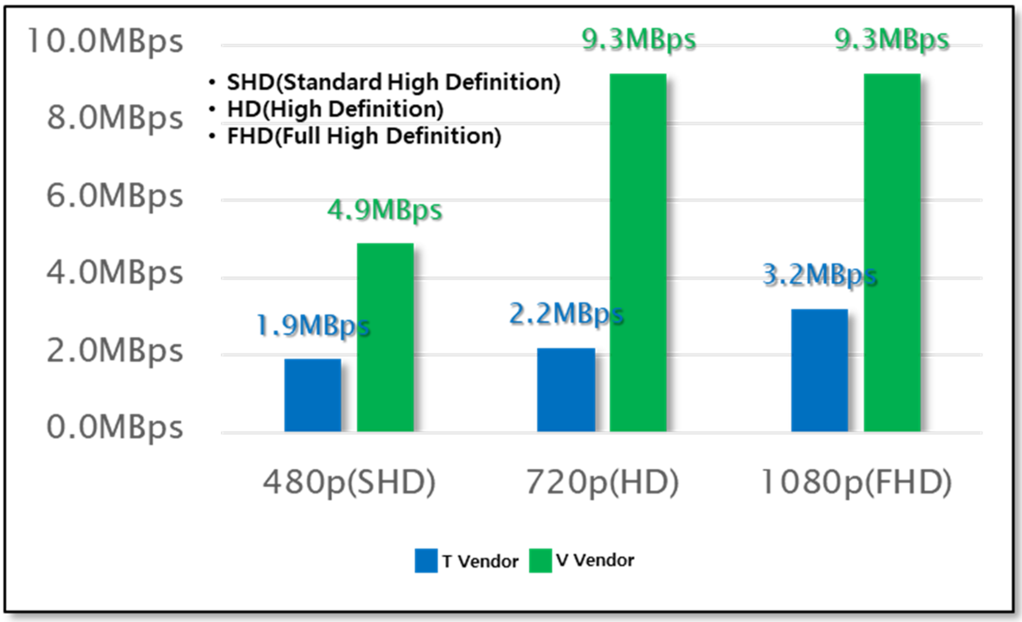

Figure 3. Comparison of bandwidth by video resolution.

In fact, the network usage measured in the environment with 400 VMs is shown in Figure 4, and the average bandwidth of less than 100 KBps per user was used in the measured bandwidth status. In addition, in the section showing the peak as the maximum value, a bandwidth of 3500 Kbps (4.375 MBps) is shown. Therefore, in an environment where 5 MBps is guaranteed by the QoS policy, VDI operation is possible without network expansion. In general, units at army battalion level or higher operate on a network that guarantees a bandwidth of 8 MBps or more, so it is possible to build a system by applying VDI technology without additional network facility expansion.

VDI technology provides the ultimate security environment through quantization. As a selective compression method according to screen properties, in addition to fast screen transmission at a low bandwidth, only coordinate values are transmitted, so even if a hacker steals it, the contents cannot be checked at all. In other words, since the information sent from the server to the client using a protocol specialized for security virtualization is transmitted as a screen value (number) rather than a Data Gran (streaming), it is impossible to steal and decrypt the information. If the necessary computer environment is established in the control room through this VDI technology, the mission can be safely performed in the same work environment at any network-connected place. The work environment can be configured in the same way as in the main control room by installing only the terminals necessary for the establishment of the preliminary control room and the smart work center. The remote work systems using VDI are recommended [28,29]. MND Defense Security Support Command suggested that it was the most reasonable and safe system. VPNs are exposed to vulnerabilities in management and operation rather than vulnerability in the technology itself. For example, not applying security patches and maintaining default accounts. It is necessary to test whether remote work of the defense network is possible with the VPN + VDI + DMZ combination. For this, first of all, it is necessary to revise the directives and regulations for the establishment of a system for remote work in the defense network. It should be implemented after system establishment, test operation, and stability evaluation for the revision of the ordinance.

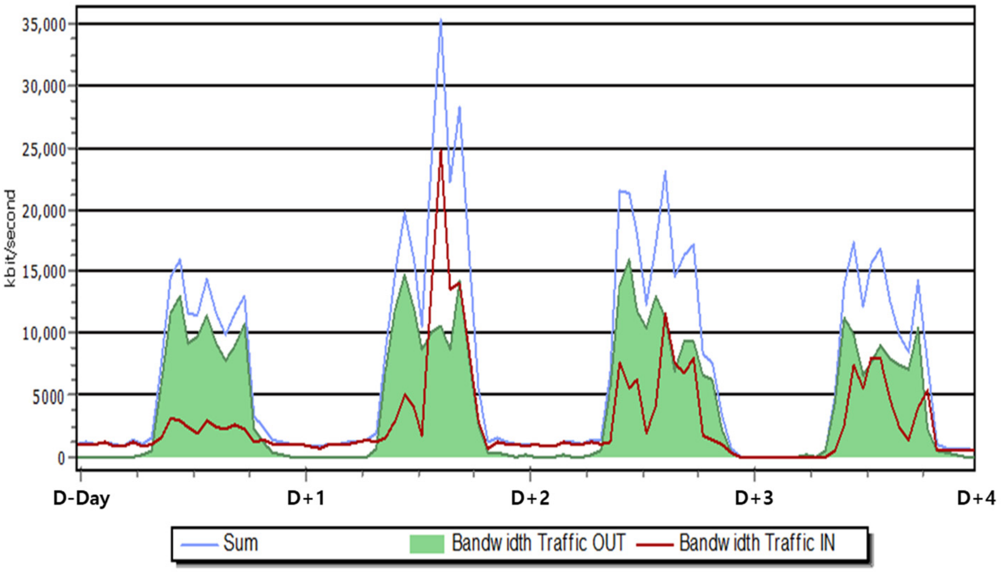

Figure 4. Bandwidth of VDI.

The results of this study have similarities with the TIC (Trusted Internet Connection) [30] presented by the U.S. CISA. The TIC provides the U.S. federal government's Internet connection standards to implement secure and reliable network connections. In terms of safely connecting heterogeneous networks, it has a similar purpose to the research results of this study. The TIC centrally monitors and manages mutual network connections in cloud and mobile environments at the U.S. federal government level. However, the method presented in this study focuses on ensuring physical connectivity by logically connecting the commercial Internet and closed networks without physical contact points. In the future, it is expected that the security functions pursued by TIC 3.0 will be combined with the network structure presented in this study to ensure more safety and reliability.

4.3. Workspace Development Concept (Case Study of Organization A)

It is necessary to establish the work that can be performed in the Internet business environment and the user concept as shown in Figure 5. For this purpose, institution A in the example does not directly carry out military missions but is an institution that conducts business in the defense domain. There are about 500 employees, and, just like the military base, they use the national defense intranet separated from the commercial Internet to perform networked tasks with the military base. In addition, the organization performs tasks connected to the outside through the defense Internet connected to the commercial

Internet. Organization A performs electronic approval, e-mail, and other various tasks through the defense intranet. Due to the characteristics of organization A, communication with the outside and work in the Internet environment are required, so the requirements for the Internet-based work environment are increasing. However, Organization A is also an organization that is subject to the Defense Security Service Order, and the task of editing or storing documents based on the commercial Internet is limited and it can perform tasks at the level of simple data retrieval. AS-IS does not allow business collaboration in the external Internet space of Organization A. TO-BE is to ensure the continuity of work in the Internet work space.

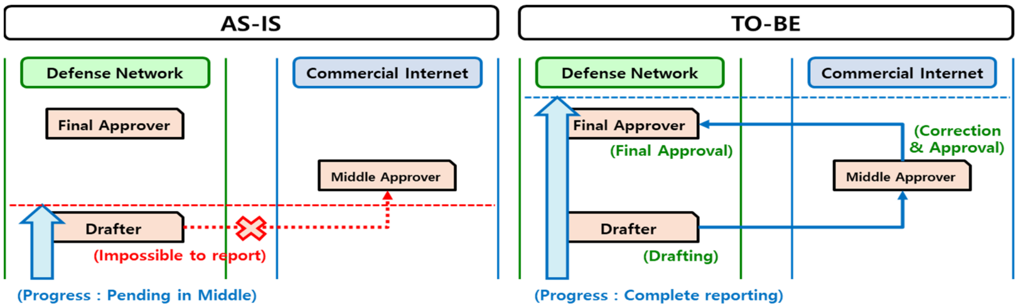

Figure 5. Concept of workplace development.

In terms of technical security, a logical network separation environment is established through the combination of VDI + DMZ + VPN. The remote work systems with VDI technology are recommended [A12]. In addition, the Defense Security Research Institute suggested that the most reasonable and safe way is to apply VDI technology for remote tasks [A13]. Based on the recommendations of the National Intelligence Service and the proposals of the National Defense Security Research Institute, an Internet-based remote non-face-to-face work plan as shown in Figure 6 was constructed.

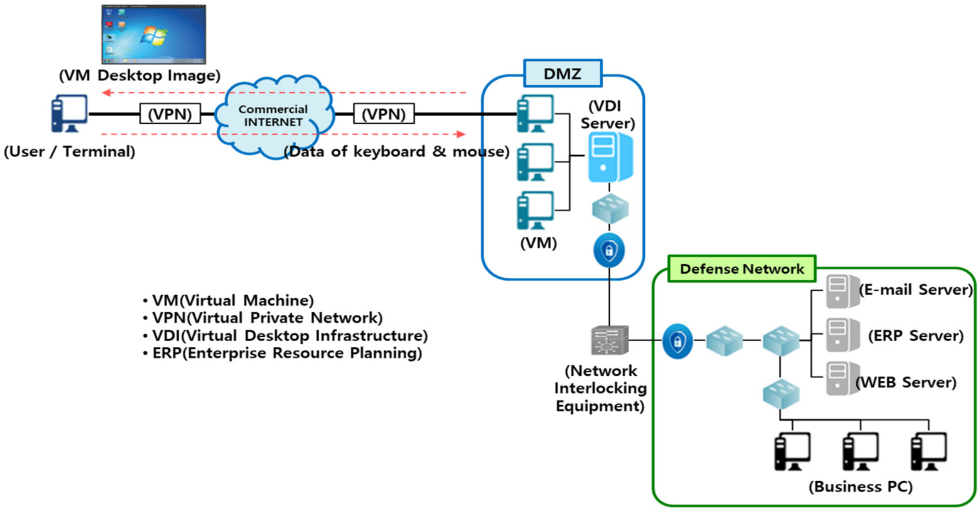

Figure 6. Proposed network configuration model for Internet-based remote non-face-to-face work.

The VPN is connected to the DMZ of the defense network through the commercial Internet, and the user is assigned a VM from the VDI server in the DMZ and is provided with the service within the defense network. Users remotely access VMs in the DMZ through the VPN. Since all services are executed in the VM in the DMZ, there are no files or other information transmitted and received over the Internet. In the VPN section, the image of the desktop screen of the VM is transmitted from the defense network to the Internet, and key information to operate the user's keyboard and mouse is transmitted to the defense network. Data transmitted and received in the VPN section is encrypted.

Therefore, even if data transmitted and received in the VPN section is obtained arbitrarily, the contents cannot be checked, and basically all operations are performed in the VM in the DMZ, so information leakage does not occur to the Internet. In addition, even if a user terminal existing on the Internet is hacked and becomes a zombie PC, dual authentication is required to access a remote system, and it is safe because there is no way to transmit data over the Internet. It is also impossible to hack the VDI server and the information system inside the defense network with keyboard and mouse key operation information transmitted from the Internet to the defense network. As a result, it is possible to provide services by safely linking heterogeneous networks with the combination of VDI + DMZ + VPN technologies. The military work system has been regulated and operated. In order to implement what is judged to be technically safe and effective, it is necessary to revise the Security-related Ordinance (ex. Defense Security Work Order, Cybersecurity Ordinance). The current directive lacks specific details on the standards to distinguish the direct linkage method from the indirect linkage method, and only the network linkage through "indirect linkage" of the storage method is allowed. It should be revised so that it is possible to connect the defense network through VDI (DMZ + VPN) from the outside. It would be better to build a regulatory sandbox concept before revising the ordinance and spread it to all areas of national defense after verifying the threat factors. In other words, it is better to build a remote work system using VDI technology temporarily (one year) for the defense network service of Agency A with the concept of a sandbox before revising the ordinance in the system establishment strategy and then test it. It is to allow and test the defense network and Internet linkage by applying VDI technology within a limited range. Since it is not necessary to perform all tasks on the Internet, it was necessary to check the necessary tasks for the Internet space in consideration of efficiency and to select priorities. An online survey was conducted, and the overall response results of the survey are shown in Figure 7. The majority of respondents (141 persons) among 282 respondents were analyzed as requiring the following functions: data exchange, messenger of A organization, mail, bulletin board, On-nara, administrative management, research management, integrated search, electronic library, etc.

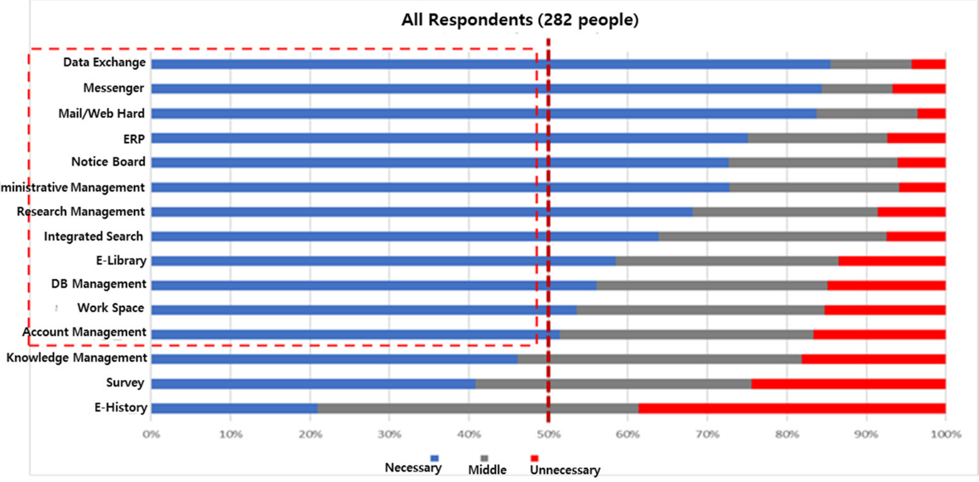

Figure 7. Results of all the responses.

If the job needs by job group are analyzed, the top five needs for remote work for research and managerial positions by job are as shown in Figure 8. In common, priority is given to those that do not cause a vacancy in work, such as messengers and data exchange e-mails.

Comprehensive analysis based on the survey response rate and other opinions shows that the data exchange system, mail, agency A messenger, and On-nara functions are required at a high rate in common in both job groups. This means that it is not a separate, independent telecommuting task during non-face-to-face work but rather requires real-time communication with in-house employees and maintaining work continuity based on the existing work environment (data). The reason is that the data exchange system is necessary to maintain business continuity in the internal and external networks, and the messenger of Organization A supports real-time smooth communication of employees between business processes. E-mail was said to be necessary for important and urgent work as internal notice, sharing of work data, and checking external e-mail.

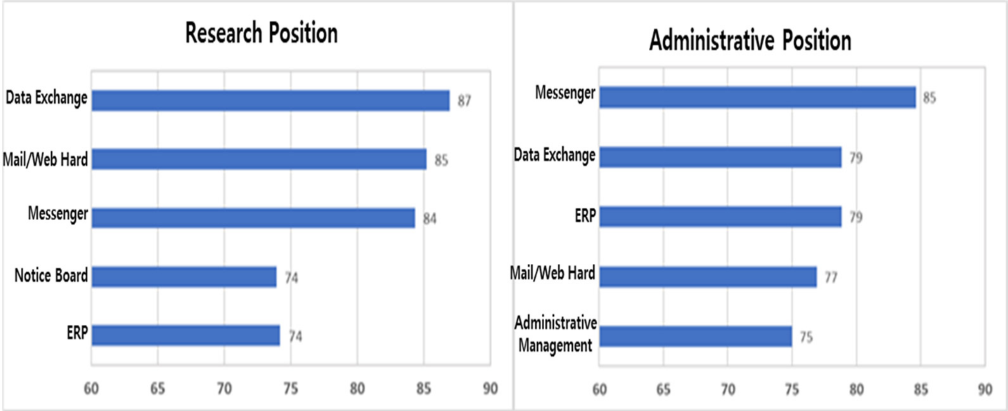

Figure 8. Results of analyzing the need for work by job group.

When divided into positions and general employees who have a lot of work related to decision-making, as shown in Figure 9, the data exchange system, mail, messenger of agency A, and the whole country function were commonly required at a high rate. This shows a similar result to the analysis of the need for each job group. However, there were many concerns about security through remote access. Overall, it can be seen that both positions and general positions require real-time work communication and maintain work continuity based on the existing work environment (data).

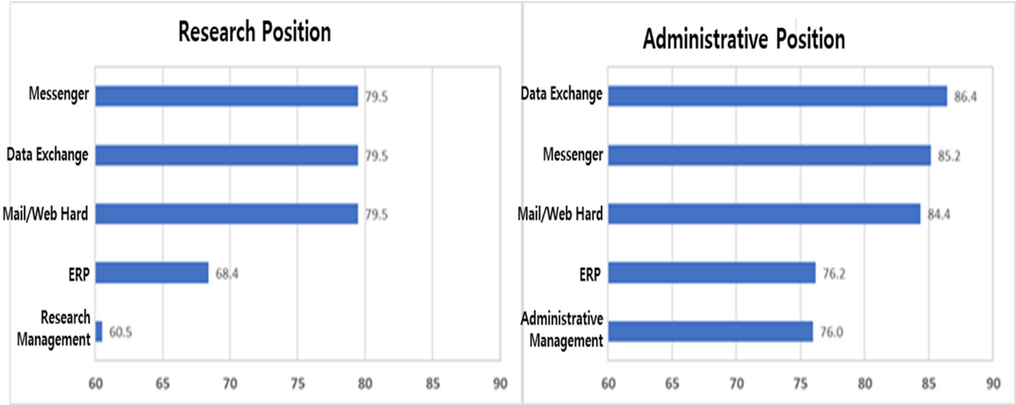

Figure 9. Results of analyzing the need for work by position status.

The demographic data of the survey respondents had little effect on the nature and characteristics of Internet-based non-face-to-face work.

5. Conclusions

Transition to a non-face-to-face work method in preparation for an infectious disease outbreak is not an option, it is a necessity. The private sector is rapidly shifting to a non-face-to-face work environment in preparation for large-scale absenteeism due to infectious diseases. Through the non-face-to-face work system, it was confirmed that work can be performed at the same level as usual. Companies are investing in facilities according to the needs of their members and changes in the environment, and this will continue. Currently, the national defense is in a situation where remote work is impossible due to the network separation policy. There will inevitably be cases where field work cannot be performed due to non-traditional threats such as infectious diseases. In this case, if an important situation occurs, it will be difficult to guarantee business continuity like a private company. Everyone recognizes that it is necessary to maintain business continuity in the face of infectious diseases and other situations.

This study suggested a method for establishing a system to maintain sustainability of the defense information system even under non-traditional threats such as infectious diseases. A safe and reliable defense non-face-to-face task execution system was proposed through the combination of VDI + VPN + DMZ technologies in a work environment that uses a defense intranet separated from the commercial Internet, such as national defense. In addition, through VDI technology, it was confirmed that the bandwidth that can be watched remotely even in 1080p (FHD)-level video transmission is guaranteed, and it requires a bandwidth of 5 MBps or less even in an environment where 400 VMs are actually operated. This indicates that the proposed system can be built and utilized without additional network facility expansion. In addition, through the case of Agency A, which is conducting defense work, we identified tasks that require collaboration in the Internet space by job character and position and confirmed that Internet-based work needs smooth communication in real time and continuity based on the existing work environment and data. Finally, it was confirmed that the system establishment and system maintenance such as the revision of the ordinance were prioritized in a limited range among various tasks. Through this, a method to maintain sustainability of the defense information system in any emergency environment was suggested.

COVID-19 was an unprecedented situation. The military decision support system must be available in all circumstances. It is important to establish relevant training and systems in peacetime and to validate procedures. The fact that the support procedure has been established is also the basis for having the driving force. Defense should consider both the efficiency of work and the effectiveness of security. Everyone is aware that the current situation is not a one-time event. Therefore, it is required that the relevant institutions put their heads together and make efforts to improve the current environment in a forward-looking manner.

Although this study analyzed the case of Korea, it can be applied to other countries as Korea's IT environment is built and operated according to international standards.

Author Contributions: Conceptualization, H.K., Y.S. and D.S.; methodology, H.K. and Y.S.; software, Y.S.; validation, H.K. and Y.S.; formal analysis, H.K. and Y.S.; investigation, Y.S., J.J. and K.K.; data curation, Y.S., J.J. and K.K.; writing—original draft preparation, H.K. and Y.S.; critical review and revision of paper, Y.S., J.J. and K.K.; supervision, D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This study was financially supported by the Seoul National University of Science and Technology.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

BCP	Business continuity plan
GVPN	Government virtual private network
VDI	Virtual desktop infrastructure
ICT	Information and communications technology
VPN	Virtual private network
DMZ	Demilitarized zone

HW	Hardware
DaaS	Desktop as a service
VM	Virtual machine
MND	Ministry of National Defense

References

1. *Establishment of a Functional Continuity Plan for the Disaster Management Agency; Joint with Related Ministries: Sejong, Republic of Korea, 2020*. Available online: Google www.google.com (accessed on 11 November 2021).
2. Kim, J.Y. *Military Role and Direction of Development against Non-Traditional Threats*; Korea Institute for Defense Analysis: Seoul, Republic of Korea, 2020.
3. Kim, D.H. *Recommendations and Implications of the U.S. Supervisory Authority's Pandemic Work Plan*; Financial Supervisory Service: Seoul, Republic of Korea, 2020.
4. Lee, Y.H. *Focusing on Educational Training and Simulation Analysis on the Direction of Development of Infectious Diseases and Military Response Capabilities*; Korea Institute for Defense Analysis: Seoul, Republic of Korea, 2020.
5. NSA Releases Two Security Guidelines as Telecommuting Drags on. Security News. September 2020. Available online: https://www.boannews.com/media/view.asp?idx=91347&kind= (accessed on 24 November 2022).
6. The Korea Atomic Energy Research Institute. KAI Hacking Channel VPN, is Growing Due to the Korean Version of the Exchange Crisis. Security News. July 2021. Available online: https://www.boannews.com/media/view.asp?idx=98828&kind=1 (accessed on 24 November 2022).
7. NASA Orders all 17,000 Employees to Work Remotely. Chosun Ilbo. March 2020. Available online: https://www.chosun.com/site/data/html_dir/2020/03/20/2020032000692.html?utm_source=naver&utm_medium=original&utm_campaign=news (accessed on 24 November 2022).
8. *COVID-19: Minimizing Critical Facility Risk*; Uptime Institute Intelligence Team: New York, NY, USA, 2020.
9. *Implementation Plan for Pandemic Influenzas*; Department of Defense: Washington, DC, USA, 2006.
10. *Defense Continuity Policy (DoD Directive 3020.26)*; Department of Defense: Washington, DC, USA, 2018.
11. *Extension of Maximum Telework Flexibilities (DoD Guidance)*; Department of Defense: Washington, DC, USA, 2020.
12. A Study on the Teleworking and Teleworking Act in Chile. Kotra Overseas Market News. April 2020. Available online: https://dream.kotra.or.kr/kotranews/cms/news/actionKotraBoardDetail.do?SITE_NO=3&MENU_ID=100&CONTENTS_NO=1&bbsGbn=322&bbsSn=322&pNttSn=181302 (accessed on 24 November 2022).
13. Spain Passes the Remote Work Act Amid the Re-Proliferation Crisis of COVID-19. Kotra Overseas Market News. October 2020. Available online: https://dream.kotra.or.kr/kotranews/cms/news/actionKotraBoardDetail.do?SITE_NO=3&MENU_ID=180&CONTENTS_NO=1&bbsGbn=243&bbsSn=243&pNttSn=184932 (accessed on 24 November 2022).
14. Due to the COVID-19 Crisis, Telecommuting Has Expanded. VOAKorea. March 2020. Available online: https://www.voakorea.com/a/coronavirus_teleworking/6029946.html (accessed on 24 November 2022).
15. *Briefing on Pending Issues Related to COVID-19 Financial Sector Response*; Financial Supervisory Service: Sejong, Republic of Korea, 2021. Financial Supervisory Service. Available online: https://www.fss.or.kr (accessed on 6 June 2021).
16. *Guidelines for Business Continuity Planning in the Event of an Infectious Disease*; Ministry of Trade, Industry and Energy: Sejong, Republic of Korea, 2020.
17. Song, E.H. Analysis of non-traditional security threat factors and countermeasures. *J. Inst. Soc. Sci.* **2016**, *27*, 247–262. [CrossRef]
18. Lee, S.M.; Han, S.J.; Lee, G.H.; Yoon, S.H. A study on the impact of COVID-19 in R&D of weapon system. In Proceedings of the Fall Conference of the Korean Society of Industrial Engineers, Jeonju, Republic of Korea, 5 October 2020; pp. 3740–3743.
19. Oh, I.S. Shadow of the untact era: The dailyization of cyber the threats. *Fut. Horiz. Plus* **2020**, *47*, 28–35.
20. *The Revision of the Enforcement Regulations of the Electronic Financial Supervision Regulations*; Financial Supervisory Service: Seoul, Republic of Korea, 2020.
21. *Environment for Remote Work (Telecommuting) to Prevent Business Interruption due to the Spread of the Novel Coronavirus within the Company and Quarantine of Infected Employees at Home*; 4th Information Protection Committee: Seoul, Republic of Korea, 2020.
22. *Guidelines for the Implementation of Flexible Work for Public Officials to Prevent the Spread of COVID-19*; Ministry of Personnel Management: Sejong, Republic of Korea, 2020.
23. *Smart Work Activation Promotion Strategy*; Ministry of Public Administration and Security: Sejong, Republic of Korea, 2020.
24. *Security Guide for the Introduction and Operation of Non-Face-to-Face Work Environments*; Ministry of Science and ICT: Sejong, Republic of Korea, 2020.
25. *Comprehensive Manual for Telecommuting*; Ministry of Employment and Labor: Sejong, Republic of Korea, 2020.
26. *Guidelines for the Use and Operation of the Smart Work Centre*; Ministry of Public Administration and Security: Sejong, Republic of Korea, 2019.
27. *Defense Information System Network Interworking Security Guideline*; Ministry of National Defense: Seoul, Republic of Korea, 2017.
28. *Remote Work Integrated Security Manual*; National Intelligence Service: Seoul, Republic of Korea, 2020.

29. *A Study on the Introduction of the Defense Online Telecommuting System*; Defense Security Research Institute of the Ministry of National Defense Security: Gwacheon, Republic of Korea, 2020.
30. Trusted Internet Connections (TIC). Available online: https://www.cisa.gov/tic (accessed on 24 November 2022).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.