Proposals for human resource development support to ensure Japan's "National Cyber Security"

"Collaboration and cooperation between private businesses and industry"

In recent years, challenges in cyber space have expanded dramatically in both breadth and depth, from crimes committed by individuals to threats involving nations, and there is an urgent need to improve response capabilities in the field of cyber security.

The "National Security Strategy," etc., decided by the Japanese government in December 2022, states that "Japan will improve our response capabilities in the field of cyber security to equal or exceed those of major Western countries." It is important to collect and share information at all stages, from peacetime to contingencies, and strengthen Japan's response capabilities in the field of cyber security as a whole, through cooperation with foreign countries, relevant government ministries and agencies, and private sectors.

In addition, "Based on the fact that policies in the field of cyber security will be centrally and comprehensively coordinated throughout the government, the Ministry of Defense (JMOD) and the Self-Defense Forces (JSDF) will raise the level of their own cyber security and promote initiatives that contribute to strengthening cooperation with relevant government ministries and agencies, critical infrastructure operators, and defense industries.

In view of the above, and for Japan to promote the realization of cyber security as one nation, we believe it will be essential for private businesses and industry to clarify issues and measures, that should be addressed in cooperation and collaboration, with regard to cyber security and the relevant roles and activities of the JMOD and JSDF.

Based on this understanding, we retired volunteers, who have been involved in cyber security while in government, asked other experts who were knowledgeable about cyber security to meet and study issues on which private businesses and industry should work together and cooperate, and to identify polices, goals, and other measures to be promoted in the future.

In particular, it is important to point out that "in order to smoothly strengthen cyber security, cooperation and support from private businesses and the industrial world is indispensable to develop human resources from a new perspective". We

hope that related businesses will unite to set up a forum for public-private discussions to realize these proposals.

Retired Volunteer members

Takashi Saito	Former Chief of Staff, JSDF Joint Staff
Shigeki Suzuki	Former Vice-Minister for Internal Affairs and Communications
Hisayoshi Ando	Former Vice Minister of Economy, Trade and Industry
Kazuhisa Shimada	Former Vice-Minister of Defense
Itaru Nakamura	Former Commissioner of the National Police Agency

<><><><><><><><><><><>

Recommendations by cyber security experts (report)

"Toward Smoothly Ensuring National Cyber Security"

I. Progress and focus of studies by National cyber security-related experts

From January to June 2023, an Experts Study Group (hereafter referred to as "ESG" – members listed at the bottom) met 13 times and has been working on issues based on the "National Security Strategy", "National Defense Strategy", and "Defense Buildup Plan" (hereafter referred to as "NSS"), which were approved by Japan's government in December 2022. The ESG considered the defense policies of major countries, such as "UK National Cyber Strategy 2022" and the "U.S. National Cyber Security Strategy", while examining the effects and influences Russia's invasion of Ukraine. Additionally, ESG members visited Japan Ground Self Defense Force's (JGSDF) Camp Kurihama, in Yokosuka – which is the site of JSDF's cyber security education.

The ESG recognizes that it is necessary for the whole country to work on how to respond to cyber incidents in which state actors of other countries are involved, or suspected to be involved, from peacetime to contingencies – and has made recommendations on how private businesses and industry should prioritize, cooperate, and work together to solve such problems.

Although the ESG's recommendations focus on these areas, the cyber security issues that Japan should address are not only countermeasures against the neutralization of weapons by cyberattacks, but also attacks on critical infrastructure, information warfare through the spread of false data (which is a characteristic of modern warfare), information warfare in the cognitive domain during peace time, and responses to cyber intelligence, etc. It should be noted that the ESG's discussions were held considering these new perspectives.

II. About the issues faced by cyber space

First, let's take a bird's-eye view of the issues faced by cyber space. The NSS states that "Japan's national interests will be seamlessly protected through cross-governmental policies in a wide range of fields, including cyber space, maritime & outer space, technology, and intelligence, to ensure the safety of our citizens both at home and abroad". The first pillar of the policy is to "improve response capabilities in the field of cyber security". This reflects the characteristics of the current security environment, in which the boundaries between military and non-military, contingency and peacetime, have become ambiguous – i.e., "hybrid warfare" has developed, and "gray zone" situations are constantly occurring.

In such a security environment, specific cyber security problems that Japan needs to deal with could include those listed below, which would be aimed at undermining Japan's decision-making system, command and direction systems, command and control (C2) of the JMOD and JSDF, and/or mission execution capabilities, such as the ability to exert force.

1. System shutdown due to DDoS attacks on information and communication systems, etc.

2. Destruction or shutdown of system functions; destruction, theft, falsification, or freezing of data due to hacking or virus intrusion onto information and communications systems.

3. Theft of IDs and passwords, leakage or disclosure of confidential information, threats, demands for financial gain, etc., by "phishing", etc.

4. Paralysis of social functions through system failures in telecommunications, electric power & other energy, finance, transportation, logistics, etc., due to single or combined means of the above.

III. Perspective of "cyber security"

1. Basic recognition

The NSS calls for "strengthening cyber security response capabilities to ensure the safe and stable use of cyber space, especially the security of the country and critical infrastructure."

As mentioned above, it is extremely important for the government to comprehensively consider possible cyber security incidents and responses to them, and for the government to take the lead in responding, while looking at the whole picture. The government is taking steps to resolve legal and organizational issues to make this possible.

On the other hand, the awareness of industry is still not enough. Although there is a shared sense of crisis regarding cyber crimes by non-state actors, it seems that the sense of crisis regarding cyber incidents involving state actors from other countries is low.

Most of Japan's information and telecommunications infrastructure has been built by private businesses, and as seen in the case of Russia's invasion of Ukraine, it becomes inevitable for businesses to have to respond to "cyber security incidents" involving state actors in order to protect themselves. Therefore, in this regard, private business and industries are also required to deepen their understanding of this situation and strengthen their proactive efforts for cyber security.

2. Responses during peacetime and deterrence of armed attack situations

The NSS states that "cyber attacks can disrupt or destroy critical infrastructure, interfere with elections in other countries, demand ransom, steal sensitive information, etc., even in the form of state-backed attacks during peacetime". Thus, cyber attacks related to cyber security are expected to undermine Japan's command and control functions, etc., during a time preceding a possible armed attack, and thereafter things might lead to a full-scale physical attack -- including more cyber "strikes" (e.g., "armed attack situation"). Therefore, it is required to be equipped with the ability to counter or stop cyber attacks even during peacetime. Such preparedness will also discourage the temptation of an adversary to launch a full-scale armed attack and deter contingencies. For this reason, it is necessary to continuously monitor cyber space to identify trends in anticipated cyber threats and signs of attacks.

3. Necessity of strengthening cooperation between related measures and international cooperation

The NSS states, "We will strengthen coordination with other policies that contribute to strengthening cyber security. Furthermore, we will continue to work

to strengthen intelligence collection and analysis in cooperation with allies and comrades, identify attackers and publicize them, and formulate international frameworks and rules".

In this regard, it is also important to support cyber capacity building in coordination with efforts to formulate international cyber norms and other related measures to improve the security environment.

Meanwhile, global companies are said to have responded effectively to cyber attacks during the Russian invasion of Ukraine. Considering the fact that the systems of Japan and industries, etc., depend on the systems of foreign companies, and the high level of cyber security capabilities of global companies, it will be important to create a mechanism to promote collaboration and to establish a closer cooperative framework with the governments of the countries concerned that have direct relationships with global companies.

In order to promote cooperation and collaboration with foreign governments and foreign companies in the field of cyber security, it is essential that a security clearance system for handling sensitive information be realized as soon as possible, not only by national and local governments, but also by businesses and industries that have access to sensitive information, under public-private partnership.

Thus, with regard to cyber security, we believe that it is necessary to promote international cooperation based on an awareness of the present status of the international framework, Japan's current state of cyber security capabilities, and its position in terms of security.

Based on the above basic recognition, the following issues have been identified as initiatives that should be particularly emphasized for the development of a cyber security "posture" and "system".

IV. Development of cyber human resources

In politics, government, industry, and academia, there is a need for top management to improve awareness of cyber security in order to be "completely prepared" and to develop human resources under continuous leadership.

On top of that, there is an urgent need to develop cyber personnel for JSDF, and it is also necessary to consider developing cyber personnel not only for JSDF but also for Japan as a whole, including the government and private businesses. In the past, cyber education in private businesses and industry seems to have been passive in terms of avoiding economic losses caused by cyber attacks. The key issues are: "development of human resources with cyber advanced capabilities" and

“expansion of the base of human resources and improvement of the environment for human resource development”. In other words, the enhancement of human resource development from two new perspectives, qualitative improvement, and quantitative expansion, is required to meet the demand for cyber human resources.

At the same time, it is also necessary to clearly position cyber duties as jobs for a new era that are different from the conventional ones, seek a common understanding among the public and private sectors, and better focus countermeasures and actions.

1. Development of human resources with advanced cyber skills

A framework is being studied by the government to determine how far to go in order to monitor and disable the cyberspace of the other side (e.g., an aggressor) as well as to protect one's own systems. As such, we are looking for “personnel with excellent practical skills to deal with individual cyber incidents” and “personnel who can look over the entire cyber issue and advise senior decision makers on what to do now”.

A. Educational cooperation and support by private businesses and industries

In the private sector and the industrial world, efforts to develop cyber security human resources began early, and there are also some companies which provide human resource development as a business on a fixed scale. In this regard, it would be effective to utilize human resource development services already available in the cyber security industry.

In particular, JMOD and JSDF have plans to train approximately 4,000 personnel assigned to cyber units and approximately 20,000 cyber personnel, including them, by 2027. We anticipate that greater cooperation with private businesses and industries will be necessary than ever before. Therefore, it is crucial for private businesses and industries to establish even closer relationships with JMOD in order to effectively respond to this demand.

B. Expanding the base of cyber human resources and improving the human resource development environment

When training cyber security personnel, it is assumed that the candidates to be trained will have a certain level of digital skills. However, it has been pointed out that there is a shortage of human resources with digital skills in Japan. To strengthen cyber security personnel, we believe that it will be important to expand the base of digitally skilled personnel and improve the human resource development environment. To that end, it is necessary to promote the following measures.

(1) Clarification of skills required for various abilities

First of all, it is necessary to analyze the various capabilities necessary to deal with cyber security incidents and clarify the skills required for those capabilities, as well as the curriculum elements, teaching materials, and exercises required to acquire them.

(2) Curriculum standardization and regular updates

On top of that, to maintain personnel who can respond to various cyber incidents, standard education curriculum elements for each field, function, and level of cyber security skills should be created. Based on this, we believe that it will be possible to gather and operate personnel with high-level skills across organizational boundaries, and that this will contribute to the improvement of organizational capabilities in cyber security. At the same time, it is also necessary to periodically update the curriculum as cyber technologies evolve.

(3) Ability certification system

In addition, competence level certification is necessary to clarify what kind of cyber security capabilities each person possesses. In Japan, the IPA has set seven skill levels in the industrial world, and there are certification systems for multiple security capabilities such as system audits. Internationally, there are global competence certification systems operated by prominent organizations such as CISSP, GIAC, and CISA, and Japanese cyber security personnel have also been certified.

(a) Examination of Japan's ability certification system that is internationally consistent

In order to collaborate and cooperate with allied countries and others on cyber security, it will be required to match the capability levels of their cyber personnel. It is also necessary to set skill levels, and to have a certification system to confirm skills that have been acquired, from the perspective of improving organizational capabilities and facilitating inter-organizational cooperation. For this reason, it is necessary to continue to consider how Japan's capability certification system should be internationally consistent, taking into account the characteristics of cyber threats and the security environment in Japan, while referring to the capability certification systems in Japan and abroad.

(b) Maintain ability certification

Since technological progress in the cyber domain is rapid, it is important to constantly brush up on skills and maintain a certain skill-level even after certification of competence. A common certification of skills is necessary for

identifying human resources and for cooperation between the public and private sectors.

In particular, for the certification of competence, consideration should be given to setting levels based on practical experiences or combining various certification systems. Additionally, from the aspect of incentives for ability certification, it is necessary to consider the positive treatment within the organization of those who have been certified.

(4) Clear positioning and treatment of cyber duties

There are examples of valuable personnel with cyber security capabilities not being effectively utilized. It is necessary to improve the understanding of managers and the general public regarding the importance of the job, and to create an environment in which the job is properly evaluated by other people. Specifically, for example, it is important to make jobs attractive in terms of hiring conditions, career paths, and job titles. In particular, human resource management and career advancement of cyber personnel in cyber-related jobs, including crisis management, should be established to avoid deterioration of skills due to assignment of cyber personnel to other jobs.

(5) Construction of human resources bank, "revolving door" system, promotion of exchange opportunities

In order to continue to secure cyber personnel on a certain scale, it is necessary to develop human resources and accumulate practical experience by enabling them to move back-and-forth between ministries and agencies and the private sector. To that end, we believe that it is necessary to realize a "revolving door" system that allows cyber security personnel to move between the public and private sectors, to grasp the current situation of human resources (i.e., personnel data bank), and to maintain the sustainability of exchanges. It is also desirable for the private sector and industry to increase opportunities for exchange, such as more active participation in government-sponsored cyber exercises (and education).

(6) Promotion of e-learning

Given the limited number of instructors who can effectively educate the ever-evolving digital knowledge, we believe that the use of e-learning, including CBL (Computer Based Learning), is an effective means to acquire basic cyber security knowledge and other skills.

In order to train a large number of personnel in a short period of time, a difficult situation can be imagined in terms of providing training facilities, equipment, and faculty capacity, depending on the group training. There are concerns that removing JSDF or company personnel from their jobs to undergo group training

may interfere with operations or business activities, and it would be more effective to have them undergo training while they are at their workplaces.

In order to expand the base of human resources, e-learning is necessary. However, the content of e-learning should not be merely passive, but also be designed to enable practical training such as “CTF” (Capture the Flag) exercises.

For example, e-learning could be used to provide a certain level of qualification to beginners in the public and private sectors, or e-learning could be used to reskill former employees who were involved in cyber-related work, program development, etc., in the past.

(7) Issues to promote exchanges with foreign universities for the development of global human resources]

In the field of cyber security, it is generally pointed out that the lack of a common curriculum with overseas universities hinders exchanges with universities in the United States and other countries.

In order to ensure cyber security in cooperation with allied countries, it is important to study at overseas universities, acquire knowledge and skills, and create personal connections. At the same time, it is necessary to improve the system for accepting exchange personnel from Japan and mutual recognition of credits with overseas universities.

V. Human Resources to Support “Active Cyber Defense” and Building a Comprehensive System

In general, cyber security incidents have inherent ambiguity as to whether they are cyber attacks or system malfunctions, as well as the ambiguity of the implementing (attacking) entities. It is extremely important to have personnel and systems that are capable of understanding what is happening in cyber space today, including attribution (identification of attackers). In particular, there is a need for a considerable number of “personnel who can grasp and direct the overall situation” and “personnel with excellent practical skills who can deal with individual cases.”

In order to make "active cyber defense" more effective, it is necessary not only to develop advanced cyber human resources, but also to build a comprehensive framework that supports it with legal aspects and systems that use AI, etc., which are rapidly advancing.

VI. Exercise environment for coordination and cooperation between the government and critical infrastructure operators

Ensuring the cyber security of various critical infrastructure systems supported by private business operators is primarily the responsibility of each business operator, and they are required to take security measures and be prepared to deal with cyber incidents.

On the other hand, the government needs to assess and deal with how the emerging cyber incidents affect critical infrastructure and national society.

Therefore, it will be a challenge to enhance collaboration between government and private entities in terms of protection, particularly for critical infrastructure operators and defense industries, from the perspective of cyber security.

Currently, private businesses and industries are individually promoting the development of cyber security personnel. Public institutions such as NICT and IPA are providing cyber security education systems and exercise platforms; and collaborative efforts between the government, private businesses, and industries are beginning -- such as CSIRT.

However, there is currently no collaborative implementation of scenario development, cyber education, personnel development, training, and exercises, considering cyber incidents ranging from “gray zone” situations to contingencies.

In order to address cyber security incidents, it is necessary to establish an environment where joint education, training, exercises, and other activities can be conducted, based on a common scenario, involving the national government, the JMOD and JSDF, private businesses, industries, and, if necessary, allied countries.

VII. Strengthening public-private partnerships

1. Necessity of national integration through public-private partnership

From the perspective of cyber security, there is a possibility that cyber attacks, in particular those carried out by controlled states, will involve sharing and coordinating areas of expertise, and collaborating to take various measures. It is difficult for a single company or organization to respond to such attacks alone. From the perspective of public-private partnerships, as seen in the example of the Japan Cyber-crime Control Center (JC3), some progress has been made. But there still is a need to integrate power as a nation through public-private partnerships, including how to strengthen cooperation between government ministries and agencies.

2. Security clearance issues in public-private partnerships

When the public and private sectors collaborate on cyber incidents, it is inevitable to obtain security clearances from private citizens and non-disclosure agreements between the government and businesses. We believe that it is necessary to have a proactive mindset that security clearances are essential for public-private partnerships to strengthen cyber security.

A. Guidelines for provision of information from the government

It is necessary to establish a management system that enables effective use of various cyber-related data. In doing so, it is important to clarify the sensitive information that should be protected, but to also share as much necessary information as possible, since data on cyber threats is essential for defense even in the private sector. In addition, in order to promote technological development related to cyber security, it is necessary to establish guidelines for the government to actively provide cyber-related information, including incident data, which cannot be obtained by the private sector.

B. Appropriate environment development for obtaining security clearance

With regard to cyber security, it is necessary to educate corporate managers and shareholders that security clearances by private-sector personnel and nondisclosure agreements with the government are indispensable in order to address cyber security through public-private partnerships. At the same time, it will be required to create the necessary administrative environment, such as providing appropriate information and evaluations to those who have obtained security clearances.

C. Building a framework for providing information from businesses and industries

There is also a reluctance to share information from private businesses and industry to the public (e.g., when cyber incident occurs) in relation to shareholders, including corporate reputation risk, or in relation to the Personal Information Protection Law. However, to improve this situation, it is necessary to support the activities of companies by taking the necessary institutional improvement measures, such as establishing rules for information handling on the government side and establishing exemption provisions for companies.

D. Fostering relationships of "visible" trust between the public and private sectors

Effectively addressing the security clearance issue does not solve all problems. It is important for the government and private companies to understand each other's roles and positions and to build a relationship of trust. A framework must be built

for constant consultation between the government and private companies to share and provide not only confidential information but also information related to cyber incidents such as OSINT (Open Source Intelligence) and other data related to cyber incidents, and to make steady efforts to foster a trusting relationship where both sides can “see each other’s face”.

E. Construction of a framework for strengthening cooperation with related private companies

In relation to paragraph D. above, it would be most effective to establish a framework for cooperation between government agencies, JMOD and JSDF, and private businesses and industry, and related private companies working together, rather than individually, with the government. In building such a collaborative organization, it is also necessary to consider its sustainability.

VIII. Recommendations for Smoothly Ensuring “National Cyber Security”

“Collaboration and cooperation between private businesses and industry”

The future response to "National Cyber Security" encompasses a wide range of issues, and the government is promoting various measures to enhance Japan's response further. The collaboration and cooperation of the industrial world are crucial for achieving more effective and timely responses.

We propose focusing on human resource development as a particularly urgent issue for industry collaboration and cooperation.

Recommendations (I)

Establishment of a framework for industry collaboration and public-private partnership

Various issues to ensure “National Cyber Security” are interconnected. Private business operators have their own areas of expertise and make individual judgments as to whether or not they are viable as businesses. But it is important to move forward and strengthen cooperation with the government from the viewpoint of protecting their own businesses as cyber threats become more serious.

1. Establishment of a framework for collaboration among cyber-related companies.

We recommend the creation of a sustainable framework that will serve as a core for the establishment and promotion of a cyber security "ecosystem" that includes: "information sharing among companies", "a certain/appropriate direction for business promotion", and "bridges between the public and private sectors", especially in relation to national security and defense.

2. Establishment of a Cyber Environment/System for Collaboration with Private Sector Businesses and Industries

To enable the private sector and industry to cooperate with the national government, the JMOD and JSDF in dealing with cyber security incidents, we recommend the development of an environment/system in which cyber personnel education, training, scenario creation, and exercises can be conducted jointly.

In order to achieve this, including the introduction of new education, exercise, and other systems, it is considered appropriate to pay attention to the following points:

A. Define the system's purpose (e.g., education, training, exercises, research

and development, etc.).

B. Determine the scope of participants (e.g., JMOD, JSDF, critical infrastructure operators, defense industry, universities, etc.).

C. How to establish a relationship with existing systems (e.g., official cyber education and exercise systems, systems provided by private companies, etc.).

D. Consider options for international cooperation with allied nations, etc.

E. How to utilize the platform for future cyber-related technology development.

F. Ensure flexibility and redundancy to respond to rapid changes in technology and the environment.

3. Establishment of regular, face-to-face meetings

It is natural to expect increased coordination within the government to address the increasingly complex challenges of cyber space. However, cooperation between the government, which encompasses legal and intelligence sectors, and private companies with technical expertise, will become even more critical. To achieve this, it is essential to first enhance the understanding of cyber security among top management levels, which could then establish a visible and trusting relationship between the government and the private sector.

At first glance, it may seem obvious and simple to establish a forum for information sharing between the public and private sectors through a framework for cooperation among cyber-related companies, as mentioned above in paragraph 1., rather than just between individual companies. However, to institutionalize this as a system, it is important to consider its relationship with existing frameworks for government-private sector communication, avoid redundancy, and build a relationship of trust by incorporating business management know-how and with a "win-win" characteristic.

Recommendations (II)

The development of advanced human resources related to "cyber security" (Qualitative improvement)

In the past, cyber talent development in the industry has predominantly focused on preventing unauthorized access, eliminating virus intrusion, defending against theft of authentication credentials, and protecting against economic losses such as ransom and exploitation, with the aim of ensuring business continuity. However, in addition to these aspects, the future will emphasize the importance of "qualitative improvement" of personnel who approach national cyber security.

The "System Communications and Cyber School" (hereinafter referred to as "Cyber School") of JSDF will be mainly responsible for the development of excellent/practical human resources capable of responding to various and individual cases, as well as providing basic education.

However, in addition to strengthening internal training within JMOD and JSDF, outsourcing to private companies is expected to be required more than before. Therefore, it is necessary to enhance the collaborative support system within industry to meet these demands.

Based on the results of the government's study of "Active Cyber Defense", it is recommended that the educational curriculum of each company be appropriately modeled (e.g., organized based on standard items).

Furthermore, it is important to consider the versatility of educational curricula, enabling the education of personnel not only within JSDF but also to include the police and critical infrastructure operators. This will contribute to a more comprehensive development of talents across multiple sectors.

Recommendations (III)

Expanding of human resources and creating a conducive environment (Quantitative expansion)

To cultivate highly skilled professionals, it is essential to expand the base of the talent pyramid and establish a conducive environment for talent development. To achieve this, measures such as facilitating access to education, standardizing curriculum elements, and harmonizing certification processes are necessary.

It is important to expand cyber human resources and improve the environment for fostering such specialized personnel in the entire country by promoting the following initiatives centering on the aforementioned "Framework for Cooperation among Cyber-related Companies".

1. Clarification of Skills Required for Various Capabilities

We recommend that the various capabilities required to deal with possible cyber security incidents, including "active cyber protection," be analyzed, and that the skills required for these capabilities and the curriculum, teaching materials, and exercises necessary to acquire these skills be clarified.

2. Standardization and Regular Updating of Curricula

To maintain personnel capable of responding to various cyber incidents, it is recommended to extract and create standardized elements and items for educational curricula, and items be identified and developed by discipline, function, and level of cyber security-related skills. It is also necessary to regularly update the curricula in accordance with the evolution of cyber technologies.

3. Internationally Aligned Certification System for Our Country

In order to collaborate and cooperate with allied countries in the field of cyber security, it is necessary to align the competence levels of cyber personnel and establish a certification system that verifies their skills. Having an internationally aligned certification system for use by Japan is crucial for enhancing organizational capabilities and facilitating inter-organizational collaboration. Therefore, it is recommended to continuously examine the establishment of an internationally aligned certification system for our country, while considering domestic and international competency certification systems, and the characteristics of cyber threats and security environment.

4. Clear Positioning and Treatment of Cyber Roles

To effectively utilize valuable personnel with cyber security capabilities, it is necessary to improve the understanding of the importance of such roles among managers and the general public and ensure that they are properly recognized by

many people. It is also important to make cyber security work attractive by specifying hiring conditions, career paths, job positions, and other factors. In particular, it is recommended that personnel management and career advancement of personnel in cyber-related jobs, including crisis management, be established to avoid deterioration of their abilities due to assignment to other, non-cyber-related jobs.

5. Establishment of Talent Banks, Implementation of "Revolving Door" System, and Promotion of Exchange Opportunities

To continuously secure an appropriate and constant level of cyber personnel, it is necessary to facilitate talent development and accumulation of practical experience through movement between government agencies and the private sector. To achieve this, it is recommended to implement a "Revolving Door" system that allows cyber security personnel involved in national security to move between the public and private sectors. Additionally, it is suggested to establish a “personnel data bank” which captures the current situation of personnel. It is also recommended that private businesses and industry increase opportunities for interaction, such as more active participation in government-sponsored cyber exercises (and education).

6. Promotion of e-Learning

To expand the talent pool, “e-Learning” is believed to be effective. However, the content of e-Learning should not be limited to being passive but should also include practical training such as participation in “Capture the Flag” (CTF) cyber defense exercises. For example, e-Learning can be used to provide a certain level of certification or risk training to beginners, in both the public and private sectors, or to offer retraining programs for personnel with previous experience in cyber-related jobs or programming development. It is recommended that relevant companies actively expand and provide e-Learning opportunities to support this goal.

IX. Conclusion

As members of the Experts Study Group (ESG), we express our sincere hope that the recommendations presented above will be swiftly implemented. We firmly believe that recognizing the cooperation and collaboration with the private sector and the industrial world is crucial in developing human resources from a fresh perspective. By doing so, we can ensure the smooth establishment and effective implementation of cyber security measures.

30 June 2023

Experts Study Group Members:

Nobushige Takamizawa

Tatsuzo Tanaka

Yasuhiko Taniwaki

Ikuo Misumi

Kenichi Sakurazawa

Takamichi Saito