ISSN 2186-6902

No. 20 December 2019

NIDS Journal of Defense and Security

NIDS

National Institute for Defense Studies, Tokyo

The National Institute for Defense Studies (NIDS) is the Ministry of Defense's core research and educational institution, conducting policy, theoretical and regional studies in the area of defense and security, while also providing officers of the Self-Defense Forces with strategic, collegelevel education. In addition, NIDS is in charge of administration of pre-war military documents, records and publications, and is considered to be the nation's foremost military history research center. *NIDS Journal of Defense and Security*, one of the institute's publications, is intended to promote research activity on, and public understanding of, security issues. Articles can be downloaded from <http://www.nids.mod.go.jp/english/>. Views expressed in the articles are solely those of authors, and do not necessarily represent the views of NIDS, the Ministry of Defense or the Japanese Government.

For more information,

Planning and Coordination Division,
The National Institute for Defense Studies (NIDS)
5-1 Honmura-cho, Ichigaya, Shinjuku-ku, Tokyo 162-8801
TEL: +81-3-3260-3011
FAX: +81-3-3260-3034
e-mail: plc-ws1@nids.go.jp

ISSN: 2186-6902

National Institute for Defense Studies, Tokyo

NIDS Journal of Defense and Security

No. 20 (December 2019)
ISSN 2186-6902

National Institute for Defense Studies, Tokyo

Replacement of the Military's Intellectual Labor Using Artificial Intelligence —Discussion about AI and Human Co-existence—*

ONO Keishi**

Abstract

The development of AI, which first began in the 1950s, has been carried out in a way that explores the logical thinking of humans using deductive or inductive inference, but this approach has become the potential and limitations of AI. The introduction of AI by the military, whose full-fledged trials began in the Second Boom of AI development in the 1970s, has today reached a level where AI can replace the thinking and decision making related to the command structure (military personnel). The introduction of such high performance AI will likely have a major impact on approaches to the military (structure and organization). However, AI, which was developed in pursuit of human logical thinking, faces with the weak point of "ad hoc response to inexperienced situations." However, such response is always required of the military (military personnel) on the battle front or at the scene of disasters. When viewed in this light, the ideal approach of the military (military personnel) for co-existence with AI comes into focus.

Introduction

Today, Artificial Intelligence (AI) is permeating into every corner of our world, and the military is no exception. The military's main interest in AI today focuses predominantly on the development and operation of Lethal Autonomous Weapon Systems (LAWS), or robots sophisticated by AI. From the invention of the spear in Stone Age (around 70,000 years ago) to the 21st century today, people have proactively used technological development for warfare and the development of weapons.[1] Debate over the development and operation of LAWS, too, is basically an extension of this. In other words, although these discussions focus on accountability and the pros and cons of entrusting decisions for attacks to autonomous weapons systems with lethal force, the basis of these discussions is that humans will proactively regulate and control LAWS. Improvements in AI performance may force a change in this paradigm in the future.

The purpose of AI development is to contribute to human's intellectual labor; yet, attempts to reduce the burden of this intellectual labor date back to the invention and use of calculating

* Originally published in Japanese in *Boei Kenkyusho Kiyo* [NIDS Security Studies], vol.21, no.2, March 2019. Some parts have been updated.

** Head, Defense Policy Division

1 See Ferrill Arther, *Senso no Kigen* [The Origins of War], translated by Suzuki Chikara and Ishihara Tadashi, (Tokyo: Kawade Shobo Shinsha, 1988), pp.24-48 for the development of prehistoric technology of weapons.

tools in ancient Mesopotamia.[2] In addition, modern computers are believed to have begun from the mechanical calculator that could perform four-arithmetic operations invented by Gottfried Wilhelm Leibniz.[3] Today's AI development, however, is largely different from these other technological developments. The main reason for this is the fact that AI technological development today eyes the replacement of intellectual human labor. In the case of the military, this means that the thinking and decision making of commanders and staff organizations can even be replaced with AI. Intellectual activities set mankind apart as the lords of creation, but in this sense, AI has the power to surpass humans.

AI, with its close to 70-year history, did not necessarily pose a threat to human's intellectual activities in the beginning. The development of AI that began in the 1950s has been pursued in a way that explores the logical thinking of humans using deductive or inductive inference. This history of development has become both the potential and the limitation of AI. As a result, this paper will look back on AI's development history as a civilian technology and then debate the replacement of the military's intellectual labor using AI and the co-existence of AI and the military (military personnel). Furthermore, advancements in AI (including Information Technology: IT) are ushering in great changes in military-industry relations, towards industrial superiority.[4] This paper does not cover military-industry relations, but this fact clearly demonstrates the extent of impacts from AI development.

1. From Supplementing to Replacing Intellectual Labor

Attempts to entrust human's intellectual activities to tools and machines have been made since ancient times. For the longest time, these attempts did not go beyond the domain of "supplementing intellectual work," but the aim of AI development is "replacing intellectual labor." Put another way, the problem was how to carry out abstract human logical thinking using a machine.

(1) Up to the First Boom of AI Development

Attempts to replace human's intellectual labor with machines began in earnest with the development and operation of computers that occurred in the United States during the middle of the 20th century. However, attempts to reduce the burden of intellectual work using calculation tools can be traced back to Mesopotamia three to four thousand years before the Common Era. Regarding the invention of the first mechanical calculator called the "Stepped Reckoner" for four-arithmetic operations by Gottfried Wilhelm Leibniz in the 17th century, Yuma Matsuda said, "Many scientists no longer had the need to endure the difficulty of calculation. This was exactly the moment when mankind was liberated from the labor of calculation."[5] Such development of calculators became the trigger behind social reforms caused by the series of information sciences also known as "the

---

2 Suzuki Hisao, and Toya Seiichi, *Soroban no rekishi* [The history of abacus] (Tokyo: Morikita Publishing, 1960), p.1.

3 Matsuda Yuma, *Jinko chino no tetsugaku* [Philosophy for artificial intelligence] (Hiratsuka-shi: Tokai University Press, 2017), p.5.

4 See Ono Keshi, "Gunsan kankeishi to sorewo meguru shiso [The History of the Military-Industrial Relations and Related Theories]," *NIDS Military History Studies Annual*, no.21 (March, 2018), pp.66-70 for relationship between the military and industries in the IT and AI age.

5 Matsuda, *Jinko chino no tetsugaku*, p.6.

intellectual industrial revolution." [6]

The systemization of logical operation by George Boole that appeared around two centuries after the invention of the "Stepped Reckoner" is said to have migrated the intellectual industry revolution into a new stage.[7] Logical operation that carries out logical inference using the four arithmetic operations "became the philosophy behind today's programs," and as a result, people "have been able to give orders to computers."[8] In other words, logical operation provides "a means for combining multiple intellectual work (calculation) following conditions." Consequently, computers were invented that can automatically carry out logical operation by simply providing algorithms (calculation methods [orders = program]). This system handles variables as an abstract concept and can be seen as "moving one step closer to human's abstract thinking." [9]

One of the most famous first computers was Electronic Numerical Integrator and Computer (ENIAC) developed in the United States in 1945. This development project was led primarily by the US Army's Ballistic Research Laboratory and the University of Pennsylvania during World War II.[10] It was implemented jointly between the military and universities, with cooperation from universities across America. The original purpose of ENIAC development was the preparation of firing tables (correlation table for type of ordinance, angle of elevation, launch explosives, wind, temperature, and humidity, etc.) for indirect shooting. The preparation of one artillery firing table required between 2,000 and 4,000 ballistic calculations. This work took 50 people three to six months even when using a desktop mechanical calculator, but with ENIAC it could be completed in one day by five people.[11] In other words, the calculation efficiency was improved between 900 and 1,800 times. However, ENIAC was a huge machine made of 18,800 vacuum tubes and it was 12 meters long, four meters high and weighed 30 tons. It also required a 24-horsepower ventilator for the heat from the vacuum tubes. Vacuum tubes broke down at a rate of about one per day and one hour was required to replace each one. As a result, the utilization rate was only 69%. Coupled with the sheer size and complex structure (around 6,000 switches), this meant ENIAC was rather far from practical.

Attaining AI is based upon the premise of advancements in computers that began with ENIAC. In 1956, an international meeting called the Dartmouth Summer Research Project on Artificial Intelligence was held on the mechanization of intellectual activities. This is where the word Artificial Intelligence (AI) was used for the first time. The development of AI until today is generally categorized into three booms. The time around this conference is considered the First Boom in the 1950s and 1960s. The features of AI around this time can be found in inference and exploration. Syllogism is a simple example of inference, which translates as "If A, then B (minor premise), and if B, then C (major premise), as a result, A is C (conclusion)". In the late 1950s, a computer program was developed in the United States that carried out theorem of geometry with

---

6 Shinagawa Yoshiya, *No to konputa* [Brain and Computer] (Tokyo: Chuko Shinsho, 1972), pp.194-205.

7 Inoue Tomohiro, *Jinko chochino* [Artificial Super Intelligence] (Tokyo: Shuwa System, 2017), pp.60-66.

8 Matsuda, *Jinko chino no tetsugaku*, p.6.

9 Nagao Makoto, *Jinko chino to ningen* [AI and Humans], (Tokyo: Iwanami shinsho, 1992), pp.2-7.

10 Herman H. Goldstine, Ch.2. in *Keisanki no rekishi* [The Computer from Pascal to Von Neumann], translated by Ryota Suekane, et al., (Tokyo: Kyoritsu Shuppan, 1979).

11 Shinagawa, *No to konputa*, pp.17-18.

deductive operation of symbolic logic using syllogism.[12]

Meanwhile, exploration involves finding the solution to a problem from among the options.[13] For example, in the case of the problem of "Move to Z from X via Y," the solution requires finding the road that leads to Y, among the roads extending in all directions from X. Even after arriving in Y, the same process needs to be carried out. If the location relationship of XYZ is not known, the correct answer must be searched for by considering solutions in a round robin format including roads that do not lead from X to Y or from Y to Z. Another example is the problem known as the "Tower of Hanoi." [14] It involves a base with three poles sticking up, and several disks with differing diameters and holes in the middle. Prior to starting the game, all the disks are lined up on one of the poles in descending order of the size of their diameter, and they are moved to the pole on the opposite side in the same shape. When doing so, one disk can be moved one time to either of the three poles, but the disks must always be stacked in descending order of the length of their diameter.

A similar problem is the Knapsack Problem where products of differing volumes and prices are placed inside a knapsack with a fixed volume with the objective to maximize the total price of the products placed in the knapsack. These examples of exploration are finite even when there are vast quantities of instances. Consequently, computers can arrive at a correct answer by using a round-robin approach. In this stage, the processing capacity of computers at the time could not make a dent since high speed processing was not possible under the given rules and conditions for problems where the number of instances increased exponentially.[15]

(2) The Second Boom and Expert Systems

The Second Boom of AI development that began in the 1970s is symbolized by the development of expert systems that attempt to replace the advice and judgement of experts. This involved users entering logical conditions in the form of "if-then" questions into a specific specialized database to narrow down the data and lead to a conclusion. Compared to the First Boom that was logical inference, the artificial intelligence of the Second Boom was deductive inference, which can also be viewed as "knowledge added to logic." It is also referred to as "knowledge engineering." [16]

An expert system holds a vast amount of data on the knowledge, experiences and intuition of experts, and by searching this database, the answer of "If A, then B" will be provided. MYCIN, an expert system developed at Stanford University in the early 1970s, was able to correctly diagnose bacterial infections with a probability of 69%.[17] Although this fell short of the probability of correct diagnosis by specialist physicians (80%), it was higher than the results of non-specialist physicians. The system demonstrated better results than specialist physicians in terms of diagnosing bacterial

---

12 Nagao, *Jinko chino to ningen*, pp.7-10.

13 Matsuo Yutaka, *Jinko chino wa ningen wo koeruka* [Does AI Surpass Humans] (Tokyo: Kadokawa EPUB sensho, 2015), pp.65-71.

14 For the minimal number of steps in the Tower of Hanoi is illustrated via mathematical induction at high school education level (Takahashi Tetsuo and Nikoshi Miyuki, "Kansu shido no ikkan to shiteno koutougakkou suugaku 'suuretsu'no jyugyo puran[Classroom plan for "sequences" in high school mathematics as part of function teaching]" *Kyojyu gaku Tankyu* [Search of Didactic Methods] Hokkaido University, no.22. [January, 2005], pp.97–100).

15 Furukawa Koichi and Fuchi Kazuhiro, "Chishiki kogaku to dai go sedai computer [Knowledge Engineers and 5th Generation Computers]," *Operations Research* vol.28, no. 6 (June, 1983), pp.3–4.

16 Nishigaki Toru, *Big data to jinko chino* [Bog data and AI] (Tokyo: Chuko shinsho, 2016), p.60.

17 Matsuo, *Jinko chino wa ningen wo koeruka*, p.88.

blood infections or meningitis.[18]

The introduction of an expert system makes it possible to reduce labor, in addition to increasing information processing speeds; therefore, the manufacturing industry also looked toward them.[19] However, the motivation was not just about reducing labor; the purpose also involved the decline in highly experienced engineers and succession of technology. Northrop Corporation (currently: Northrop Grumman Corporation), which had faced challenges from declining engineers and declining competency, introduced an expert system called ESP, gaining hints from MYCIN, for streamlining manufacturing processes.[20] At the time, its F-5 and F-18 fighters were made from between 11,000 and 20,000 parts, and vast amounts of time were required for the manufacturing process formulation of each part.[21]

As a result, the company used ESP to answer the question of "what process to use for which material" around 30 times, whereby systemizing the flow of narrowing down the material and processing format, and then determining the selection of the right machine or tool for the job and correct processing sequence. During the parts manufacturing process formulation, even an experienced engineer had to carefully examine the material and processing based on their experience and knowledge, and then select the tool or machine for subsequent work (experienced engineers prefer using something familiar rather than the most optimal tool or machine) as well as consider the processing sequence. This series of process formulation work required two to three people about one hour. Using ESP, however, this work was able to be performed by a single person in around 10 to 15 minutes. Furthermore, even a less experienced engineer was able to master the work procedures with the same degree of proficiency as a highly trained engineer, including "This material is processed in this way using this machine following this procedure." In this manner, as the number of engineers declined, Northrup was able to assign engineers freed up by the introduction of AI (ESP) to work on other more difficult work.

The question and answer posed to ESP of "what process to use for which material" is prepared based on the experiences of a highly trained engineer (generalization of experience and knowledge). When turned into data, the knowledge of an expert accounts for a vast quantity of data. Incorporating this vast data into systems supported technological progress in increasing the capacity of memory media. Consequently, underpinned by the high expectations placed in expert systems by business and industry at the time, some 3,000 systems were developed in the United States and 1,000 each in Japan and Europe.[22] ESP introduced by Northrup was one of these systems.

---

18 Geoff L. Simons, *Jinko chino* [Introducing Artificial Intelligence], translated by Tamura Koichiro and Sato Takeshi, (Tokyo: Kindai Kagaku Sha, 1986), p.210.

19 Shimura Masamichi, *Jinko chino* [Artificial Intelligence], (Tokyo: Shin OHM bunko, 1989), p.56.

20 Edward Feigenbaum, et al. *Expert company* [The Fifth Generation: Artificial Intelligence & Japan's Computer Challenge to the World], translated by Nomoto Haruyo, (Tokyo: TBS-Britannica, 1988), pp.37-55.

21 F-15 is said to be comprised 100,000 components (Chaki Akiyoshi, "Kokuki ijibuhin no hokyu kanri ni tsuite [Supply Management of Maintenance Parts for Aircrafts]," *Boei syutoku kenkyu* [Defense Acquisition Research] vol.3, no. 4 (March, 2010): p.3).

22 Yamaguchi Takahira, "Dai 5-sedai computer kara kangaeru AI project [AI Projects Based on 5th Generation Computers]," *Artificial Intelligence* vol.29, no.2 (March, 2014), pp.116-117.

2. Military-Use AI in the Second and the Third Booms

Full-fledged military-use AI was developed by applying the expert systems of the Second Boom in AI development. These systems left a certain degree of operational track record, but given the limit attached to expert systems, even when supplementing the intellectual work of humans, they did not go as far as replace it. This was followed by the Third Boom of AI that greatly transformed the development concept from around 2010. This boom is still taking place today.

(1) The Second Boom and Military-Use AI

The expert systems of the Second Boom were also developed into military-use systems. In the US Navy's threat assessment and countermeasure planning system, information on the type of target captured by radar, estimated intention of the target, and presentation of responses, etc., were provided to commanders.[23] In addition, RAND Corporation developed Tactical Air Target Recommender (TATR) jointly with the US Air Force as a support system for plan formulation when attacking an enemy air base. TATR is also one type of expert system, and the series of attack plan formulation from selection of target and selection of weapons to use was carried out using the following procedures.[24]

Initially, TATR assessed multiple enemy air bases. In this process, it first determined the vulnerability and operational capacity of each enemy air base, and later, taking into account the operational situation of the enemy air bases, other relevant matters, and the tactical objective of the US Air Force's air operations, it assigned a priority order for attacks of the enemy air bases. After assigning this priority, it calculated the attack effects on each enemy air base (damages to enemy air bases = extent of reduced operational capacity). In this manner, TATR displayed a list of the enemy air bases in order of attack priority, the attack method believed to be the best, along with the types and numbers of friendly aircraft to send for the attack, and then prepared an attack plan based on the results of these estimates.

In order to perform such a calculation, TATR requires a database to refer to as needed. This database is composed of the attribution of enemy air bases (location, elevation, area, weather info), operational capacity of enemy bases (attack capability, air-defense capability, supply provision capability, damage restoration capability), and detailed information concerning friendly attack aircraft, weapons and ordinance, etc. This database is updated following progress in fighting, and (since the operational capacity of friendly and enemy forces changes with attacks) information collected from the fighting is entered manually. If the damage situation of the enemy is unknown even when implementing the attack plan presented by TATR, damages of the enemy side expected in the attack plan are reflected in the database.

TATR is an expert system. The experience and knowledge of experts is generalized in the system. This is embedded into a program that selects the optimal combination of friendly aircraft type and numbers along with ordinance to use and number after determining the priority attack ranking and target of enemy air bases (aircraft, anti-aircraft weaponry, runways, and various facilities, etc.). It also determines the attack effects (whether the enemy air base will suffer extensive, major or minor damages) during an actual attack using these combinations (aircraft

---

[23] Donald Michie, and Rory Johnston, *Souzou suru computer* [The creative computer: Machine intelligence and human knowledge], translated by Kimura Shigeru, (Tokyo: TBS-Britannica, 1985), pp.51-52.

[24] Description of TATR is based on Monti Callero, et. al., *TATR: A Prototype Expert System for Tactical Air Targeting* (Santa Monica: Rand Corporation, 1984).

type, number and ordinance, etc.) along with the variable of the enemy's recovery speed from damages, based on the experience of experts.

The ultimate goal of TATR is to formulate an attack plan for enemy air bases, but this can also be used in war games (military simulations). For example, the knowledge of experienced operators is reflected in TATR, so operators with little experience are expected to quickly acquire the knowledge of unit operations of an experienced operator through training using TATR. In addition, as preparation for planned operations, it can also be used to identify preparatory items. Furthermore, the system can also be utilized to verify unit composition and consider the information that should be collected before the start of operations.

Attempts were also made to apply expert systems to anti-submarine warfare (ASW), with a certain degree of results achieved (CLASSIFY system).[25] In ASW, detecting submarines using sonar is key, but higher performance sonar can also pick up many other sources of sound outside of enemy submarines, so it is extremely difficult work to sort out the target's sound from other sounds. On top of this, this work relies heavily on the rule of thumb of sonar operators, which made it almost impossible to use mathematical processing. The rule of thumb of operators is formed by experience operating sonar and expert knowledge concerning the echoing of soundwaves.

As a result, CLASSIFY is used to obtain information on the intensity and characteristics of active sonar echoes, doppler changes, angular velocity, radar reflectivity, and passive sonar information. Experts in ASW combine this, considering the quality of this information, to detect the target submarine. The problem here is that each expert considers quality based on his or her experience (determination of coefficient for variables), but when reflecting this in a system, only the experience of certain people can be reflected. Put another way, the decision of which information to emphasize during which situation varies by expert, but when building a system, only one of these can be reflected. This is an unavoidable limitation of not only CLASSIFY but any expert system.

The second problem is that targets detected with consideration of quality vary greatly. For example, even when detecting the same submarine, radar reflectivity cannot be used as a determining element if it is underwater, but the same is not true when the submarine is surfaced. In other words, the coefficient of the system's configuration and variables should be changed following the target to be detected, but this system falls into the cycle of having the purpose to detect a target. Having said that, however, the development of CLASSIFY carries great meaning in systemization in the ASW field method (heuristic) for solving a problem by narrowing down solutions based on repetition of logical conditions in the format of "If – then" by system and operator, instead of logical problem solving (algorithm).[26] As a result, this enabled, albeit partially, the systemization of submarine detection that had relied on experts' rule of thumb until then.

---

[25] For CLASSIFY, refer Ingemar J. Cox and Lewis J. Lloyd, "Artificial-Intelligence Systems in Antisubmarine Warfare: Results of a Pilot Study with Expert Systems," *Saclantcen Memorandum* SM-176 (Dec., 1984).

[26] On the other hand, in the initial development of TATR, logicality was desired while heuristic methods were attempted to be eliminated (Monti Callero, et. al., "TATR: An Expert Aid for Tactical Air Targeting" *A RAND Note*, N-1796-ARPA (January, 1982), pp.29-30).

(2) The Third Boom and Deep Learning

However, the Second Boom eventually waned in the middle of the 1990s. Once the amount of knowledge (conditions) entered into a system becomes large, it makes it possible to respond to complex events. However, when this input information is vast, it becomes a hypothesis or guess with probability such as "Based on experience, if A, first it should be B" rather than the firm outcome of "If A, 100% B." Narrowing down data using this logical condition inevitably causes calculation errors to become larger. Even for logical conditions that are 99% correct, such as the case of ESP, the accuracy even for 30 times repetation is 74% (0.99 to the 30th power) and in the case of logical conditions with 95% accuracy, the accuracy after 30 times is 21% (0.95 to the 30th power). This makes it rather difficult to say these systems can withstand practical use. Furthermore, there are cases where decisions are different among experts even when using the same data, and the conclusion reached by AI inevitably faces such limitations.

More than anything else, the tacit knowledge (intuition and rule of thumb) of people, regardless if they are experts or not, was basically impossible to systemize. A human doctor, based on their tacit knowledge, can arrive at a diagnosis even when only obtaining vague information (e.g., "stomach pain"). AI, however, will be stuck without identifying in detail "the part of the stomach, which organ is experiencing what type of symptoms or condition." [27] AI cannot reach a diagnosis with abstract information such as "the top right of my stomach hurts like someone is pressing it down."

To overcome this, a collection of anticipated questions and answers between doctors and patients must be prepared by a person beforehand and entered into the AI system. In this process, question and answers are repeated with patients to gradually materialize abstract information, but a great deal of labor is required to create these questions and answers. Even so, if the patient's answer differs even a little from the expected response, AI will not be able to go any further. In addition, the questions and answers of doctors and patients are created based on "conventional wisdom" shared by people, and in case of developing a system, this conventional wisdom must be included, but it is vast and unclear, making it extremely difficult to systemize explicitly.[28]

Later, the Third Boom began that continues on from the 2010s to today. Unlike the Second Boom where the correct answer was narrowed using logical conditions (deductive inference), the Third Boom is characterized by identifying the correct answer using statistical processing (inductive inference). In order to increase statistical accuracy, the larger the number of sample data the better (big data), and each of these sample data must be broken down into uncorrelated feature values mutually in comparatively small clusters (components and factors) (deep learning). Furthermore, after breaking down into these feature values, the coefficient of each feature value must be revised correlating with the original sample data, for the abstraction and generalization of sample data. This series of tasks is left to AI (machine learning) to increase the accuracy of decisions. In this process, as a result of vast amounts of data used, AI is nearly able to acquire tacit knowledge, expanding the scope of application (Table 1).

The problem here can be found in the fact that logical explanation of how a decision was reached cannot be obtained even with more accurate AI decisions, including the tacit knowledge

---

27 Matsuo, *Jinko chino wa ningen wo koeruka*, pp.89-90.

28 Nagao, *Jinko chino to ningen*, pp.180-182.

mastered in this manner. For example, AI such that can beat a prominent professional shogi (chess-like Japanese board game) player learned records of more than 60,000 games played since about four hundred years ago and broke them down into more than 10,000 feature values.[29] In addition, it is said that recent shogi software is processing and evaluating the positional information of pieces for upwards of 100 million possibilities.[30] Even if the coefficient attached to these variables on the order of 10,000 or 100 million can be demonstrated inductively as a result of statistical processing, it is impossible to explain deductively why a certain value was reached. That is, AI simply presents the highly accurate results. More than likely, this could be the actual state of the tacit knowledge possessed by people.

Habu Yoshiharu, a professional shogi player and holder of seven lifetime titles, refers to this situation as a "black box." [31] In other words, AI's decision making has become invisible to people, and Habu states his concerns about becoming excessively reliant on this, and therein lies the awareness that the "decision making process essentially differs between AI and people." However, learning amounts are simply incomparable between people and AI, but in terms of "indicating the results inductively," they are likely the same. Incidentally, the shogi software called Ponanza, which beat Sato Amahiko, former Meijin (champion) titleholder, during a match between professional shogi player and shogi software in 2013, developed by Yamamoto Issei, a professor at Aichi University, has data containing 800 billion moves.[32] In addition to records of matches, this data is the result of learning from games played between shogi software competing against each other (a match involving professional shogi players requires several hours, but a match between AI software is finished in only several seconds each time).[33] Certainly, it would likely be impossible

Table 1: Summary of Each AI Boom

		Application scope	Logic
First Boom (1950s to 60s)	Logic deductive inference	△ (Puzzles and games, etc.)	◎
Second Boom (1970s to 80s)	Knowledge deductive inference	○ (Expert systems, etc.)	○
Third Boom (2010s to present)	Statistical (learning) inductive inference	◎ (Pattern recognition & machine translation, etc.)	△

Source: Partially revised the table on p.172 in Nishigaki Toru, *Big data to jinko chino* [Bog data and AI] (Tokyo: Chuko shinsho, 2016).

29 Hoki Kunihito and Watanabe Akira, *Bonanza VS shoubu no* [Bonanza vs. competitive brain – Will the best shogi software eclipse humans?], (Tokyo: Kadokawa Shoten, 2007), pp.27-28. The oldest existing record of a game of shogi is as old as 1607 (Matsumoto Hirofumi, *Kishi to AI ha dou tatakatte kitaka* [How Have Shogi Players and AI been Competing?], [Tokyo: Yosensha, 2017], p.21).

30 Yamamoto Issei, *Jinko chino wa donoyouni shite 'meijin' wo koetanoka* [How did AI eclipse famous people?—Fundamentals of machine learning, deep learning and reinforcement learning as taught by the developer of the world's best shogi AI software Ponanza], (Tokyo: Diamond Inc., 2017), p.140.

31 Habu Yoshiharu and NHK Special News Crew, *Jinko chino no kakushin* [The Core of Artificial Intelligence], (Tokyo: NHK Shuppan shinsho, 2017), p.36.

32 *Newton bessatsu* [Special edition of Newton], (May 2018), p.100.

33 Each professional player has 9 hours per game in a professional shogi competition (sum of 18 hours), which takes place over two days. To date, the longest thinking time spent on one move was 5 hours and 24 minutes (Japan Shogi Association website: https://www.shogi.or.jp/ column/2017/01/post_68.html).

for a human shogi player to learn and analyze such a large amount of data even in one lifetime, but there is believed to be no major difference between shogi player and AI in the thought process leading to tacit knowledge thereafter.

(3) Increasing AI's Thinking and Decision-Making Capability

As discussed above, humans have already been "liberated from intellectual work" by the invention of the calculator and computer. The First and Second Booms of AI development (especially the latter) not only liberated humans from simple intellectual work, but also focused on the perspective of "supplementing thinking and decision-making." These booms ended halfway, but in the Third Boom currently underway, development has gone beyond supplementing to "replacing thinking and decision-making (intellectual labor)." This means that intellectual labor, which was the bastion of humans, is able to be replaced by AI. Discussions are now underway from all sides about this.

The reason why the replacement of thinking and decision-making is possible first thanks to significant improvements in processing speed (computer performance). In the IT field, instead of conventional progressive technological advances such as these improvements, exponential technological innovations are progressing as indicated by Moore's law.[34] This means that vast amounts of data physically impossible for humans can now be processed by a machine instantaneously. In other words, the amount of knowledge used as a basis for decision-making by a system is already greatly superior to that of humans. Vast amounts of data must be handled to carry out work commensurate with a system that can be called artificial intelligence, but until recently the processing speeds of computers had not been enough for it.[35]

In recent years, improvements in computer performance have made deep learning a reality, and made it possible to utilize vast amounts of data for this purpose. In June 2012, Google successfully developed a program using deep learning methods that can recognize a cat without the help of humans (Table 2). This system operated 1,000 computers for three days to read the data of 10 million photographs to learn which picture is a cat and which is not. However, it is said that using a computer in the 1990s to perform the same work would take more than 6,000 years.[36]

In addition to this, IBM's supercomputer called Watson, which beat a quiz champion on an American quiz show in February 2011, analyzed data equivalent to 200 million pages at the time, and it did not require three seconds to present the results of its analysis.[37] The processing speed of Watson sped up 24 times in the four years since.[38] IBM's Deep Blue, which beat a world champion

---

34 Moore's Law is stated by Gordon Moore, one of the co-founders of Intel Inc., that the degree of integration on IC doubles at every 18 months to 2 years ("Moore's Law at 40, Happy birthday, The tale of a frivolous rule of thumb," *The Economist*, Mar. 23rd 2005, http://www.economist.com/node/3798505). However, the same law also applies to the processing speed of IC, capacity of memory medium, and circuit capacity for wireless data communication, optical communication, and the internet, pointing to the exponential evolution of IT technology as a (P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-first Century* [New York: The Penguin Press, 2009], p.99).

35 Nishigaki, *Bigu deta to jinko chino*, pp.76-89.

36 Ono Kiyoshi, "Deep learning nyumon Introduction to Deep Learning]," *Intec Technical Journal*, vol.17 (September, 2016), p.30.

37 Kozaki Yoji, *Jinko chino kaitai shinsho* [AI Guidebook: Understanding the system and utility of AI from scratch] (Tokyo: Science eye shinsho, 2017), p.67.

38 Hachiyama Koji. "Beikoku ni okeru jinko chino ni kansuru torikumi no genjo [Current Status of AI Initiatives in the USA]" *Information-Technology Promotion Agency NY Report*, (February, 2015), p.3.

of chess in 1997, is said to be able to calculate 300 million moves in one second.39[39] The shogi software called Bonanza developed by Hoki Kunihiko, associate professor at the University of Electro-Communications, is able to read four million moves in one second.[40] These results have basically benefited from increasing hardware performance.

The factors of number two are deeply related to number one, but this is because non-standardized data can now be handled. Conventional data entry into a computer involved quantifying non-standardized data (analog) into digital form with the help of people. This can now be analyzed by reading recognition of language along with images, videos and voices as data. Citing an example, in 2015, IBM acquired a company that owns medical information and digital charts for 50 million people followed by a company that manages medical imaging data of 200 million sheets, in order to expand its healthcare business.[41] Incidentally, some 200,000 reference works on cancer treatment are registered in a specialized database every year and these records contain many images. The advancement in AI in recent years has made it possible to analyze non-standardized data such as images and sentences.

The factor of the third is cited as AI's thinking and decision-making is not affected by fatigue like humans. As a concrete example, according to Shai Danziger, et. al., there is research about the relationship between judge rulings and fatigue in Israel.[42] According to this, as a general theory, rulings handed down at times close to the end of work tend to be stricter on the defendant than those handed down during early hours of the day. In addition, in case of rulings after a recess, rulings

Table 2: Improving AI Capability

Year	Developer	Details
1980	M. Reeve, D. Levy	Moor beats world champion in Othello
1994	University of Alberta (Canada)	Chinook beats world champion in Checkers
1997	IBM	Deep Blue beats world champion in chess
2010	Univ. of Electro-Communication, Univ. of Tokyo, et al.	Akara 2010 beats female titleholder in Shogi
2011	IBM	Watson beats quiz champion on American quiz show
2012	Google	AI automatically recognizes cat
2013	Yamamoto Issei	Ponanza records first overwhelming victory of professional shogi player
2016	Google	AlphaGo beats world champion in Go
2016	National Institute of Informatics et al.	Torobo-kun posts the highest score on a university entrance exam (written portion)

Note: The numbers of cases for each game were; 10 to the 30th power for Checkers, 10 to the 60th power for Othello, 10 to the 120th power for Chess, 10 to the 220nd power for Shogi, and 10 to the 360th power for Go (Japan Science and Technology Agency, " Kenkyu kaihatsu no fukan houkokusho [2015] [Report on research and development – Information science technology field [2015]]" [2015], pp.357-359).

39 Matsubara Jin, *AI ni kokoro wa yadoru noka* [Does a heart reside in AI?], (Tokyo: Shueisha International Inc., 2018), p.64.

40 *Newton bessatsu*, p.32.

41 Japan Health Sciences Foundation, "Iryo bunya ni okeru big deta narabini ICT • AI no rikatsuyo no saishindoko [Big data in the medical field and latest trend in ICT & AI utilization], (March, 2017), p.125.

42 Shai Danziger, et al., "Extraneous factors in judicial decisions," *Proceeding of the National Academy of Sciences (PNAS)*, vol.108, no.17 (April, 2011), pp.6889-6892.

that were stricter prior to the recess were observed to be eased after the recess. This indicates the possibility that even judges who are trained in correct and impartial rulings cannot avoid the impact of fatigue on their thinking and decision-making.

3. AI Advancements and Replacement of Intellectual Labor in the Military

In the previous section, discussions about practical examples of AI as a support method for decision making focused mainly on the application of expert systems in the Second Boom. However, the AI in the Third Boom that is currently underway transcends "support of decision making" where human's "decision-making itself (intellectual labor) can be replaced. Below, the author will attempt to examine the replacement of intellectual labor using AI by the military.

(1) Replaceability of the Military's Functions using AI

Traditionally, labor replacement by computer was limited to routine work for which rules were clear. But, after the First and Second Booms, in the Third Boom of recent years, AI has been able to replace non-routine work. The abstraction and generalization of this non-routine work is made possible with big data. Of course, the progress of hardware that enables instantaneous deep learning of big data and breakdown to uncorrelated feature values (abstraction and generalization) has been vital to this. These are also the core technology underpinning the Third Boom of AI. Carl Benedikt Frey and Michael A. Osbone of Oxford University presented the famous report called *The Future of Employment: How susceptible are jobs to computerisation?* in 2013.[43] This report examined the replaceability of 702 occupations based on US Labor Department classifications using AI (including robots) from the middle of the 2010s to the middle of the 2020s, but military occupations were not subject to consideration. As a result, the author compiled the replaceability using AI of occupations similar to each military function after largely categorizing these functions into the three areas of headquarter (staff organizations), combat units, and support units (Table 3). At the same time, the replaceability of each occupation by AI produced by Frey and Osbone is shown side by side.

This merely allocates the predicted value of replaceability by AI of the occupations considered to be close to these military functions. However, from this, certain tendencies can be interpreted. For example, in the near future, there is a low possibility that command and management duties will be replaced by AI, but there is a high possibility for replaceability of duties supporting these. Moreover, even for non-routine duties, the judgement of humans is indispensable for the time being regarding management and supervision. For the most general management duties, replacement by AI will come into view, even for supervisors.

In future military units, the commander will make decisions based on their own experience and intuition (tacit knowledge) while referencing documents prepared by AI. Even if physical work in the field is replaced by AI (robots), the management and supervision will be carried out by humans. Military is active on battlefields and at the scenes of disasters, which requires the frequent occurrence of "ad hoc response to inexperienced situations." This type of judgement is difficult for AI, but this can be easily forecast from the characteristic of AI in which feature values is analyzed

[43] Carl Benedikt Frey and Michael A. Osbone, "The Future of Employment: How susceptible are jobs to computerisation?" *Oxford Martin School Working Paper, University of Oxford* (September, 2013).

using statistical processing of past sample data.

However, according to Frey and Osbone, it remains difficult to use AI to replace occupations that require "1. Non-standardized perception and manipulation," "2. Creative intelligence," and "3. Ability to build cooperative relationships with others by adapting to social human relationships."[44] Among these, 1) presents technological difficulties of hardware and software, while 2) cannot avoid the reliance of AI decisions on statistical processing of past sample data. In addition, 3) is the ability of personal relations in a human society known as "social intelligence," which is the most difficult to replace using AI (and the least suitable). Conversely speaking, the hurdles of 1) may be reduced with technological advancements, but for 2) ad hoc response to inexperienced situations poses a major challenge for AI. In addition, examples were introduced of AI creating works of art, but these are nothing more than the "imitations" of past artists' work (statistically close), and not "artistic creations." 3) should be viewed as AI occupies a different existence as humans and it cannot be resolved since AI cannot be a member of human society.

Military functions for which computerization is believed to be difficult as indicated in Table 3 truly require all three. Specialized analysis provided by AI will likely become even more accurate in the future, but this analysis assumes that the preconditions will not change from the current situation. For example, AI that can beat the best shogi players learns tens of thousands of matches over the past 400 years and learns more than matches as the result of battles between AI software. The assumptions of these are all the same (9 x 9 board, 40 pieces in total, move of each piece, etc.). However, in the activities of the military (battlefield or scene of disaster, etc.), the assumptions are not uniform, and they change on occasion. In the case of shogi, this would mean the board suddenly expands to 12 x 15 during a match, or the number of pieces increases to 60, and the moves change suddenly (soldiers and spears can move backwards which is not allowed in the current rule, etc.), normalizing "ad hoc response to inexperienced conditions." It is believed that "the ability to respond to sudden, unpredictable situations inherent in humans" will not be replaced by AI for the next 20 years.[45]

(2) Entry and Analysis of Non-Standardized Data and Staff Functions

The important thing when considering labor replacement using AI is whether input and output is standardized or not. The first computers had to have inputs standardized (entry using punch card), and outputs was inevitably standardized. This means that even in today's everyday life most computers have had their inputs and outputs standardized. On the other hand, computers have gradually been able to cope with non-standardized input (distinguishing handwritten numbers, etc.).[46] For example, using the example of Table 2, the input of checkers, chess, shogi and go are

---

44 Frey and Osbone, "The Future of Employment,"pp.25-30.

45 Eto Minoru, "Economic classroom AI and work style: The rise of various freelance work." *The Nikkei*, (February 27, 2018).

46 For example, the world's first handwriting recognizing automatic postal code reading and sorting machine was developed and brought to application by Toshiba in 1967 (Toshiba website: http://toshiba-mirai-kagakukan.jp/learn/history/ichigoki/1967postmatter/index_j.htm).

Table 3: Replaceability of Military Functions by AI (including robots)

Military functions		Resembling occupation	Probability of substitution by AI
HQ (staff)	General Affairs	First-Line Supervisors of Office & Administrative Support Workers	1.4%
		Administrative Services Managers	73 %
	Intelligence	Social Scientists & Related Workers	4 %
		Market Research Analyst & Marketing Specialists	61 %
	Operations	Training & Development Specialists	1.4%
		Business Operations Specialists	23 %
	Logistics	Medical & Health Services Managers	0.73%
		Logisticians	1.2%
	Planning	Urban & Regional Planners	13 %
	Communications	Computer &Information Systems Managers	3.5%
		Information Security Analysts, Web Developers & Computer Network Architects	21%
	Legal	Lawyers	3.5%
		Paralegals & Legal Assistants	94 %
	Adjutant	Executive Secretaries & Executive Administrative Assistants	86 %
Combat Unit		First-Line Supervisors of Fire Fighting & Prevention Workers	0.36%
		First-Line Supervisors of Police & Detectives	0.44%
		Police & Sheriff's Patrol Officers	9.8%
		Firefighters	17 %
		Airline Pilots, Copilots & Flight Engineers	18 %
		Captains, Mates, and Pilots of Water Vessels	27 %
		Police, Fire & Ambulance Dispatchers	49 %
		Transit and Railroad Police	57 %
		Sailors & Marine Oilers	83 %
		Security Guards	84 %
Support Unit		First-Line Supervisors of Mechanics, Installers & Repairers	0.3%
		First-Line Supervisors of Transportation & Material-Moving	2.9%
		Chefs and Head Cooks	10 %
		Air Traffic Controllers	11 %
		Commercial Pilots	55 %
		Transportation, Storage & Distribution Managers	59 %
		Aircraft Mechanics & Service Technicians	71 %
		Heavy and Tractor-Trailer Truck Drivers	79 %
		Cooks, Institution and Cafeteria	83 %
		Laborers & Freight, Stock & Material Movers, Hand	85 %

Source: Made by the author based on Carl Benedikt Frey and Michael A. Osbone, "The Future of Employment: How susceptible are jobs to computerisation?" *Oxford Martin School Working Paper, University of Oxford* (September, 2013), pp.61-77.
Note: Shaded cells indicate replaceability of 50% or higher.

standardized and output is also standardized.[47] However, the automatic recognition of a cat (2012) had non-standardized input (input images from the Internet without changing), but Torobo-kun (2016) has evolved to the point where it can respond to both non-standardized input and output of a university entrance exam.[48]

However, the command functions and chain of command indicated as difficult to be replaced by AI in Table 3 can be viewed as duties that require non-standardized input and output. Yet, current computers are not fully capable of non-standardized output. In other words, there is sufficient potential for duties that involve the combination of "non-standardized input and standardized output" to be replaceable by AI for the time being. In the military, staff duties are one of the occupations that this combination of "non-standardized input and standardized output" applies to.

Lieutenant-General William G. Pagonis, who commanded the 22nd Support Command during the Gulf War (1991), states that an index card (three inch x five inch) was an effective means of communicating complex information and orders based on his experience in the Gulf War.[49] In the IT world of today such information exchanges can likely be done by email and even Pagonis himself says he used the index card and email together during the battle.[50] This is an archetype example of non-standardized information. The handwritten entry on a card (although these cards were also typed apparently), and even email, has a basic format and is non-standardized form of information. The main duty of staff organizations is to organize and categorize this information and then convey and coordinate it to the right departments.

A similar situation occurred during the rescue work following the Great East Japan Earthquake of 2011. At Ishinomaki Red Cross Hospital, which is a disaster designated hospital for the Ishinomaki medical district in Miyagi Prefecture, physician Ishii Tadashi, who was the frontline commander of medical assistance as the "disaster medical coordinator" immediately after the earthquake, faced difficulties in information shortages, organization and conveyance.[51] Ishinomaki City had 300 evacuation shelters, but immediately after the disaster there was no information whatsoever on the hospitalized and injured, as well as the presence of food and water and condition of sanitation and heating. As time passed, however, information soon overflowed and at the same time requests began to emerge that exceeded this information. Most of this information was conveyed verbally (in person or over the telephone) and it was managed by handwritten notes on paper. Later, the Japanese subsidiary of Google systematized this information management as part of its support for disaster relief.[52] The nature of this information was non-standardized, but data organization had to be performed by the system and input, breakdown and analysis had to

---

47 The go software that can even defeat professional players uses Monto Carlo tree search in its algorithm instead of evaluation function that is used in chess and shogi software (Nikkei Big Data ed., *Google ni manabu deep learning* [Learn Deep Learning from Google], (Tokyo: Nikkei Business Publications, 2017), pp.68–71. As the program chooses moves randomly with high probability of winning, even though there are more number of cases in go than shogi, the program itself is considered rather straightforward.

48 Iwane Hidenao and Anai Hirokazu, "Suuri shori niyoru syushi mondai eno chosen [Taking on examination questions via formula manipulation]" *FUJITSU* vol.66, no.4 (July, 2015), pp.19–25.

49 William G. Pagonis and Jeffrey L. Cruikshank, *Moving Mountains: Leadership and logistics from the Gulf War* (Boston: Harvard Business School Press, 1992), pp.189-191.

50 Ibid, p.189, p.226.

51 Ishii Tadashi, *Higashi nihon daishinsai, ishinomaki saigaiiryo no zenkiroku* [The Great East Japan Earthquake Full Report on Ishimaki Disaster Medical Treatment], (Tokyo: Kodansha bluebacks, 2012), pp.66-70.

52 Ibid., pp.89-93.

rely on people.

Certainly, looking at Table 3, the replacement of labor in the military using AI is believed to be not suitable for command units (staff organizations). However, from the perspective of "input of non-standardized data and breakdown and analysis," an aspect different from this can be observed. For the military's staff organizations, the transport and organization of overflowing information in the form of non-standardized data during a contingency occupies a large weighting of operations. During the Great East Japan Earthquake, the command of the North Eastern Army of the Japan Ground Self-Defense Force (GSDF) that functioned as the HQ for the Joint Task Force (JTF-TH) saw a sharp increase in operations for formulating rescue plans, organization, analysis, search, and conveyance of various information, and coordination with relevant departments, while the organization's manpower was lacking absolutely. Consequently, additional staff were dispatched from various units and were placed in charge of these operations. In this manner, AI, which copes with the input and analysis of non-standardized data, was expected to greatly reduce the burden of the command unit and staff. This applies not only to large-scale disasters, but also to other contingencies with various complex information brought from relevant departments without close interactions during normal times, such as the protection and evacuation of Japanese nationals abroad and protecting the Japanese people from armed attacks.

In addition, Ishii introduced the following during a review committee meeting held after the disaster. The first requirement after a disaster is information collection, and there was a common understanding that the most effective approach for it is that the rescue providers (= rescue information receiver) instruct "the types of information necessary for rescue and information should be collected following the instruction" (this is likely the same today).[53] However, a person in charge at Google who worked on the development of the information organization system for evacuation shelters of the Ishinomaki Red Cross Hospital during the Great East Japan Earthquake said at the review committee meeting that "It doesn't matter what information, please gather every piece of information available. You don't need to worry about whether information is important or not. It is our job as experts to "prepare" the collected information. My message is to collect all forms of information possible and leave the rest to us."[54]

This statement directly and easily articulates the processing of information (non-standardized and standardized) by AI within the staff organization. The phrase "all forms of information" mostly refers to non-standardized data, and "'prepare' collected information (breakdown and analysis)" is made by AI ('experts'). In addition, large amounts of data increase the decision-making capability of AI, and information that may not be needed or information that is questioned as important is automatically judged according to a high degree of accuracy.

(3) The Military's Combat and Non-Combat Units and Advancements in AI

A general trend observed from Table 3 suggests that the replacement of labor by AI (including robots) may follow the trend of "support units > combat units > command units (staff organizations)." In addition, even for combat units and support units, duties related to command and management are believed to have a low possibility of replacement by AI. As discussed in the previous sections,

53 Ibid., pp.94-95.

54 Ibid., p.95.

improvements in processing capability of non-standardized data indicate that replacement by AI is not necessarily a low possibility even for command (staff organization) duties in the future. However, in the military, the ratio of support units and command units (staff organizations) is increasing. What type of impact will this tendency and the potential of replacement of intellectual labor by AI have on the organization and structure of the military?

Martin van Creveld argues that the ratio of combat units and supply units in the military cannot easily be determined.[55] However, John J. McGreath quantitatively indicates that the ratio between combat and non-combat units (tooth-to-tail ratio: T3R) is declining based on trends in the structure of US Army units since World War I. The figure presents a graph of the values calculated by McGreath. Here, the T3R is presented as a ratio calculated by dividing the number of personnel in combat units by that of non-combat units (the sum of command units and support units).[56] Based on the figure, the main factors for the decline in the T3R are the declining ratio of combat units and the increasing ratio of support units. Furthermore, the ratio of command personnel had continued to increase since World War I, but since the end of the Cold War (1991: Gulf War; 2005: Iraq War) it has declined. However, the value for the Iraq War of 2005 includes all private sector contractors included in support units.[57] Given this, private sector contractors are believed to be uniformly categorized in support units despite the fact they are responsible for certain command and management functions (supervision, planning and coordination).

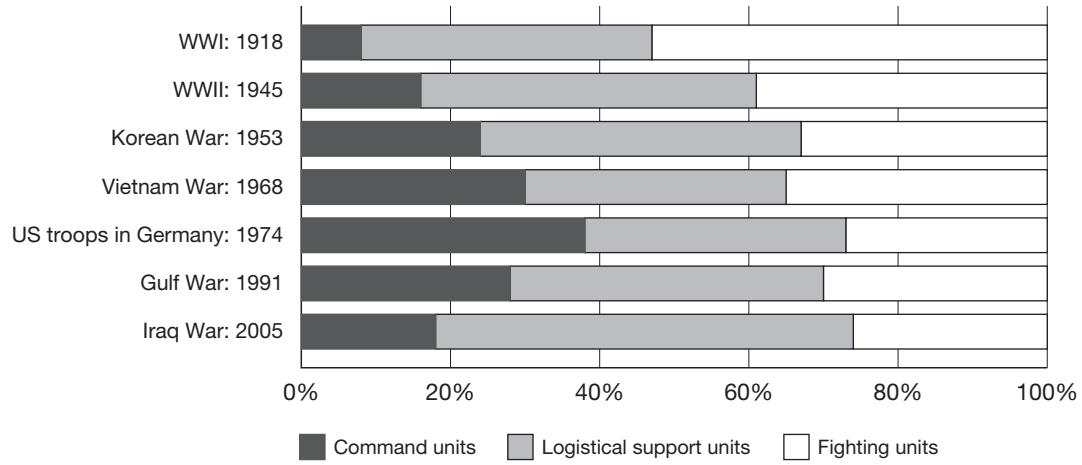


Figure - Ratio of Personnel Belonging to the Command, Logistical Support and Combat Units of US Infantry Divisions (1918–2005)

Note: The value for the Iraq War includes private contractors for logistics support units.
Source: Made by the author based on John J. McGrath, "The Other End of the Spear: The Tooth-to-Tail Ratio (T3R) in Modern Military Operations" *The Long War Series Occasional Paper* 23 (Fort Leavenworth, KS: Combat Studies Institute Press, 2007), p.103.

---

55 Martin van Creveld, *Hokyusen* [Supplying War: Logistics from Wallenstein to Patton], translated by Sato Sasaburo, (Tokyo: Chuko bunko, 2006), pp.384-393

56 John J. McGrath, "The Other End of the Spear: The Tooth-to-Tail Ratio (T3R) in Modern Military Operations" *The Long War Series Occasional Paper* 23 (Fort Leavenworth, KS: Combat Studies Institute Press, 2007), p.2.

57 Ibid, pp.52-53.

AI today (Third Boom) has the characteristic of significantly increasing recognition accuracy of non-standardized data. As has already been discussed, this is believed to be linked to the greatly increasing possibility for the replacement of command unit (staff organizations) functions in the military. As indicated in the figure, however, at the time of the Iraq War in 2005, the personnel of the command and management units of the entire military was less than 20% (18%), which was hardly changed from World War II (16%).

Given this, the following can be pointed out as a long-term trend. Support units have seen an uptick in the percentage, but replacement of labor by AI is possible to a certain degree as seen in Table 3. On the other hand, there is believed to be a possibility for replacement by AI for combat units, too. As a result, the downtrend in the T3R is expected to either weaken or reverse into an uptrend. Put another way, the structure of the military, whereby non-combat units have bloated, will perhaps swing back in the future based on the introduction of AI (the weighting of combat units will get larger). There are many discussions about the reduced manpower and elimination of manpower in combat units from the introduction of robots.[58] However, the replacement of intellectual labor brought about by the introduction of AI (robots) indicates that non-combat units, especially support units are no exception.

Closing – Co-existence of AI and Humans (Military Personnel)

AI development has close to 70 years of history. AI has been commercialized to a certain degree and applied to military-use from around 40 to 50 years ago. The functions of AI at this stage were limited to "supplementing the intellectual labor" of humans, but in the Third Boom of AI development that began around 10 years ago, the "replacement of intellectual labor" of humans until then began to enter the field of view. As indicated in the outcomes of chess, shogi and go matches, AI has already achieved a level that surpasses humans in intellectual games. In view of this, it is believed that AI will be able to "replace the intellectual labor" of humans in the military in the not too distant future.

How will AI and humans (military personnel) co-exist in the future military where most intellectual labor has been replaced by AI (robots)? At the present time, it is no easy task to find the answer to this question, but at the very least the military side, too, likely cannot avoid some form of change in its structureand organization with the introduction of AI. Habu Yoshiharu quoted the remarks of Mogi Kenichiro, a Japanese brain scientist, saying "Modern society is constructed based on the assumption that human IQ is at most around 100." He continues, "If the IQ of artificial intelligence reached 4,000, [omitted], the approach to society will probably change completely at that time." [59] "The possibility that approaches will change completely" also applies to the military, which forms part of human society. These discussions are materialistic, but if the progress of human society could be quantified, it can be said that the speed of IT and AI progress

[58] A representative work in this field includes P. W. Singer, *Wired for War*. For the mechanical soldiers conceived by Leonard Da Vinci, refer to Taddei, Mario, *Da Vinci ga hatsumei shita robot* [Robot Di Leonardo Da Vinci], translated by Matsui Takako, (Tokyo: Futami Shobo, 2009).

[59] Habu and NHK Special News Crew, *Jinko chino no kakushin*, p.36.

under Moore's Law greatly exceeds that.[60]

Although not a dramatic change such as replacement of intellectual labor by AI, the capital intensification of the military brought about by the modernization of equipment as indicated in the figure caused the T3R to gradually decline, while the military's structure and organization has become the dependent variable of technological progress.[61] At the same time, Table 3 can be said to predict to some degree the military's structure and organization when AI is capable of replacing intellectual labor. However, humans' psychological resistance to reliance on AI cannot be refuted for the core components of intellectual labor such as decision making. People have pointed out since the time of the Second Boom that this is a major obstacle to the introduction of AI in the military.[62]

Although its development is progressing at the fastest pace, it appears that AI will not be able to gain the same capacity as humans in terms of "ad hoc response to inexperienced situations" anytime in the near future. As is the case with chess, shogi and go, however, in some localized situations, at the current point in time AI is able to present a faster and more preferable response than humans. Even in such cases, the synthesis of the local, most suitable solution produced by AI is not necessarily the most suitable solution for society as a whole. As a result, the problem of "synthesis error" cannot be avoided.[63] Incidentally, the horizon line effect is cited as a further issue of AI (e.g., when a disadvantage occurs, prioritizing actions that do not allow this disadvantage to emerge).[64] This is not AI-like behavior, which pursues the optimal solution through logic and reason, by not postponing the problem directly and falling into the danger of thinking that the results are the greatest strength, and it also shows the bad habits of humans.

However, Tobe Ryoichi compared the military leaders of the Meiji (1967 – 1911) and Showa (1926 – 1945) periods and stated that compared to the latter with specialized military jobs, the former had elements of broader learning and groundings in the samurai way.[65] At the same time, he concluded that "military personnel in leadership positions must have not only logical and analytical capabilities, but also have prudence, sagacity and decision-making capabilities from a broader perspective." In other words, compared to the military leaders of Showa who pursued local, specialized, optimal solutions, those of Meiji were able to find the optimal solution holistically and socially. The term holistic likely includes "inexperienced situations," while prudence and intelligence exclude "problem postponement." In addition, "depth of wisdom (= decision-making

---

60 The discussion based on historical materialism that serves as the prelude to the indication here refers to Simone Weil, *Sensou ni kansuru shosatsu* [Investigations into war], translated by Ito Akira in Hashimoto Ichimei, and Watanabe Kazutami eds. *Simone Weil chosaku-syu vol.1* [Works of Simone Weil vol.1, Reflections on Wars and Revolution: Early Critiques], (Tokyo: Shunjusha Publishing, 1968), pp.125-126.

61 For detail on capital intensive nature of the military, refer to Ono Keishi. "Jinko dotai to anzenhosho [Demographic trend and security]" *NIDS Journal of Defense and Security*, no.19, vol.1 (March, 2017), pp.4-5, pp.13-17, Brian Nichiporuk, *The Security Dynamics of Demographic Factors* (Santa Monica: RAND Corporation, 2000), p.27, p.29, and Paul Poast, *The Economics of War* (New York: McGraw-Hill Irwin, 2006), p.91.

62 Randolph Nikutta, "Artificial intelligence and the automated tactical battlefield," Allan M. Din ed., *Arms and Artificial Intelligence: Weapon and Arms Applications of Advanced Computing* (Oxford: Oxford University Press, 1987), p.109.

63 The error in synthesis is an issue in microeconomics, however, there are also risks of similar situations happening in system development (contradiction between systems) (Nagao, *Jinko chino to ningen*, pp.185-187.).

64 Habu and NHK Special News Crew, *Jinko chino no kakushin*, pp.86-89.

65 Tobe Ryoichi. "Meiji no gunjin to showa no gunjij [Military leaders in Meiji era and Showa era," *Military History* vol.52, no.1 (June, 2016), forward.

ability during unresolved situations)" by which Hironaka Heisuke, a prominent mathematician and Fields Medal laureate, cited as the superiority of the human brain over computers, too, could be viewed as similar.[66] The starting point for discussing the ideal vision for military units and personnel to co-exist with exceptionally correct and logical AI is believed to be in this area.

[66] Hironaka Heisuke describes the depth of knowledge as generosity and decisiveness as leap (Hironaka Heisuke, *Gakumon no hakken* [Discovery of studies: mathematicians talk about their thoughts and learning], (Tokyo: Kodansha bluebacks, 2018), pp.51-58.

Nuclear Weapon States, Nuclear Umbrella States, and the Treaty on the Prohibition of Nuclear Weapons (TPNW)*

ICHIMASA Sukeyuki**

Abstract

The Treaty on the Prohibition of Nuclear Weapons (TPNW) was adopted by the United Nations in July 2017 with the support of nearly two-thirds of the international community, despite opposition between nuclear weapon states and nuclear umbrella states on how to proceed with nuclear disarmament. Although the TPNW's preamble details its relationship with pre-existing treaties, a number of problems have been pointed out vis-à-vis the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) and the Comprehensive Nuclear-Test-Ban Treaty (CTBT). Additionally, analysis of the issues identified in the TPNW negotiations by the nuclear weapon states and the nuclear umbrella states suggests that they can be roughly aggregated into: i. The issue of the involvement of nuclear weapon states, ii. Concerns about the division of the international community, iii. Nuclear deterrence considerations, iv. Awareness of an increasingly severe international security environment, v. Warning about the risk of weakening the NPT system (concerns about compatibility with existing treaties), and vi. Inadequacies in verification mechanisms. The challenge for nuclear arms control and disarmament in the era of TPNW discussions is to find answers for these issues. It will become ever more important to consider the essential issues around nuclear deterrence and nuclear disarmament in order to facilitate constructive consensus-building among all concerned parties, looking ahead to the 2020 NPT Review Conference.

Introduction

In January 2018, the Bulletin of Atomic Scientists announced that its "Doomsday Clock" was set at 2 minutes to midnight, a matter that was widely covered in the media.[1] The Doomsday Clock is an attempt to illustrate how much time humanity has left until the end of the world, with the clock's hand striking midnight as a metaphor for the end of human history. The Doomsday Clock started in 1947, and was initially set at 7 minutes to midnight. It was then set at 2 minutes to midnight in 1953 following successful hydrogen bomb tests by the United States and the Soviet Union. The minute hand returned to 12 minutes to midnight when the Partial Test Ban Treaty (PTBT) came into effect in 1963 with the agreement of the United States, the Soviet Union, and the United

* Originally published in Japanese in *Boei Kenkyusho Kiyo* [NIDS Security Studies], vol.21, no.1, December 2018. This a translated version with the latest corrections and revisions as of June 2019.

** Senior Fellow, Defense Policy Division

1 "The Doomsday Clock: A Timeline of Conflict, Culture, and Change," The Bulletin of Atomic Scientists, 2018, https://thebulletin.org/timeline.

Kingdom, but in 1968 the minute hand once again advanced, to 7 minutes to midnight, with the outbreak of regional conflicts such as the Vietnam War, the Indo-Pakistani war, and the Arab-Israeli conflict. The Doomsday Clock was set back again in 1972 to 12 minutes to midnight as a result of the U.S.-Soviet Strategic Arms Limitation Talks (SALT) and the establishment of the Anti-Ballistic Missile Treaty, which were viewed as reducing competition over nuclear development. However, the minute hand later continued to advance, and in 1984, when the U.S.-Soviet Cold War deepened and contact between the two sides was cut off, the Doomsday Clock was set to 3 minutes to midnight. The Doomsday Clock struck its most distressing reading in the final stages of the Cold War, but then, with the collapse of the Cold War in 1991, it was set at 17 minutes to midnight, the best reading in its history. However, this did not last for long, and the minute hand gradually advanced, following the growing demand in the United States for a review of nuclear forces (1995, 14 minutes to midnight), nuclear tests in India and Pakistan (1998, 9 minutes to midnight), the rise of the threat of nuclear terrorism (2002, 7 minutes to midnight), and the U.S.-Russia Moscow Treaty (2010, 6 minutes to midnight), finally reaching 2 minutes to midnight in 2018, the worst reading since 1953.[2] As for background regarding the progress of the Doomsday Clock's minute hand in recent years, the outlook at the Bulletin of Atomic Scientists has darkened, because in addition to North Korea's nuclear weapons development, the United States and Russia have pointed out each other's treaty violations, the Intermediate-Range Nuclear Forces Treaty (INF) is expected to be abolished in full, there have been delays in negotiations, and the future of the New Strategic Arms Reduction Treaty (New START) is uncertain.[3]

In general, nuclear weapons management / disarmament has, from a historical perspective, had "waves," and the swell of these waves may increase, or be relatively low, depending on changes in the international security environment.[4] However, there are few precedents in which the Doomsday clock has been set at less than 3 minutes to midnight, and it should not be overlooked that the current critical awareness surrounding nuclear weapons is rising to the same level as when the United States and the Soviet Union were immersed in competitive development of hydrogen bombs under the Cold War structure. Amidst such a severe international security environment surrounding nuclear weapons, much attention was paid to the adoption of the Treaty on the Prohibition of Nuclear Weapons (TPNW) at the United Nations General Assembly in September 2017 and the fact that international momentum for international nuclear disarmament had resulted in the concluding of a multilateral treaty. This was also the focus of much attention by civil society and the media in Japan. Subsequently, the International Campaign to Abolish Nuclear Weapons (ICAN), an international NGO closely involved in negotiations, was awarded the Nobel Peace Prize. However, the nuclear weapon states and the majority of the nuclear umbrella states, which benefit from the extended deterrence of the nuclear weapon states, have taken opposing stands towards the TPNW negotiations. In particular, none of the nuclear weapon states participated in the TPNW negotiations held at the United Nations from March 27 to 31, 2017. The Japanese

---

2 Ibid.

3 John Mecklin, ed., "It is 2 Minutes to Midnight: 2018 Doomsday Clock Statement," The Bulletin of the Atomic Scientists, 2018, https://thebulletin.org/sites/default/files/2018 Doomsday Clock Statement.pdf.

4 Sukeyuki Ichimasa, *Kakujikken Kinshi no Kenkyu: Kakujikken no Senryakuteki Gani to Kokusaikihan* [A Study on the Comprehensive Nuclear-Test-Ban: International Norm and its Strategic Implications], (Tokyo: Shinzansya, 2018), p. 230.

government, which has advocated nuclear disarmament for many years as the only country to have ever suffered atomic bombings, also expressed an adverse view of the TPNW negotiations. In March 2017, Ambassador Nobushige Takamizawa issued a statement regarding Japan's position of not participating in TPNW negotiations as follows: "From discussions and considerations so far, it has become clear that the ban treaty concept has been unable to obtain understanding and involvement of nuclear-weapon states. Furthermore, this negotiation has not been formulated to pursue nuclear disarmament measures that will actually lead to the elimination of nuclear weapons, in cooperation with the nuclear weapon states. Regrettably, given the present circumstances, we must say that it would be difficult for Japan to participate in this Conference in a constructive manner and in good faith."[5]

Subsequently, the nuclear weapon states and all nuclear umbrella states, with the exception of the Netherlands, were absent from the negotiations, and the countries participating in the TPNW negotiations prepared an agreement text in a very short period of time and adopted the treaty on July 7, 2017, with 122 in favor, 1 in opposition (the Netherlands), and 1 absent (Singapore). As a result of nearly two-thirds of the international community working in partnership with civil society, a treaty was adopted that prohibits all nuclear weapons-related activities, including undertaking not to develop, test, produce, acquire, possess, stockpile, use or threaten to use nuclear weapons.[6] But from a different perspective, the remaining nearly one-third of the international community expressed their disapproval with the TPNW from its negotiation phase, and that remains the case today.

This paper considers the issues with and prospects for the TPNW after the negotiations concluded, taking into account the arguments between the nuclear weapon states and the nuclear umbrella states over the TPNW.

1. Overview of the Treaty on the Prohibition of Nuclear Weapons (TPNW)

(1) Historical Background Leading to the Drafting of the Treaty

One of the TPNW's roots is the model Nuclear Weapon Convention (mNWC),[7] which the UN Secretary-General distributed to all UN member states in 1997 at the request of Costa Rica, as well as a revised mNWC in 2008, which was again distributed to UN member states in response to a follow-up request from Costa Rica and Malaysia. Even as one of the TPNW's roots, the mNWC itself is very different from today's TPNW in terms of the structure of the verification mechanism.[8] At the time, the International Court of Justice (ICJ) was asked by the UN General Assembly, against a backdrop of strong international public opinion and voices from civil society,

---

5 Statement by H.E. Mr. Nobushige TAKAMIZAWA, Ambassador Extraordinary and Plenipotentiary, Permanent Representative of Japan to the Conference on Disarmament at the High-level Segment of the United Nations conference to negotiate a legally binding instrument to prohibit nuclear weapons, leading towards their total elimination, March 27, 2017, New York.

6 "UN conference adopts treaty banning nuclear weapons," United Nations News, July 7, 2017, https://news.un.org/en/story/2017/07/561122-un-conference-adopts-treaty-banning-nuclear-weapons.

7 "A/C.1/52/7," Official Document System of the United Nations, November 17, 1997, http://documents-dds-ny.un.org/doc/UNDOC/GEN/N97/334/78/IMG/N9733478.pdf?OpenElement.

8 Sukeyuki Ichimasa, "Dai 14-ko Kakugunshuku no Kensho Sochi Oyobi Fukagaku-sei" Ippan Shadan Hojin Nihon Senryaku Kenkyu Forum Hen, *NPT Handbook*," ["Section 14: Verification and Irreversibility of Nuclear Disarmament," Japan Forum for Strategic Studies (ed), *NPT Handbook*] (Japan Forum for Strategic Studies, 2017), p. 84.

for advisory opinions on the question of Does the threat or use of nuclear weapons in any case violate international law? In 1996, the ICJ clarified the view that nuclear weapons generally violate international law,[9] and the mNWC was drafted as a mock model treaty after compiling drafts from civil society experts such as lawyer groups, etc.[10] The later revised version of the mNWC then led to UN Secretary General Ban Ki-moon's five point proposal on nuclear disarmament in 2008. The five-point proposal for nuclear disarmament consisted of i. a request for all Nuclear Non-Proliferation Treaty (NPT) parties, in particular the nuclear weapon states, to fulfil their obligation under the treaty to undertake negotiations on effective measures leading to nuclear disarmament, ii. a request for the Security Council permanent members to commence discussions on security issues in the nuclear disarmament process, iii. a reaffirmation of the "rule of law which includes the early entry into force of the Comprehensive Nuclear-Test-Ban Treaty (CTBT), commencement of negotiations for the Fissile Material Cut-off Treaty (FMCT) without preconditions, and support for the entry into force of the Central Asian and African nuclear-weapon-free zones, iv. accountability and transparency of nuclear weapon states, and v. an appeal for the necessity of various complementary measures associated with disarmament of the weapons of mass destruction and other new weapons bans.[11]

Afterwards, when the humanitarian approach to nuclear disarmament was adopted at the 2010 NPT Review Conference, a joint statement on the humanitarian aspect of nuclear weapons was announced by 16 countries at the first NPT preparatory committee in 2012. Then, similar proposals were also submitted by 34 volunteer countries at the United Nations General Assembly in the same year.[12] At the second NPT preparatory committee in 2013, nuclear disarmament debate quickly gained endorsement, with 74 countries expressing support at the venue for a joint speech[13] delivered by South Africa, on the humanitarian aspect of nuclear weapons.[14]

Beyond discussions within the NPT framework, considerations also progressed from outside the conference. From 2013 to 2015, the International Conferences on the Humanitarian Impact of Nuclear Weapons were held in Oslo, Nayarit and Vienna. Nuclear weapon states, namely the United States and the United Kingdom, also participated in the conference, and various discussions were held on the humanitarian impact of nuclear weapons from a scientific point of view. Following this, at the 2015 Vienna Conference, the third such conference, the Pledge presented at the Vienna Conference on the Humanitarian Impact of Nuclear Weapons by Austrian Deputy Foreign Minister

---

9 Eiichi Sugie, "Kakuheiki to Kokusai Shisaibansho" [Nuclear Weapons and the International Court of Justice], *Chukyohogaku*, No. 32, 1997, pp. 3-6.

10 "Kakuheiki Kinshi Jyokaku to Iu Rekishi-teki Kaikyo" o Jitsugen Shita Costa Rica no Shikake ""[Costa Rica's "Scheme"" that Acheived the "Historic Achievement of the Nuclear Weapons Convention"]," Harbor Business Online, August 15, 2017, https://www.excite.co.jp/News/society_g/20170815/Harbor_business_148971.html.

11 "The Secretary-General's five point proposal on nuclear disarmament: The United Nations and security in a nuclear-weapon-free world," United Nations Office for Disarmament Affairs, July 30, 2018, https://www.un.org/disarmament/wmd/nuclear/sg5point/.

12 Mitsuru Kurosawa, "2013 NPT Preparatory Committee and Nuclear Disarmament," *Journal of Osaka Jogakuin University*, Vol.10 (2013), pp. 85-87.

13 "2015 nen NPT Unyo Kento Kaigi Dai 2 Kai Junbi Iinkai (Hyoka to Gaiyo) [2015 NPT Review Conference 2nd Prepatory Committee (Evaluation and Summary)]" Ministry of Foreign Affairs, May 3, 2013, http://www.mofa.go.jp/mofaj/gaiko/page3_000130.html.

14 Sukeyuki Ichimasa, "Threat of Cascading 'Permanent Blackout' Effects and High Altitude Electromagnetic Pulse (HEMP)," *NIDS Journal of Defense and Security*, Vol.18, No.2, February 2016, p. 18.

Michael Linhart[15] and the Humanitarian Pledge by the supporting states were issued.[16] In parallel with these, the UN General Assembly adopted a 2012 resolution (A/RES/67/56) that decided to implement an open-ended working group for multilateral nuclear disarmament negotiations to achieve and maintain a world free of nuclear weapons. The United Nations General Assembly subsequently adopted a 2013 resolution (A/RES/68/46) and a 2014 resolution (A/RES/69/41), and on December 7, 2015, adopted a resolution (A/RES/70/33)[17] to promote multilateral nuclear disarmament negotiations, based on a report (A/70/460) from the First Committee of the UN General Assembly. Then, on December 23, 2016, the United Nations General Assembly adopted a resolution (A/RES/71/258) [18] for the commencement of multilateral consultations, and the aforementioned TPNW negotiations began.

(2) Structure of the TPNW

The structure of the TPNW, published on the United Nations website on July 7, 2017, is as follows.[19]

Article 1	Prohibitions
Article 2	Declarations
Article 3	Safeguards
Article 4	Towards the total elimination of nuclear weapons
Article 5	National implementation
Article 6	Victim assistance and environmental remediation
Article 7	International cooperation and assistance
Article 8	Meeting of States Parties
Article 9	Costs
Article 10	Amendments
Article 11	Settlement of disputes
Article 12	Universality
Article 13	Signature
Article 14	Ratification, acceptance, approval or accession
Article 15	Entry into force
Article 16	Reservations
Article 17	Duration and withdrawal

---

15 "Pledge presented at the Vienna Conference on the Humanitarian Impact of Nuclear Weapons by Austrian Deputy Foreign Minister Michael Linhart," Vienna Conference on the Humanitarian Impact of Nuclear Weapons, December 8-9, 2014, https://www.bmeia.gv.at/fileadmin/user_upload/Zentrale/Aussenpolitik/Abruestung/HINW14/HINW14_Austrian_Pledge.pdf.

16 "Humanitarian Pledge," Vienna Conference on the Humanitarian Impact of Nuclear Weapons, December 8-9, 2014, https://www.bmeia.gv.at/fileadmin/user_upload/Zentrale/Aussenpolitik/Abruestung/HINW14/HINW14vienna_Pledge_Document.pdf.

17 "A/RES/70/33," Official Document System of the United Nations, December 11, 2015, http://undocs.org/A/RES/70/33.

18 "A/RES/71/258," Official Document System of the United Nations, January 11, 2017, http://undocs.org/A/RES/71/258.

19 "Treaty on the Prohibition of Nuclear Weapons," Official Document System of the United Nations, July 7, 2017, https://treaties.un.org/doc/Treaties/2017/07/20170707 03-42 PM/Ch_XXVI_9.pdf.

Article 18 Relationship with other agreements
Article 19 Depositary
Article 20 Authentic texts

Given the scope of the treaty, the structure of the treaty text is relatively simple compared to other existing disarmament and non-proliferation agreements. One of the TPNW's characteristic is, for instance, the lack of provisions relating to the Treaty's implementing body, such as provided for in the Chemical Weapons Convention (CWC) and the CTBT, and the absence of provisions relating to decision-making bodies analogous to an Executive Board. Moreover, in precedents such as the CWC and the CTBT, verification-related provisions tend to be positioned as particularly important elements in the treaty. (*In the case of the CWC, there is the "Annex on Implementation and Verification" (Verification Annex), and the CTBT has "Article IV. Verification," and "Protocol Part I. The International Monitoring System and International Data Centre functions," "Protocol Part II. On-site inspections," and "Protocol Part III. Confidence Building Measures"). On the other hand, the mechanism for verifying compliance with the agreement is not stipulated in detail in the TPNW. Specifically, Article 4, Paragraph 6 of the TPNW stipulates that "The States Parties shall designate a competent international authority or authorities to negotiate and verify the irreversible elimination of nuclear-weapons programmes, including the elimination or irreversible conversion of all nuclear weapons-related facilities in accordance with paragraphs 1, 2 and 3 of this Article," but as for the means of conducting the verification, it is only stipulated, in Article 4, Paragraph 1, that "The competent international authority shall report to the States Parties. Such a State Party shall conclude a safeguards agreement with the International Atomic Energy Agency sufficient to provide credible assurance of the non-diversion of declared nuclear material from peaceful nuclear activities and of the absence of undeclared nuclear material or activities in that State Party as a whole."

From the viewpoint of international politics and international law, the focus has been mainly on the relationship between the NPT and the TPNW. However, this paper points out that the TPNW's provisions related to the prohibition of nuclear tests and its relationship with the CTBT also require careful consideration. For instance, Article 1, Paragraph 1 of the TPNW stipulates that "Each State Party undertakes never under any circumstances to: (a) Develop, test, produce, manufacture, otherwise acquire, possess or stockpile nuclear weapons or other nuclear explosive devices." In addition, Article 1, Paragraph 1 also proscribes "(d) Use or threaten to use nuclear weapons or other nuclear explosive devices." What is of note here is the phrase "experiments with nuclear weapons or other explosive nuclear devices," or, more specifically, the definition of "experiment." In the negotiation process for the TPNW draft, there was also a point of contention over if the TPNW should newly prohibit computer simulations, hydrodynamic tests, laser fusion experiments, and subcritical experiments, which were not included in the scope of the CTBT.[20] However, the TPNW preamble also clearly mentions the relationship with the CTBT. Historically,

[20] John Burroughs, "Key Issues in Negotiations for a Nuclear Weapons Prohibition Treaty," *Arms Control Today*, June 2017, https://www.armscontrol.org/act/2017-06/features/key-issues-negotiations-nuclear-weapons-prohibition-treaty.

the CTBT has adopted the "zero yield concept" [21] based on the idea that no nuclear yield should be allowed. For this reason, there is an interpretation[22] that the TPNW has also banned nuclear tests based on the same definition of nuclear explosion as the CTBT. However, considering that Article 1(a) prohibits the "production and manufacture of nuclear weapons or other nuclear explosive devices," aside from its technical verifiability, it can be read that the TPNW intends more, in a practical sense, than what is prohibited by the CTBT.[23]

At the moment, it is said that at the meetings related to the CTBT Organization Preparatory Committee, discussions and statements in the context of TPNW will not be included in the conference reports.[24] However, when the TPNW comes into effect in the future, it may be necessary to assume that a political gap will possibly arise at the other nuclear disarmament related fora.[25] Of course, there is another way of looking at the issues surrounding the TPNW and the prohibitions of nuclear testing. For example, there are positive indications that if the TPNW comes into effect in the future, there will also be new momentum for the CTBT to enter into force.[26] In any case, it goes without saying that, at the appropriate timing, efforts should be made to ensure that there is a constructive relationship between the TPNW and existing nuclear disarmament agreements.

On the other hand, Article 4 of the TPNW calls for the complete elimination of nuclear weapons, "Each State Party that after 7 July 2017 owned, possessed or controlled nuclear weapons or other nuclear explosive devices and eliminated its nuclear-weapon programme, including the elimination or irreversible conversion of all nuclear weapons-related facilities, prior to the entry into force of this Treaty for it, shall cooperate with the competent international authority designated pursuant to paragraph 6 of this Article for the purpose of verifying the irreversible elimination of its nuclear-weapon programme," and Article 4, Paragraph 2 stipulates that "Notwithstanding Article 1 (a), each State Party that owns, possesses or controls nuclear weapons or other nuclear explosive devices shall immediately remove them from operational status, and destroy them as soon as possible but not later than a deadline to be determined by the first meeting of States Parties, in accordance with a legally binding, time-bound plan for the verified and irreversible elimination of that State Party's nuclear-weapon programme, including the elimination or irreversible conversion of all nuclear-weapons-related facilities." These TPNW provisions go far beyond the scope of the nuclear disarmament obligations set out in Article VI of the NPT. The strong wording ("shall") for nuclear weapon states also recalls that the treaty was drafted with an inflexible determination to abolish nuclear weapons. In addition, the fact that Article 6 of the TPNW deals with victim assistance and environmental remediation, as mentioned in the discussion on the humanitarian impacts of nuclear weapons, represents the origin of TPNW negotiations.

As described above, various problems have been raised over the relationship between the TPNW and the NPT. However, the relationship with existing international treaties is clearly

---

21 Ola Dahlman, Jenifer Mackby, Svein Mykkelveit and Hein Haak, eds., *Detect and Deter: Can Countries Verify the Nuclear Test Ban?* (New York: Springer, 2011), p. 21.

22 Oliver Meier, Sira Cordes and Elisabeth Suh, "What Participants in a Nuclear Weapons Ban Treaty (Do Not) Want," Bulletin of the Atomic Scientists, June 9, 2017, https://thebulletin.org/2017/06/what-participants-in-a-nuclear-weapons-ban-treaty-do-not-want/.

23 Ichimasa, *Kakujikken Kinshi no Kenkyu* [A Study on the Comprehensive Nuclear-Test-Ban] pp. 227-228.

24 Author's interview with the CTBTO related conference participants, April 13, 2019.

25 Ichimasa, *Kakujikken Kinshi no Kenkyu* [A Study on the Comprehensive Nuclear-Test-Ban] pp. 227-228.

26 Shervin Taheran, "Trump Administration Silent on CTBT," *Arms Control Today*, October 2017, p. 25.

mentioned in the preamble of the TPNW as follows.

It states that "Reaffirming also that the full and effective implementation of the Treaty on the Non-Proliferation of Nuclear Weapons, which serves as the cornerstone of the nuclear disarmament and non-proliferation regime, has a vital role to play in promoting international peace and security," "Recognizing the vital importance of the Comprehensive Nuclear-Test-Ban Treaty and its verification regime as a core element of the nuclear disarmament and non-proliferation regime," and "Reaffirming the conviction that the establishment of the internationally recognized nuclear-weapon-free zones on the basis of arrangements freely arrived at among the States of the region concerned enhances global and regional peace and security, strengthens the nuclear non-proliferation regime and contributes towards realizing the objective of nuclear disarmament."

(3) The Impact of Civil Society Efforts on Treaty Negotiations

After the 2010 NPT Review Conference and international conferences on the humanitarian aspects of nuclear weapons, the process leading to the TPNW negotiations saw strong involvement by civil society, as symbolized by The International Campaign to Abolish nuclear Weapons (ICAN), and coordinated action by the negotiation-promoting countries that assisted ICAN. On the subject of arms control and disarmament treaties that are set against a backdrop of such civil society involvement, and setting aside international organizations such as the United Nations that permit the active participation of NGOs, there are examples of NGOs with specialized knowledge and skills exerting great influence in various fields. One such case is the Ottawa Process for the prohibition of anti-personnel landmines. Furthermore, there are instances in which large, influential countries have taken action at the urging of NGOs,[27] which has in turn sent a strong message to other countries.[28] Thus, there has emerged a process whereby the national policies of various countries are being affected by the "norms" sought by NGOs.[29] It is evident that such a process was also generally followed in the TPNW negotiations.

Prior to receiving the Nobel Peace Prize,[30] on July 7, 2017, ICAN Executive Director Beatrice Fihn issued a statement regarding the adoption of TPNW: "It is beyond question that nuclear weapons violate the laws of war and pose a clear danger to global security. No one believes that indiscriminately killing millions of civilians is acceptable – no matter the circumstance – yet that is what nuclear weapons are designed to do. Today the international community rejected nuclear weapons and made it clear they are unacceptable" and additionally that "As has been true with previous weapon prohibition treaties, changing international norms leads to concrete changes in policies and behaviors, even in states not party to the treaty. The strenuous and repeated objections of nuclear-armed states is an admission that this treaty will have a real and lasting impact."[31]

---

27 Kenki Adachi, "The Ottawa Process: formation of anti-personnel landmines ban regime" (Yushindo, 2004), pp. 49-50.

28 Ibid., p. 70.

29 Ibid., p. 71.

30 "The Nobel Peace Prize 2017: International Campaign to Abolish Nuclear Weapons (ICAN)," The Official Web Site of the Nobel Prize, July 30, 2018, https://www.nobelprize.org/nobel_prizes/peace/laureates/2017/.

31 "The United Nations Prohibits Nuclear Weapons," International Campaign to Abolish Nuclear Weapons, July 7, 2017, http://www.icanw.org/campaign-news/the-united-nations-prohibits-nuclear-weapons/.

(4) Comprehensive Approach for Nuclear Disarmament or Building Blocks / Step-by-Step Approach

Prior to the treaty negotiations, the TPNW proponents, nuclear weapon states, and nuclear umbrella states announced different policy approaches with the same goal: the comprehensive approach and the building blocks approach. The former approach was an idea from countries promoting the TPNW and sought to achieve a world without nuclear weapons by stipulating the prohibition of nuclear weapon use and the threat of nuclear weapon development / possession / use, as legal obligations, and then developing international norms for the elimination of nuclear weapons in a comprehensive manner. On the other hand, the latter approach was mainly advocated for by nuclear weapon states and nuclear umbrella states. With the final goal being a world without nuclear weapons, it is based on existing relevant multilateral agreements and international treaties and gradually builds up nuclear non-proliferation and substantive reductions while taking a critical look at the actual international security environment (also called the "step-by-step approach").

There have been various discussions made about these two approaches and common ground can be found on some issues. For example, that the proponents of the TPNW advocate a comprehensive approach does not necessarily mean that they disregard existing multilateral agreements or international treaties. One of the major TPNW proponents, Austria, stated in 2016 that it "fully supports all legal and practical measures that contribute to the overarching goal of achieving a world free from nuclear weapons," specifically listing practical measures "such as entry into force and universalization of the CTBT, the negotiation of an FMCT, the elaboration of effective verification tools for nuclear disarmament, the granting of negative security assurances and no first use policies by nuclear weapons States, measures for de-alerting, deemphasizing the role of nuclear weapons in security doctrines and other measures," stressing that "all these measures can and have to be pursued simultaneously with the establishment of a legally-binding instrument to prohibit nuclear weapons."[32] In this way, even if TPNW proponents are dissatisfied with the conventional method, instead of abandoning the current NPT regime and pursuing nuclear disarmament anew under the TPNW, they can pursue an approach that balances the merits of both the building blocks approach and the TPNW. However, the TPNW negotiations have been followed in parallel by discussions between TPNW supporters and TPNW skeptics, with various statements being issued about the negotiation process itself, including on the scope of the treaty, participating countries, the relationship with existing nuclear disarmament and non-proliferation treaties, and the current international security environment. Examining these issues and continuing dialogue will eventually produce meaningful common ground.

In any case, civil society and countries promoting the negotiations had no shortage of expectations that the TPNW would serve as a measure for fulfilling the obligation under Article VI of the NPT to pursue nuclear disarmament negotiations, and that it would address the double standard applied to those inside and outside the NPT, the expanding gap between those inside and outside the NPT regime, and loopholes that enabled nuclear proliferation to be disguised as peaceful uses of nuclear energy.

---

[32] "Shiryo 2 Osutoria Daihyo Tomasu Hainotsu no Seimei (bassui-yaku)" [Document 2: Statement by Austrian Ambassador Thomas Hajnoczi (Excerpt)], Peace Depot, October 14, 2016, http://www.peacedepot.org/nmtr/506-7-03/.

2. Reactions of Nuclear Weapon States, Nuclear Umbrella States, and Other Non-Nuclear Weapon States Before, During and After the TPNW Negotiations

It has already been mentioned that while the TPNW gained the support of nearly two-thirds of the international community, the remaining one-third of countries have, from the negotiation process, expressed disapproval of the treaty. The major problem here is that these remaining countries still rely on nuclear deterrence for security while supporting existing efforts for a world without nuclear weapons. As such, it is a reality that they take a position against the TPNW since it is not consistent with their security policy. This chapter presents a summary of stances and responses from the major nuclear weapon states and the nuclear umbrella states to the TPNW negotiations and the treaty itself, along with attempts to identify issues common to those countries in terms of their non-support for the TPNW.

(1) Nuclear Weapon States

(A) The Five Nuclear Weapon States (N5)

The five nuclear weapon states (N5),[33] in a Joint Statement issued at the 2015 NPT review conference, stated that "We reaffirm the shared goal of nuclear disarmament and general and complete disarmament as referenced in the preamble and provided for in Article VI of the NPT," and then, in particular on nuclear disarmament, that "We continue to believe that an incremental, step-by-step approach is the only practical option for making progress towards nuclear disarmament, while upholding global strategic security and stability (*emphasis here and below is added by author)." Furthermore, it was pointed out that "All States can help fulfill this goal by creating the necessary security environment through resolving regional tensions, tackling proliferation challenges, promoting collective security, and making progress in all areas of disarmament."

In the 2016 N5 Joint Statement,[34] it was stated that "The P5 reaffirmed the ongoing relevance of all provisions of the Action Plan adopted by consensus at the 2010 NPT Review Conference that remains an indispensable roadmap for the implementation of all the three pillars of the NPT" and also that "The P5 all reaffirmed the importance of full compliance with existing, legally-binding arms control, nonproliferation, and disarmament agreements and obligations as an essential element of international peace and security." Interestingly, the line "The P5 also decided to seek enhanced international understanding of the role of nuclear weapons in the overall international security environment" can be interpreted as a request for the international community to understand the significance of nuclear weapons as a deterrent.

Then, in the N5 Joint Statement[35] issued in July 2017 when the TPNW was adopted by the United Nations General Assembly, stating that "Accession to the ban treaty is incompatible with the policy of nuclear deterrence, which has been essential to keeping the peace in Europe and

---

33 "Statement by the People's Republic of China, France, the Russian Federation, The United Kingdom of Great Britain and Northern Ireland, and the United States of America to the 2015 Treaty on the Non-Proliferation of Nuclear Weapons Review Conference," United Nations 2015 NPT Review Conference, July 30, 2018, http://www.un.org/en/conf/npt/2015/statements/pdf/P5_en.pdf.

34 "Joint Statement From the Nuclear-Weapons States at the 2016 Washington, DC P5 Conference," U.S. Department of State, September 15, 2016, https://2009-2017.state.gov/r/pa/prs/ps/2016/09/261994.htm.

35 "Joint Press Statement from the Permanent Representatives to the United Nations of the United States, United Kingdom, and France Following the Adoption of a Treaty Banning Nuclear Weapons," United States Mission to the United Nations, July 7, 2017, https://usun.state.gov/remarks/7892.

North Asia for over 70 years." as well as the criticism that "This treaty offers no solution to the grave threat posed by North Korea's nuclear program, nor does it address other security challenges that make nuclear deterrence necessary."

(B) NATO

On September 20, 2017, NATO issued a press release concerning the TPNW.[36] This press release, while explaining policies for nuclear deterrence and disarmament presented at the NATO Warsaw Summit in July 2016, states that NATO is pursuing a world without nuclear weapons, under Article VI of the NPT, and that the existence of the step-by-step method and verification mechanisms for compliance with the agreement will contribute to international peace and stability. Of particular note in this press release is where it clearly points out NATO's stance on nuclear weapons that "The fundamental purpose of NATO's nuclear capability is to preserve peace, prevent coercion, and deter aggression. Allies' goal is to bolster deterrence as a core element of our collective defence and to contribute to the indivisible security of the Alliance. As long as nuclear weapons exist, NATO will remain a nuclear alliance." Additionally, strong criticism towards the TPNW was added, saying that "Seeking to ban nuclear weapons through a treaty that will not engage any state actually possessing nuclear weapons will not be effective, will not reduce nuclear arsenals, and will neither enhance any country's security, nor international peace and stability. Indeed it risks doing the opposite by creating divisions and divergences at a time when a unified approach to proliferation and security threats is required more than ever."

(C) The United Kingdom

The United Kingdom, in a statement[37] issued on July 8, 2017, said that "As a responsible Nuclear Weapons State the UK continues to work with international partners towards creating the conditions for a world without nuclear weapons." and then, "However, we will not sign the treaty which has been published today. As we have previously made very clear, we do not believe that this treaty will bring us closer to a world without nuclear weapons. This treaty fails to address the key issues that must first be overcome to achieve lasting global nuclear disarmament." Specifically, "It will not improve the international security environment or increase trust and transparency." and "This treaty also risks undermining and weakening the Nuclear Non Proliferation Treaty" were cited as missing key issues. It was then noted that "As has been made clear, the UK, as a Nuclear Weapons State, has been pursuing a step by step approach to nuclear disarmament consistent with the NPT and its other treaty commitments."

---

[36] "Press Release (2017) 135: North Atlantic Council Statement on the Treaty on the Prohibition of Nuclear Weapons," North Atlantic Treaty Organization, September 20, 2017, https://www.nato.int/cps/ua/natohq/news_146954.htm.

[37] "UK Statement on Treaty Prohibiting Nuclear Weapons," UK Foreign & Commonwealth Office, July 8, 2017, https://www.gov.uk/government/news/uk-statement-on-treaty-prohibiting-nuclear-weapons.

(D) France

France also issued a statement[38] on July 7, 2017, saying that "France did not take part in the negotiations for this treaty and does not intend to comply with it. The treaty does not bind us and does not create new obligations." Additionally, France had criticisms that "France's security and defence policy, just like those of the allies and other close partners, is based on nuclear deterrence" and "a treaty banning nuclear weapons risks affecting the security of the Euro-Atlantic region and international stability. The treaty is also likely to undermine the Treaty on the Non-Proliferation of Nuclear Weapons, the cornerstone of the non-proliferation regime."

(2) Nuclear Umbrella States and Other Major Non-Nuclear Weapon States

(A) Japan

Japan issued the following statement at the First Session of the Conference to Negotiate a Legally Binding Instrument to Prohibit Nuclear Weapons, Leading Towards their Total Elimination in March 2017, saying that "It is therefore crucial to have a realistic perspective as to how nuclear disarmament measures can contribute effectively to addressing actual security concerns that each country and region faces," also that "the engagement of the nuclear-weapon states is indispensable for the advancement of nuclear disarmament." and that "The most important thing is to build confidence and trust among states, including nuclear-weapon states, and thereby accumulate various realistic and practical measures through bilateral and multilateral efforts, such as agreeing on a concrete measure to reduce nuclear weapons." It was then noted that "It is also necessary to resolve regional issues and thereby to remove the elements that give states the motives to possess nuclear weapons. In this way, we have to accelerate our efforts to create an enabling security environment for the elimination of nuclear weapons," and that "After accumulating such efforts, through actions by all countries, including nuclear-weapon states and non-nuclear-weapon states, we can then expect to reach what our proposed Progressive Approach calls "a minimisation point," at which the number of nuclear weapons will be very low. Only when this achievement is within reach, will it be possible to make an effective and meaningful legal instrument as the final building block to achieve and maintain a world free of nuclear weapons," and then continuing that "At that stage, we will be able to give further thought to an appropriate framework for nuclear disarmament, including a multilateral nuclear weapons convention, which should be nondiscriminatory and internationally verifiable."[39] The statement addresses the severe international security environment while pointing out the importance of involvement from the nuclear weapon states at the highest levels, and that it is only possible to consider a verifiable nuclear disarmament framework after promoting a realistic approach to nuclear disarmament or promoting the building block approach, and after reaching the so-called "minimization point," the stage at which nuclear weapons have been sufficiently reduced. In addition, Minister for Foreign Affairs Fumio Kishida, at a press conference held at the Prime Minister's Official Residence around the time the TPNW was adopted, answered that "We

---

38 "Adoption of a Treaty Banning Nuclear Weapons (New York, 7 July 2017)," France Diplomatie, 2017, https://www.diplomatie.gouv.fr/en/french-foreign-policy/united-nations/events/events-2017/article/adoption-of-a-treaty-banning-nuclear-weapons-07-07-17.

39 "Statement by H.E. Mr. Nobushige TAKAMIZAWA, Ambassador Extraordinary and Plenipotentiary, Permanent Representative of Japan to the Conference on Disarmament at the High-level Segment of the United Nations conference to negotiate a legally binding instrument to prohibit nuclear weapons, leading towards their total elimination," Ministry of Foreign Affairs, July 30, 2018, https://www.mofa.go.jp/mofaj/files/000243024.pdf.

consider that this treaty differs from our view and approach, which is aimed at 'a world free of nuclear weapons.' We believe we should not exacerbate the serious situation of the confrontation between nuclear-weapon states and non-nuclear-weapon states. Specifically, we will patiently and firmly pursue the arrangements we have been striving for to date including frameworks participated by both sides such as the Nuclear Non-Proliferation Treaty (NPT), the Comprehensive Nuclear-Test-Ban Treaty Organization (CTBT) and the Fissile Material Cutoff Treaty (FMCT)."[40]

Although it was not a statement that directly referred to the TPNW, Prime Minister Shinzo Abe responded to a Representative's question in a House of Representatives Plenary Session, saying that "As the only country to have ever suffered the devastation of atomic bombings during war, Japan will work with both nuclear weapon states and non-nuclear weapon states, playing a leading bridging role and striving to realize, from a realistic point of view, a world free of nuclear weapons,"[41] explaining that Japan's position should be as a "bridging role." In addition, Minister of Foreign Affairs Taro Kono pointed out that the humanitarian aspect and security considerations are always important when addressing nuclear disarmament and that it is necessary to move nuclear weapon states to realize nuclear disarmament and abolition, but that the TPNW cannot do so. In addition, the TPNW does not take into account actual security perspectives and has not received the support of non-nuclear weapon states such as Japan, the Republic of Korea, Germany, and other NATO countries that are exposed to nuclear threats.[42] Furthermore, Minister Kono warned that, no matter how grand and noble the TPNW's purpose is in the abolition of nuclear weapons, participating in a treaty that immediately makes nuclear weapons illegal will undermine the legitimacy of nuclear deterrence, and, as a result, people's lives and property could be endangered by nuclear threats, as symbolized by North Korea's nuclear weapons.[43]

(B) Germany

On October 6, 2017, the German deputy government spokesperson issued a statement in response to ICAN's receipt of the Nobel Peace Prize,[44] and, after sending congratulations on behalf of the German government for the Nobel Prize Committee's selection and ICAN's award, made the appeal that "the German government is 'firmly committed to the goal of achieving what is termed 'global zero,' or a world that is completely free of nuclear weapons.'" Continuing, she said that "Some states, however, still see nuclear weapons as something that can be used in military conflicts. 'For as long as this remains the case, and Germany and Europe are threatened by this, the need to uphold a nuclear deterrent remains. This is assured by NATO.'" Although it was a soft tone and coupled with congratulations to ICAN, this should be seen as a request for understanding for the position of NATO member states in regard to the TPNW.

---

40 "Press Conference by Foreign Minister Fumio Kishida," Ministry of Foreign Affairs, July 11, 2017, https://www.mofa.go.jp/press/kaiken/kaiken3e_000025.html.

41 *Sankei Shimbun*, January 26, 2018.

42 Taro Kono, "Kakuheiki Kinshi Jyoyaku" [Treaty on the Prohibition of Nuclear Weapons], Blogos, November 21, 2017, http://blogos.com/article/260530/.

43 Ibid.

44 "Nobel Peace Prize 2017: For a world without nuclear weapons," The Federal Government, October 6, 2017, https://www.bundesregierung.de/Content/EN/Artikel/2017/10_en/2017-10-06-friedensnobelpreis_en.html.

(C) Australia

Australia, one of the nuclear umbrella states that led the Non-Proliferation and Disarmament Initiative (NPDI) together with Japan, expressed its stance towards the TPNW on the Department of Foreign Affairs and Trade's website.[45] The site stated that "The Australian Government is not participating in the abovementioned UN Conference to negotiate a treaty to ban nuclear weapons. This approach is consistent with our clear and longstanding position on the proposed treaty to ban nuclear weapons which recognises that such a treaty does not offer a practical path to effective disarmament or enhanced security," continued that "a ban treaty risks undermining the NPT which Australia rightly regards as the cornerstone of the global non-proliferation and disarmament architecture" and then warned that "A ban treaty could create parallel obligations and thus ambiguity and confusion and would deepen divisions between nuclear and non-nuclear weapons states." It then pointed out that "With a simple prohibition treaty, there would also be no effective verification measures to ensure compliance."

(D) Norway

Norway, as a member of NATO, a nuclear alliance, is in the position of being a nuclear umbrella state, but at the same time is in a unique position and has demonstrated a strong presence, such as showing a marked increase in public debate since 2010 ahead of its hosting of the 2013 Oslo Conference on the humanitarian impact of nuclear weapons.[46] However, as a result of a change in Norway's government in 2015, its position on nuclear weapon's humanitarian impact has altered significantly. Consequently, Norway voted against all three nuclear weapons related resolutions at the 2015 United Nations General Assembly.[47] The Norwegian Minister of Foreign Affairs, Børge Brende issued a statement that Norway, as a member of the NATO nuclear alliance, as shown by NATO's "New Strategic Concept", cannot support nuclear weapons related resolutions at the United Nations General Assembly, and additionally that these resolutions should not be supported by any NATO member states.[48] However, there was strong pushback[49] on this issue from the various domestic opposition parties, and in a Norwegian People's Aid public opinion poll in September 2017, 78% of survey respondents answered that Norway should sign the TPNW.[50] Afterwards,

---

45 "Australia's Nuclear Non-Proliferation and Disarmament Policy," Australian Government Department of Foreign Affairs and Trade, July 30, 2018, http://dfat.gov.au/international-relations/security/non-proliferation-disarmament-arms-control/nuclear-weapons/Pages/australias-nuclear-non-proliferation-and-disarmament-policy.aspx.

46 Sukeyuki Ichimasa, "Dai 14-ko Kakugunshuku no Kensho Sochi Oyobi Fukagaku-sei" Ippan Shadan Hojin Nihon Senryaku Kenkyu Forum Hen, *NPT Handbook*," ["Section 14: Verification and Irreversibility of Nuclear Disarmament," Japan Forum for Strategic Studies (ed), *NPT Handbook*] (Japan Forum for Strategic Studies, 2017), p. 22.

47 "Norway did not Support UN Resolutions on Nuclear Weapons," Norwegian People's Aid, November 3, 2015, https://www.npaid.org/News/News-archive/2015/Norway-did-not-support-UN-Resolutions-on-Nuclear-Weapons.

48 "Norway blasted over UN nuclear vote," *News in English.no*, November 4, 2015, http://www.newsinenglish.no/2015/11/04/norway-blasted-for-un-nuclear-vote/.

49 "Norway's Parliament wants a ban on nuclear weapons," Norwegian People's Aid, March 10, 2015, https://www.npaid.org/News/News-archive/2016/Norway-s-Parliament-wants-a-ban-on-nuclear-weapons.

50 "8 out of 10 thinks that Norway should sign the UN ban on nuclear weapons," *Norway Today*, September 6, 2017, http://norwaytoday.info/news/8-10-thinks-norway-sign-un-ban-nuclear-weapons/.

the opposition party came to power in December, and it was reported[51] that a policy review for the TPNW was being considered, based on the views of civil society and experts. In fact, on February 8, 2018, a resolution was passed in the Storting (the Norwegian Parliament), with 56 in favor and 43 opposed, requesting the government investigate the possibility of participating in the TPNW as a NATO member.[52] This development resulted in a great deal of attention being paid to the Storting's investigation, and when the investigation's report was published on the official website on November 28, 2018, it concluded once again that the Norwegian government should not join the TPNW after considering factors that would arise with participation in the TPNW, Norway's obligations as a NATO member, and the problem that TPNW was negotiated outside the NPT framework, etc.[53]

As an aside, during the 2018 time period, movement at the parliamentary level regarding the possibility of participating in the TPNW was not limited solely to the Norwegian case. According to ICAN, the international NGO, a bill in Italy is said to have passed Parliament on the eve of the TPNW's adoption in September 2017, with the bill ordering a governmental investigation into the possibility of participating in the TPNW as a NATO member and, in particular, the compatibility of being a 'nuclear alliance' member state with a treaty that legally requires the prohibition of nuclear weapons.[54]

(E) Sweden

Although it is not a NATO member state, as in the aforementioned cases of Norway and Italy, it was also reported in October 2017 that Sweden nominated Lars-Erik Lundin of the Stockholm International Peace Research Institute (SIPRI) to investigate effects accompanying the Swedish government's participation in the TPNW.[55] Such an investigation in Sweden takes into consideration and confirms the TPNW's consistency with Sweden's involvement in existing treaties such as the NPT, the CTBT, or European Union (EU) related agreements in addition to Sweden's bilateral and multilateral security and defence policy cooperations.[56] Although Sweden expressed its support when the TPNW was adopted, it appears that Sweden is reluctant to proceed to signing and ratification the TPNW, as the country has recognized that the treaty itself contains critical elements that are at odds with what it is seeking.[57]

---

51 *Tokyo Shimbun*, December 24, 2017.

52 *Shimbun Akahata*, February 10, 2018.

53 "Review of the consequences for Norway of ratifying the Treaty on the Prohibition of Nuclear Weapons," Government of Norway, November 28, 2018, https://www.regjeringen.no/en/dokumenter/review_tpnw/id2614520/#overall.

54 "Italian Parliament Instructs Italy to Explore Possibility of Joining the Nuclear Ban Treaty," International Campaign to Abolish Nuclear Weapons, September 20, 2017, http://www.icanw.org/campaign-news/italian-parliament-instructs-italy-to-explore-possibility-of-joining-the-nuclear-ban-treaty/.

55 "SIPRI Fellow to Lead Inquiry on Sweden and the Treaty on the Prohibition of Nuclear Weapons," Stockholm International Peace Research Institute, October 25, 2017, https://www.sipri.org/news/2017/sipri-fellow-lead-inquiry-sweden-and-treaty-prohibition-nuclear-weapons.

56 "Inquiry into the consequences of a possible Swedish accession to the Treaty on the Prohibition of Nuclear Weapons," Government Offices of Sweden, October 23, 2017, http://www.government.se/press-releases/2017/10/inquiry-into-the-consequences-of-a-possible-swedish-accession-to-the-treaty-on-the-prohibition-of-nuclear-weapons/.

57 Alicia Sanders-Zakre, "States Hesitate to Sign Nuclear Ban Treaty," *Arms Control Today*, September 2017, https://www.armscontrol.org/act/2017-09/news/states-hesitate-sign-nuclear-ban-treaty.

(F) The Netherlands

It can be said that the Netherlands is the nuclear umbrella state that attracted the most attention during the TPNW negotiations. The Netherlands, the only NATO member state that participated in the TPNW negotiations via a decision by the States General (the Netherland's Parliament), emphasized that "such an instrument should be verifiable as well as comprehensive and that it should enjoy the support of nuclear-weapon possessors and non-nuclear-weapon states alike in order to be effective," additionally stating "And that it must not detract from the NPT and Article VI, including the chronology inherent therein."[58]

(G) Iceland

In Iceland, when the TPNW was released for signing, Minister for Foreign Affairs Gudlaugur Thór Thórdarson stated that "Iceland's position towards nuclear weapons is very clear: that the aim shall be a world without nuclear weapons, and that these weapons shall be destroyed in a systematic, mutual manner. The most realistic way to do this, which is also the way which we believe will be most effective, is to continue to rely on the agreements and processes that already exist, such as the Non-Proliferation Treaty (NPT) and the Comprehensive Test-Ban Treaty (CTBT)."[59]

To this point, this paper has reviewed statements from major countries and regional organizations, and the major points can be summarized as follows: i. The issue of the involvement of nuclear weapon states, ii. Concerns about the division of the international community, iii. Nuclear deterrence considerations, iv. Awareness of an increasingly severe international security environment, v. Warning about the risk of weakening the NPT regime (concerns about compatibility with existing treaties), and Vi. Inadequacies in verification mechanisms. Of these, i., iii., and iv. have been consistent points of criticism for the TPNW in the context of nuclear deterrence, followed by ii. and v., which can be seen as widely accepted concerns that the TPNW will erode the NPT itself and confuse each country's efforts towards nuclear disarmament.

(3) Cross-Regional Group: Non-Proliferation and Disarmament Initiative (NPDI)

In the TPNW negotiation process, the movements of nuclear umbrella states attracted a great deal of media attention, particularly towards the stances of states and regional groups (cross-regional groups) that have been strongly involved in nuclear disarmament. As one of these groups, the NPDI featured in this section has membership across various regions, from nuclear umbrella states and other non-nuclear weapon states such as Japan, Australia, Canada, Chile, Germany, Mexico, the Netherlands, Nigeria, the Philippines, Poland, Turkey, and the UAE, etc. Below is an overview of the stances the NPDI has expressed following the TPNW negotiations. First, the NPDI Joint Statement, issued to the 2017 First Session of the NPT Preparatory Committee,[60] mentioned

---

58 "United Nations Conference to negotiate a legally-binding instrument to prohibit nuclear weapons, leading towards their total elimination agenda item 8 (b) Statement by The Netherlands," United Nations PaperSmart, http://statements.unmeetings.org/media2/14683480/netherlands.pdf.

59 Lowana Veal, "Iceland, Norway Debate UN Nuclear Weapons Ban Treaty," *IDN-INPS*, August 23, 2017, https://www.indepthnews.net/index.php/armaments/nuclear-weapons/1321-iceland-norway-debate-un-nuclear-weapons-ban-treaty.

60 "Non-Proliferation and Disarmament Initiative (NPDI) Joint Statement to the first session of the NPT PrepCom, Vienna, May 2-12, 2017," Ministry of Foreign Affairs of Japan, July 30, 2018, http://www.mofa.go.jp/mofaj/files/000256421.pdf.

the TPNW negotiations at the beginning, stating that "The NPDI acknowledges that differences exist with regard to the ongoing negotiations of a legally binding instrument to prohibit nuclear weapons. Indeed, those differences are also reflected within the NPDI membership. They will not, however, affect our undertaking to continue working towards the implementation of the 2010 NPT Action plan. The NPDI remains absolutely united in our commitment to the NPT and trusts that these negotiations do not negatively impact the current NPT Review Cycle."

The NPDI held a Foreign Ministerial Meeting in New York in September 2017 for the first time in three years and issued a Joint Statement.[61] The Joint Statement (*refer to the 3rd revision, from September 17, 2017) did not directly refer to the TPNW. On the other hand, wording for the 2020 NPT Review Conference was inserted, to "assess the current challenges to nuclear disarmament and the non-proliferation of nuclear weapons and to reaffirm the critical importance of concerted action to work towards our shared goal of a world free of nuclear weapons."[62] Also, in recognition that "The current geopolitical situation underlines the need to strengthen and uphold the NPT," the NPDI will pursue the three pillars of peaceful use, non-proliferation, and nuclear disarmament for a successful 2020 NPT Review Conference. At that time, specific references began with criticism for North Korea's nuclear weapons development and ballistic missile test launches, but there were also mentions for the implementation of the Joint Comprehensive Plan of Action (JCPOA) for Iran, the pursuit of transparency, the International Partnership for Nuclear Disarmament Verification (IPNDV), hastening the entry into force of the CTBT, the early commencement of the FMCT negotiations, and recalling the proven effectiveness of nuclear-free zones.[63] In particular, the NPDI touches on high-level political leadership and unwavering involvement in the NPT while actively pursuing specific results for nuclear disarmament, stressing that they are an essential foundation for a substantial reduction in nuclear weapons around the world and for concrete progress towards the complete elimination of nuclear weapons.[64]

From these statements, the NPDI, which is composed of nuclear umbrella states and other non-nuclear weapon states, can be regarded as taking a convention NPT-oriented stance (step-by-step approach).

3. Arguments and Issues to be Considered around the TPNW

(1) Various Policy Stances in Support for the TPNW as Seen with Signatories and Ratified Countries

The TPNW was adopted after several twists and turns, but it is a very interesting point that there are subtle differences in the level of support between the result of the vote on the treaty, held at the UN General Assembly on July 7, 2017, and the actual situation of ratifications to date. First of all, as was mentioned earlier, the results had 122 in favor of the treaty, 1 against, and

---

61 "Non-Proliferation and Disarmament Initiative 9th Ministerial Meeting (Rev.3 as of 19 September 2017), New York City," Government of the Netherlands, September 21, 2017, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/diplomatieke-verklaringen/2017/09/21/non-proliferation-and-disarmament-initiative/NPDI+Ministerial+statement+Rev+III+170913.pdf.

62 Ibid.

63 Ibid.

64 Ibid.

1 abstention.[65] On the other hand, as of September 20, 2017, when the treaty was released for signing, 50 countries became signatories, and only three countries ratified the treaty (Guyana, Vatican, Thailand).[66] Ratification or accession from 50 countries is required for the treaty to enter into force, but Thomas Hajnoczi, Ambassador of Austria to the United Nations in Geneva, who led the TPNW negotiations, indicated that it would take two to two and a half years from adoption of the Treaty to its entry into force.[67]

As of the end of June 2019, when approximately 24 months have passed since the treaty was released for signing, the TPNW's latest signatory and ratification status, as announced by ICAN, is that 70 signatory countries and 23 countries have ratified it.[68] The names of the signatory countries (with signing date in parentheses) and ratifying countries (with ratification date in parentheses) are shown below.

> Signatory Countries: Algeria (September 20, 2017), Angola (September 27, 2018), Antigua and Barbuda (September 26, 2018), Austria (September 20, 2017), Bangladesh (September 20, 2017) Benin (September 26, 2018), Bolivia (April 16, 2018), Brazil (September 20, 2017), Brunei (September 26, 2018), Cabo Verde (September 20, 2017), Cambodia (January 9, 2019), Central African Republic (September 20, 2017), Chile (September 20, 2017), Colombia (August 3, 2018), Comoros (September 20, 2017), Congo (September 20, 2017), Costa Rica (September 20, 2017), Côte d'Ivoire (September 20, 2017), Cuba (September 20, 2017), Democratic Republic of the Congo (September 20, 2017) Dominican Republic (June 7, 2017), Ecuador (September 20, 2017), El Salvador (September 20, 2017), Fiji (September 20, 2017), Gambia (September 20, 2017), Ghana (September 20, 2017), Guatemala (September 20, 2017), Guinea Bissau (September 26, 2018), Guyana (September 20, 2017), Vatican (September 20, 2017), Honduras (September 20, 2017) ,Indonesia (September 20, 2017), Ireland (September 20, 2017), Jamaica (December 8, 2017), Kazakhstan (March 2, 2018), Kiribati (September 20, 2017), Laos (September 21, 2017), Libya (September 20, 2017), Liechtenstein (September 20, 2017), Madagascar (September 20, 2017), Malawi (September 20, 2017), Malaysia (September 20, 2017), Mexico (September 20, 2017), Myanmar (September 26, 2018), Namibia (December 8, 2017), Nepal (September 20, 2017), New Zealand (September 20, 2017), Nicaragua (September 22, 2017), Nigeria (September 20, 2017), Palau (September 20, 2017), Palestine (September 20, 2017), Panama (September 20, 2017) Paraguay (September 20, 2017), Peru (September 20, 2017), Philippines (September 20, 2017), Saint Lucia (September 27, 2018), Saint Vincent and the Grenadines (December

---

65 "General Assembly - other United Nations conference to negotiate a legally-binding instrument to prohibit nuclear weapons: Second session, Vote Name: Item 9, A/CONF.229/2017/L.3/Rev.1, Draft Treaty on the Prohibition of Nuclear Weapons," United Nations Office for Disarmament Affairs, July 30, 2018, https://s3.amazonaws.com/unoda-web/wp-content/uploads/2017/07/A.Conf_.229.2017.L.3.Rev_.1.pdf.

66 "List of Countries which Signed Treaty on the Prohibition of Nuclear Weapon on Opening Day," United Nations Office for Disarmament Affairs, September 20, 2017, https://www.un.org/disarmament/list-of-countries-which-signed-tpnw-on-opening-day-20-september-2017/.

67 *Tokyo Shimbun*, November 27, 2017.

68 "Signature/ratification status of the Treaty on the Prohibition of Nuclear Weapons," International Campaign to Abolish Nuclear Weapons, June 20, 2019, http://www.icanw.org/status-of-the-treaty-on-the-prohibition-of-nuclear-weapons/.

8, 2017), Samoa (September 20, 2017), San Marino (September 20, 2017), Sao Tome and Principe (September 20, 2017), Seychelles (September 26, 2018), South Africa (September 20, 2017), Thailand (September 20, 2017), East Timor Democratic Republic (September 26, 2018), Togo (September 20, 2017), Tuvalu (September 20, 2017), Uruguay (September 20, 2017), Vanuatu (September 20, 2017), Venezuela (September 20, 2017), Vietnam (September 22, 2017)

Ratifying Countries: Austria (May 8, 2018), Cook Islands (September 4, 2018), Costa Rica (July 5, 2018), Cuba (September 30, 2017), El Salvador (January 30, 2019), Gambia (September 26, 2018), Guyana (September 20, 2017), Vatican (September 20, 2017), Mexico (January 16, 2018), New Zealand (July 31, 2018), Nicaragua (July 19, 2018), Palau (May 3, 2018), Palestine (March 22, 2018), Panama (April 11, 2019), Saint Lucia (January 23, 2019), Samoa (September 26, 2018), San Marino (September 26, 2018), South Africa (February 22, 2019), Thailand (September 20, 2017), Uruguay (July 25, 2018), Vanuatu (September 26, 2018), Venezuela (March 27, 2018), Vietnam (May 17, 2018)

In light of the number of votes at the United Nations on July 7, 2017 in favor of the TPNW's adoption, it must be noted that the signature and ratification process has made a slow start. Additionally, most of the countries listed here are not directly exposed to nuclear or security threats, as has been pointed out by the nuclear weapon and nuclear umbrella states. In this context, it is likely that close attention will be paid to discussions on signing and ratifying the treaty occurring among other remaining countries that have agreed to the adoption of the TPNW in July 2017.

(2) Debate over the Evaluation of the TPNW and its Relationship with the NPT

The TPNW negotiations have attracted worldwide attention, and, in fact, various debates have arisen, including on the demise of nuclear weapon states and the nuclear umbrella, and issues of the treaty's significance and entry into force. For example, former US Secretary of Defense William J. Perry, who has disseminated significant amounts of information about a world without nuclear weapons, said that the TPNW's adoption by the United Nations was a strong moral demand to nuclear weapon states. It is the voices of 120 countries that feel their survival is in danger because of nuclear weapons, and, while there is no single solution to remove the threat of nuclear weapons, he pointed out that it is important to avoid the introduction of new nuclear weapons, which are an unnecessary risk factor that can lead to destabilization, and that further efforts beyond the TPNW will be required to reduce this threat, such as the early entry into force of the CTBT, the new START extension agreement, and the continuation of key issues at the nuclear security summit.[69] Ambassador Thomas Hajnoczi evaluated the importance of the TPNW as norm-making to aim for a world without nuclear weapons, which has not been possible even 47 years after the NPT came into effect. Increasing momentum for nuclear disarmament can be expected via the TPNW by first creating a norm and then aiming to abolish nuclear weapons.[70]

---

69 William Perry, "UN Adopts New Treaty on the Prohibition of Nuclear Weapons," wjperryproject, July 7, 2017, http://www.wjperryproject.org/notes-from-the-brink/un-adopts-new-treaty-on-the-prohibition-of-nuclear-weapons.

70 *Mainichi Shimbun*, July 12, 2017.

Discussions on the relationship between the NPT and the TPNW have been deepening in recent years, and there has been attention paid, in particular, to voices concerned about the division of nuclear disarmament among the NPT member states. As an example of this, non-nuclear weapon states will be divided into TPNW and NPT proponents, and there is a risk that the NPT will be hollowed out in the future. As for the verification measures, the TPNW has been criticized for lacking substance because it does not include any additional requirements for the existing NPT safeguards.[71] On the other hand, the criticism of making an additional new treaty, despite the existence of the NPT, does not make sense in response to such comments; the TPNW's Preamble and Article 18 do not impair obligations to other treaties, and Article 3 clearly states the maintenance of obligations related to NPT safeguards. In addition, none of the states supporting the TPNW are suggesting that the NPT is unnecessary, and the view that the TPNW is nullifying the NPT regime is wrong. The NPT's own problems have led to the treaty's weakening in recent years, and nuclear disarmament can be pursued by following both means, rather than by choosing between joining the TPNW or taking the building blocks approach involving the promotion of the CTBT's early entry into force, early commencement of the FMCT negotiations, and measures for greater nuclear transparency.[72] Meanwhile, although various dissatisfactions with the NPT have become a driving force towards the adoption of the TPNW, it has also been pointed out that the NPT has established a process for nuclear disarmament but is not aiming for nuclear abolition.[73] As shown below, the NPT has an obligation, in Article VI, to negotiate nuclear disarmament, but this is only a commitment to negotiate. The treaty itself does not stipulate a process that leads to the elimination of nuclear weapons aside from the resolutions and action plans adopted by the NPT Review Conferences.

> NPT Article VI: *Each of the Parties to the Treaty undertakes to pursue negotiations in good faith on effective measures relating to cessation of the nuclear arms race at an early date and to nuclear disarmament, and on a treaty on general and complete disarmament under strict and effective international control.*

In fact, there were a wide range of issues in the TPNW negotiations, but, as has been mentioned in this paper, the most notable focus was the relationship between the TPNW and the NPT. In the initial negotiations for the draft treaty, some concerned states tried to specify that the provision of TPNW would not affect the rights and obligations of NPT signatories, but this text was removed due to pushback from Egypt and South Africa, and the Netherlands also insisted that text be inserted stating that the provisions of the NPT will take precedence when disputes arise between the TPNW and the NPT in the future.[74] As a result, the NPT was not mentioned during

---

71 *Mainichi Shimbun*, July 12, 2017.

72 "Kakuheiki Kinshi Jyoyaku -- Hihan ni Kotaeru" [The Nuclear Weapons Ban Treaty -- Answering Criticism], Akira Kawasaki's Blog, July 12, 2017, http://kawasakiakira.at.webry.info/201707/article_1.html. Mr. Akira Kawasaki (Peaceboat co-Chairman) is a member of the International Steering Committee of ICAN, which won the Nobel peace Prize.

73 Heigo Sato, *"Kaku naki Seikai o Nozomunara, Nihon ha Kakuheiki Kinshi Jyoyaku ni Sanka shite ha ikenai,"* [If you Want a World Without Nuclear Weapons, Japan should not Participate in the Nuclear Weapons Convention], Gendai Business, August 21, 2017, http://gendai.ismedia.jp/articles/-/52629.

74 *Yomiuri Shimbun*, July 6, 2017.

the drafting, and the wording of the TPNW was revised to "The implementation of this Treaty shall not prejudice obligations undertaken by States Parties with regard to existing international agreements, to which they are party, where those obligations are consistent with the Treaty."[75]

(3) Differences in Stance among Countries Promoting the TPNW Negotiations

In addition, differences in each country's stance during the negotiation process are not only limited to the relationship between the TPNW and the NPT. From the perspective of civil society, which was deeply involved in the negotiation process, the drafting of the treaty proceeded with a mix of so-called idealism and realism, and it was made clear that the drafting came to fruition in a surprisingly short time under the direction of Ambassador Whyte Gómez, who was Chairman of the negotiations.[76] Of particular note is that it was pointed out that some proposals were made to water down the treaty.[77] With regard to the different stances of the TPNW negotiation participants, the Bulletin of the Atomic Scientists issued an analysis made by Oliver Meier, Sira Cordes and Elisabeth Suh, titled "What participants in a nuclear weapons ban treaty (do not) want." (*Please refer to table 1 "Idealistic/Realistic Policy Stances of countries participating in TPNW negotiations" summarized by the author based on the abovementioned analysis.)[78]

The most striking aspect of this table is the existence of countries that are explicitly opposed to including two important issues in the TPNW draft: i. the threat of nuclear weapon use and ii. obligations for nuclear weapon states (a timeline for abolition and validated disposal). As described in "What participants in a nuclear weapons ban treaty (do not) want," Austria and Mexico were opposed to the former, and Ireland, Malaysia, and New Zealand were opposed to the latter. These countries were regarded as key players in the treaty negotiations that had a corresponding presence, but careful attention should be paid to the background and intent of excluding issues, as i. is directly related to the logic of nuclear deterrence, and ii. leads to the establishment of conditions that encourage participation from nuclear weapon states. Furthermore, looking at the items in the table, there are some issues that have not yet been clearly stated, even in countries that have already ratified the treaty as of the time of this article's writing. These may be points to consider when looking at the intentions of TPNW promoting countries and the history of the treaty's negotiations (*However, it should also be noted that the table may not comprehensively record each country's statements during the TPNW negotiations).

Conclusion

50 years have passed since the NPT came into effect. Japan ratified the NPT in 1976, six years after it came into force, but it was not ratified until 1992 by either France or China, which are key nuclear weapon states as defined by the treaty. The TPNW received nearly two-thirds of the support of all United Nations member states and was negotiated and adopted in a very short period

---

75 Ibid.

76 Gaukhar Mukhatzhanova, "The Nuclear Weapons Prohibition Treaty: Negotiations and Beyond," *Arms Control Today*, September 2017, pp. 12-19.

77 Ibid. In addition, Iran, Egypt, Brazil, and Argentina are listed as countries that have made proposals and discussions that can be considered modifications (*Details of the discussions were not disclosed).

78 Oliver Meier, Sira Cordes and Elisabeth Suh, "What Participants in a Nuclear Weapons Ban Treaty (do not) Want," The Bulletin of the Atomic Scientists, June 9, 2017, https://thebulletin.org/what-participants-nuclear-weapons-ban-treaty-do-not-want10829.

of time. Just as a matter of possibility that is worth noting, the history of past nuclear disarmament and non-proliferation efforts suggests that, even though the pace of signing and ratification is off to a slow start, it should not be ruled out that the number of ratifying countries will increase over the medium- to long-term and that the treaty's impact will increase.

If disarmament is defined as an effort to abolish specific weapons, then the TPNW is the first disarmament treaty covering all nuclear weapons, and participation in the TPNW is a signal that indicates the intention of making nuclear weapons relics of the past. Although this is similar to the work that was previously realized in the form of the CWC for chemical weapons, chemical weapons and nuclear weapons have different strategic values in the first place, even though they are both categorized as weapons of mass destruction, and there is a corresponding large difference between the "haves" and the "have-nots." With many countries still having security architecture that depends on nuclear deterrence, it is natural that various debates have arisen regarding the pros and cons of negotiating and participating the TPNW. With that being said, the countries promoting TPNW and civil society have tried to generate momentum for nuclear disarmament, which has stagnated under the current NPT regime, and it is also true that they have reinvigorated the international debate on nuclear disarmament. Therefore, there is, to some extent, value in such an initiative, in and of itself. Nevertheless, there are divergent opinions on a number issues, even among the countries that participated in the TPNW negotiations. The treaty itself came together in a very short period of time, and it seems that there is still room for argument regarding the detailed wording.

It is also necessary to continue to pay attention to the fact that the adoption of the TPNW has resulted in the division of the international community. This is especially true among non-nuclear weapon states, with a division between the nuclear umbrella states and other countries. Some political gaps may still emerge for the next 2020 NPT Review Conference. The 2015 NPT Review Conference failed to adopt a final document. The adoption of the final document of the 2020 NPT review conference may also create an undesired conflict between countries promoting the TPNW, who are seeking to refer to the TPNW, and countries that are opposed to the treaty. Much expectation is therefore being placed on diplomatic efforts to mediate between the relevant countries. In fact, there were some instances of TPNW references in various country statements at the second session of the NPT Preparatory Committee held in Geneva in 2018. As an example, South Africa states that the TPNW is a positive step towards the abolition of nuclear weapons and welcomes and supports this as contributing to the implementation of NPT Article VI.[79] Additionally, New Zealand, from the standpoint of the New Agenda Coalition (NAC), expressed concern over language in its Preparatory Committee Chair's summary that referred to the TPNW. Specifically, the Chair's summary described the intention of multiple parties to oppose the TPNW (Chair's summary, paragraph 41), only mentioning the ratification process and the treaty's status (paragraph 40), and without mentioning the countries that support the TPNW.[80] Similar to the New Zealand issue, Ireland, after pointing out that many countries welcomed the TPNW's adoption,

---

[79] "Statement by South Africa on the Draft Chair's Summary at the NPT Second Precpom," United Nations PaperSmart, May 4, 2018, http://statements.unmeetings.org/media2/18559906/south-african-npt-statement-on-the-chairs-summary.pdf.

[80] "New Agenda Coalition comments on Draft Chair's factual summary (NPT/CONF.2020/PC.II/CRP.3) at the 2nd Preparatory Committee of 2020 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons (Working Paper)," May 4, 2018, http://statements.unmeetings.org/media2/18559870/new-zealand-nac-wp-on-4-may-comments-on-chairs-summary.pdf.

conveyed regret that the Chair's summary did not mention the session's discussions in an accurate and balanced manner.[81]

At the 2019 third session of the NPT Preparatory Committee, Brazil, Costa Rica, Ireland, Indonesia, Mexico, New Zealand, Nigeria, South Africa, Australia, and other countries that led the TPNW negotiations issued resolution 73/48, the Joint Statement, which once again emphasized that the TPNW is fully compatible with and complementary to the NPT.[82]

As discussed in this paper, the countries supporting the TPNW are by no means seeking the collapse of the NPT regime. At the 2020 NPT Review Conference, efforts must be made to avoid a failure to adopt a final document and to ensure constructive consensus-building. Conversely, countries that did not participate in the TPNW negotiations must also demonstrate the appropriateness of the "step-by-step" method within the framework of NPT regime. Needless to say, there are many obstacles to this endeavor. However, as discussed in this paper, it is important to strive to find answers to the following issues surrounding the TPNW: i. The issue of the involvement of nuclear weapon states, ii. Concerns about the division of the international community, iii. Nuclear deterrence considerations, iv. Awareness of an increasingly severe international security environment, v. Warning about the risk of weakening the NPT system (concerns about compatibility with existing treaties), and vi. Inadequacies in verification mechanisms. To that end, it will become even more important for the international community to consider the essential issues surrounding nuclear deterrence and nuclear disarmament.

In connection with these issues, worthy of note are the deliberations of the Group of Eminent Persons Substantive Advancement of Nuclear Disarmament, an initiative led by the Japanese government and launched in 2017, involving experts and specialists from Japan and from abroad. The Group held multiple discussions, including on the role of nuclear weapons, the purpose of nuclear deterrence, and an assessment of the minimization point, and in March 2018 it submitted its recommendations, entitled "Building Bridges to Effective Nuclear Disarmament - Recommendations for the 2020 Review Process for the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) -, to Foreign Minister Kono."[83] This proposal points out a number of bridging issues related to the above items i.-vi. so as to avoid the stagnation of nuclear disarmament. In fact, at the 2nd NPT Preparatory Committee meeting held in April 2018, Minister Kono's statement at the General Debate included a proposal from the Group of Eminent Persons.[84] Additionally, continued efforts are being made to encourage in-depth discussions among NPT member states, as advocated in the Group of Eminent Persons' "Kyoto Appeals" in March 2019 and the proposals

---

81 "Statement by Ambassador Michael Gaffey, Permanent Representative of Ireland to the United Nations and other International Organizations in Geneva At the 2018 Preparatory Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) Geneva," United Nations PaperSmart, May 4, 2018, http://statements.unmeetings.org/media2/18559873/ireland-closing-remarks.pdf.

82 "Joint Statement on the Treaty on the Prohibition of Nuclear Weapons (TPNW)," May 2, 2019, http://statements.unmeetings.org/media2/21491996/austria-behalf-1.pdf.

83 "Building Bridges to Effective Nuclear Disarmament," Ministry of Foreign Affairs, March 29, 2018, https://www.mofa.go.jp/files/000349264.pdf.

84 "Foreign Minister Taro Kono delivered a statement at the General Debate of the First Session of the Preparatory Committee of the 2020 NPT Review Conference," Ministry of Foreign Affairs, April 24, 2018, https://www.mofa.go.jp/dns/ac_d/page4e_000804.html.

for the third session of the NPT Preparatory Committee in April 2019.[85]

Nevertheless, it is necessary to monitor the results and future developments of discussions about nuclear weapons that are occurring at the parliamentary level in some countries, on points such as not participating in nuclear disarmament treaties that do not meet the country's security requirements and conditions, or, alternatively, considering participation as long as the country's security requirements and conditions are met. There are also a number of movements from among the nuclear weapon states, seeking to achieve a breakthrough in the situation. Notable examples include the announcement by the United States of the "Creating an Environment for Nuclear Disarmament (CEND) Initiative" and the establishment of a "Creating an Environment Working Group (CEWG)."[86] What kinds of policy approaches these lead to will be a matter of great interest.[87]

In any case, it is true that the TPNW, whether one likes it or not, was adopted by the United Nations General Assembly. If support for the treaty grows in the future, then it is indeed possible that the number of ratifying countries may increase as well. To add one point in that regard, the TPNW has an amendment clause (Article 10) that makes it possible to submit a treaty amendment even after the treaty enters into force. In other words, there is still an opportunity to review the present concerns about the TPNW in the future after the ratification or acceptance of the treaty. As a conclusion to the above consideration, a constructive bridge between nuclear weapon states, nuclear umbrella states, and non-nuclear weapon states that support the NPT and promote the TPNW will need to be realized. It is strongly hoped that efforts toward a "world without nuclear weapons" will continue in a sustainable and positive manner.

---

85 "Kakugunshuku no Jisshitsu tekina Shinten no tame Kenjin Kaigi, Kyoto Appeal (Gaiyo)" [Group of Eminent Persons for Substantive Advancement of Nuclear Disarmament], Ministry of Foreign Affairs, April 2019, https://www.mofa.go.jp/mofaj/files/000469288.pdf.

86 Remarks by Dr. Christopher Ashley Ford Assistant Secretary, Bureau of International Security and Nonproliferation, Disarmament Side Event, Third Preparatory Committee for the 2020 NPT Review Conference, United Nations, New York, April 30, 2019, https://geneva.usmission.gov/2019/05/01/arms-control-and-international-security-lessons-from-disarmament-history-for-the-cend-initiative/.

87 Paul Meyer, "Creating an Environment for Nuclear Disarmament: Striding Forward or Stepping Back?" *Arms Control Today*, April 2019, https://www.armscontrol.org/act/2019-04/features/creating-environment-nuclear-disarmament-striding-forward-stepping-back.

Table 1. Idealisitic/Realistic Policy Stances of countries participating in TPNW negotiations

	Should be Prohibited (Stances Based on Idealism)	Shoud be Excluded (Stances Based on Realistic Considerations)	Unknown or Did Not Express Intention
Possession, Use, Acquisition, Manufacturing, or Deployment of Nuclear Weapons	Algeria, Austria, Brazil, Chile, Cambodia, Costa Rica, Cuba, Ecuador, Egypt, Fiji, Ghana, Indonesia, Iran, Ireland, Jamaica, Malaysia, Mexico, Nepal, New Zealand, Nigeria, Peru, the Philippines		Argentina, Bangladesh, Cambodia, Dominican Republic, Ethiopia, Equatorial Guinea, Guatemala, the Vatican, Honduras, Japan, Kazakhstan, Kuwait, Laos, Libya, Liechtenstein, Marshall Islands, Mongolia, Morocco, Myanmar, the Netherlands, Papau New Guinea, Palestine, Saudia Arabia
Transfer of Nuclear Weapons	Algeria, Austria, Brazil, Chile, Cambodia, Costa Rica, Cuba, Ecuador, Fiji, Indonesia, Iran, Ireland, Jamaica, Mexico, Nepal, New Zealand, Nigeria, the Philippines		Argentina, Bangladesh, Cambodia, Dominican Republic, Egypt, Ethiopia, Equatorial Guinea, Ghana, Guatemala, the Vatican, Honduras, Kazakhstan, Kuwait, Laos, Libya, Liechtenstein, Malaysia, Marshall Islands, Mongolia, Morocco, Myanmar, the Netherlands, Papau New Guinea, Palestine, Peru, Saudia Arabia
Stockpiling of Nuclear Weapons	Algeria, Austria, Brazil, Chile, Cambodia, Costa Rica, Cuba, Ecuador, Fiji, Ghana, Indonesia, Ireland, Jamaica, Mexico, Nepal, New Zealand, Nigeria, the Philippines		Argentina, Bangladesh, Cambodia, Dominican Republic, Egypt, Ethiopia, Equatorial Guinea, Guatemala, the Vatican, Honduras, Iran, Kazakhstan, Kuwait, Laos, Libya, Liechtenstein, Malaysia, Marshall Islands, Mongolia, Morocco, Myanmar, the Netherlands, Papau New Guinea, Palestine, Peru, Saudia Arabia
Threatening the Use of Nuclear Weapons	Chili, Colombia, Costa Rica, Mexico, Ecuador, Fiji, Indonesia, Iran, Jamaica, Nepal	Australia, Mexico	Algeria, Argentina, Bangladesh, Brazil, Cambodia, Dominican Republic, Egypt, Ethiopia, Equatorial Guinea, Ghana, Guatemala, the Vatican, Honduras, Ireland, Japan, Kazakhstan, Kuwait, Laos, Libya, Liechtenstein, Malaysia, Marshall Islands, Mongolia, Morocco, Myanmar, the Netherlands, New Zealand, Nigeria
Participation in Nuclear Planning/ Nuclear Sharing	Algeria, Brazil, Cambodia, Mexico		Argentina, Austria, Bangladesh, Cambodia, Chili, Costa Rica, Cuba, Dominican Republic, Equatorial, Egypt, Ethiopia, Equatorial Guinea, Fiji, Ghana, Guatemala, the Vatican, Honduras, Indonesia, Iran, Ireland, Jamaica, Japan, Kazakhstan, Kuwait, Laos, Libya, Liechtenstein, Malaysia, Marshall Islands, Mongolia, Morocco, Myanmar, Nepal, the Netherlands, New Zealand, Nigeria
Obligations for Nuclear Weapons States (Timeframe to Abolition/Verified Disposal)	Argentina, Chili, Colombia, Costa Rica, Cuba, Ecuador, Egypt, Fiji, Indonesia, Iran, Jamaica, Mexico, Nepal	Ireland, Malaysia, New Zealand	Argentina, Austria, Bangladesh, Brazil, Cambodia, Dominican Republic, Ethiopia, Equatorial Guinea, Ghana, Guatemala, the Vatican, Honduras, Japan, Kazakhstan, Kuwait, Laos, Libya, Liechtenstein, Marshall Islands, Mongolia, Morocco, Myanmar, the Netherlands

Source: Prepared by the author based on the following paper. (Oliver Meier, Sira Cordes and Elisabeth Suh, “What participants in a nuclear weapons ban treaty (do not) want,” The Bulletin of the Atomic Scientists, June 9, 2017.)

The Rise of China and Strengthening of Security Cooperation Between Japan, the United States, and Australia: With a Focus on the 2000s*

SATAKE Tomohiko**

Abstract

This paper will analyze why and how US-Japan-Australia security cooperation developed in the 2000s, mainly from the allied perspective (Japan and Australia). Existing literature notes that the United States aimed to form an alliance opposing China from the start of the 2000s by strengthening relationships with its allies. In contrast, Japan and Australia's perception of China was different to that of the United States. This especially applied to Australia, geographically distant from China, which prioritized strengthening its relations with China through diplomacy and trade over direct antagonism. Regardless of this, both Japan and Australia worked to strengthen security cooperation between Japan, the United States, and Australia based on a strategy of "supplementing" the United States' regional and global role by furthering cooperation between its allies in peacekeeping operations and non-traditional areas of security. The strengthening of security cooperation between Japan, the United States, and Australia during the 2000s developed in order to maintain and enhance the United States' presence based on the "hub and spokes" alliance system, rather than to directly oppose China.

Introduction

After the Cold War, a bilateral alliance system centered around the United States (the so-called "hub and spokes" system) continued in the Asia Pacific Region. At the same time, there was increased cooperation between allied countries, including the United States. A typical example of this is the security cooperation between Japan, the United States, and Australia. Both Japan and Australia had strengthened bilateral defense exchanges immediately following the end of the Cold War. This cooperation rapidly grew when Trilateral Strategic Dialogue (TSD) between the three countries was established at the start of the 2000s. The first ministerial-level TSD took place in March 2006; in March the following year the Japan-Australia Joint Declaration on Security Cooperation was announced, and in June the two countries started the 2+2 Foreign and Defense Ministerial Consultations. After this, cooperation between Japan, the United States, and Australia continued to grow, and in recent years has extended to traditional security areas such as

* Originally published in Japanese in *Boei Kenkyusho Kiyo* [NIDS Security Studies], vol.21, no.2, March 2019. Some parts have been updated.

** Policy Simulation Office Senior Research Fellow

antisubmarine warfare and amphibious operations in addition to peacekeeping operations (PKO) and non-traditional security areas.[1]

Existing literature points out that in the context of the changing American alliance system after the Cold War, the United States shifted its strategy to deal with China as China's influence rapidly increased in the region. For example, Nina Silove argues that in the first half of the 2000s the George W. Bush administration strengthened and modernized the capacity of its regional allies, including Japan and Australia, to prevent the hegemonic rise of China in the region by forming a "federated network" through stronger relationships between its allies.[2] According to Silove, strengthening security cooperation between the United States' allies and partner countries from the 2000s onwards, including the security cooperation between Japan, the United States, and Australia, was nothing less than a deliberate construction created through the United States' "external balancing" vis-à-vis China, rather than something that developed naturally.[3]

However, Silove's study is unclear as to why allied countries such as Japan and Australia accepted this strategic concept of the United States. As is discussed below, at the start of the 2000s, there were considerable differences in Japan, the United States, and Australia's perceptions of, and their relations with, China. Notably, due to Australia's geopolitical distance from China and the economic importance of its relationship with China, it kept a certain distance from the United States' competitive attitude towards China. There were even those among Japanese and American policy makers who expressed concerns about Australia's attitude towards China. Why, then, despite differences in their perception and policies vis-à-vis China, did Japan and Australia strengthen their bilateral, and, including the United States, trilateral security cooperation?

In relation to this point, Yusuke Ishihara notes the importance of the role that the United States has come to play in the relationship between Japan and Australia.[4] According to Ishihara, in the context of Australia aiming to develop its relationship with Japan in particular, there was a "longstanding insight [on the Australian side] concerning the importance of the United States' role in the Asia Pacific, and the role of the Japan-America alliance in this context." He writes that even after 2007, when the Japan-Australia Joint Declaration on Security Cooperation was announced, the increased bilateral relationship between Japan and Australia has developed with their relationships with the United States as the base.[5] Although this is an incredibly important point, the main thrust of Ishihara's analysis fundamentally concerns the Japan-Australia bilateral relationship, and is not entirely clear on what logic led their relationships with the United States to reinforce bilateral or US-Japan-Australia trilateral security cooperation.

Thus, the aim of this paper is to clarify the circumstances in which US-Japan-Australia

---

1 Andrew Shearer, *Australia-Japan-U.S. Maritime Cooperation: Creating Federated Capabilities for the Asia Pacific* (Washington DC: Center for Strategy and International Studies, 2015).

2 Nina Silove, "The Pivot before the Pivot: U.S. Strategy to Preserve the Power Balance in Asia", *International Security*, Vol. 40, No. 4, pp. 45-88.

3 Ibid., p. 76.

4 Yusuke Ishihara, "Reisengo Nichigo Kankei no Hatten to Chugoku 'Chyaina Gyappu' to 'Chyaina Consensasu' no Aida de [The Development of Japan-Australia Relations after the Cold War and China: Between the 'China Gap' and 'China Consensus']", Yoshihide Soeya (ed.), *Chitsujo Hendo to Nihon Gaiko: Kakudai to Shushuku* [The Changing Order and Japanese Diplomacy: 70 years of Expansion and Contraction] (Tokyo: Keio University Press, 2016), p. 220.

5 Ibid.

security cooperation developed in the 2000s, based on the points made by Ishihara above, mainly in the context of Japanese and Australian relations with the United States. The first chapter below will show how Japan and Australia's perceptions of China differed to those of the United States from the second half of the 1990s to the beginning of the 2000s. In order to maintain American engagement with the region, however, they voluntarily and actively participated in establishing the TSD.

Next, Chapter 2 will examine the process that deepened practical relationships in the field of non-traditional security, triggered by the 9/11 terrorist attacks in the United States, with a focus on Japan, the United States, and Australia; it will clarify the existence of strategies common to both Japan and Australia that were behind this process, "supplementing" the United States' regional and global role. Chapter 3 will discuss the idea that although Japan, the United States, and Australia were strengthening and institutionalizing security cooperation in the context of the rise of China, the main focus was not China—the target was actually to maintain and strengthen the United States' presence in the region. In addition, although the main cause of the increased security cooperation between Japan, the United States, and Australia in the 2000s was the rise of China, this paper will conclude with the suggestion that it developed in the context of maintaining and strengthening the United States' presence based on the "hub and spokes" system, rather than with a direct focus on China.

1. The Rise of China and the Beginning of the TSD

(1) Background

After the Cold War, especially from the mid-1990s onwards, Japan, the United States, and Australia each strengthened their bilateral security relationships. In Australia, there were politicians and professionals who proposed the possibility of trilateral security cooperation. In fact, it is said that the idea of trilateral cooperation between Japan, the United States, and Australia had "obtained a foothold of sorts in Australia's strategic policy agenda" by the mid-1990s.[6] However, the Japanese side was wary that Japan and Australia would create "Unnecessary doubts over whether it was creating a new relationship of military cooperation centered on its alliance with the United States" among Japan's neighbors.[7] Through the '90s, policy makers on the American side stressed the tradition of bilateral alliances, and did not show great interest in security cooperation with Japan and Australia.[8]

It was the establishment of the new Bush administration in the United States in January 2001 that changed the status quo. The Bush administration's foreign policies, especially the core of its Asia policy, involved an emphasis on "power" focused on military strength, and maintaining an American-led order backed by that power while sharing the burden with its regional democratic allies. The Bush administration considered China, rapidly gaining power in Asia, as a competitor rather than a strategic partner, and called for the unity of its democratic allies in the region,

---

6 Hugh White, "Trilateralism and Australia: Australia and the Trilateral Strategic Dialogue with America and Japan", in William T. Tow, Mark J. Thomson, Yoshinobu Yamamoto and Satu P. Limaye (eds.), *Asia-Pacific Security: US, Australia and Japan and the New Security Triangle* (London and New York: Routledge, 2007), p. 105.

7 Yukio Sato, "*Toi Kuni' kara 'paatonaa' e* [From a 'Far Away Country' to a 'Partner']", *Gaiko Forum* [Foreign Affairs Forum], August 1997, p. 43

8 White, "Trilateralism and Australia", p. 104.

including Japan and Australia, to oppose China's challenge[9]. According to Robert D. Blackwill, who served as a diplomatic advisor to President Bush, the construction of a "more interrelated system of alliances" would make it possible to curb the actions of a "hostile hegemonic power" in the region, and to "more evenly distribute the strategic burden in Asia."[10]

To the United States, Japan was its most important partner in accomplishing this regional strategy. As is well known, a US bipartisan report in 2000 welcomed Japan to expand its role in security, and become a more equal American allied partner. The report (the so-called "Armitage-Nye Report") was written by a researcher and a professional who later became a senior official in the Bush administration. The report also advocated revitalizing the United States-Japan alliance based on the model of the United States-Great Britain alliance[11]. Quite simply, the United States anticipated the rise of China in the future, and wished to maintain and strengthen the American-led regional order in a more effective manner by committing to maintaining its leadership role in the region while, at the same time, encouraging an expansion of its allies' capabilities, including Japan.

Meanwhile, Japan was gradually strengthening its guard against China, which had rapidly increased its defense expenditure from the 1990s onwards. From around the middle of this decade, Chinese armed forces increased their activity in the seas around Japan, deploying "research vessels" in the area around the Senkaku Islands and warships in Japan's Exclusive Economic Zone in the East China Sea, among other actions. Based on this, in 1995 there was a Japanese expert who predicted that the Chinese navy would "advance into the Sea of Japan in the not-too-distant future."[12] The Defense of Japan (annual white paper) had also included information about the increase in China's military spending, modernization of its armed forces, and increased maritime activity each year since 1996.[13] Defense of Japan 2001 included an account saying that "Careful consideration should be given as to whether" the aim of China's modernization of its military strength "is exceeding what is required for China's defense; it is necessary to pay attention to this tendency in the future."[14] The feelings of the Japanese people towards China also considerably worsened compared to those of the Cold War period due to China's repeated nuclear tests, the Taiwan Strait Crisis, the Chinese attitude towards historical issues, and other factors.[15]

However, whereas China's defense expenditure rapidly increased, Japan's defense spending remained almost the same. It is known from this that Japan did not think that the Chinese threat was all that urgent at the time. Rather, from 1994 Japan and China began holding defense exchanges and security dialogues, and in November 2000 they maintained a good relationship in terms of

---

9 Governor George W. Bush, "A Distinctly American Internationalism," Ronald Regan Presidential Library, Simi Valley, California, November 19, 1999, cited in Green 2017, p. 484.

10 Robert D. Blackwill, "An Action Agenda to Strengthen America's Alliances in the Asia-Pacific Region", in Blackwill and Paul Dibb (eds.), *America's Asian Alliances* (Cambridge, MA: MIT Press, 2000), p. 125.

11 The United States and Japan: Advancing Toward a Mature Partnership, INSS Special Report, October 11, 2000, pp. 3-4. http://www.dtic.mil/dtic/tr/fulltext/u2/a403599.pdf.

12 Hiramatsu, *Gunji Taikokukasuru Chugoku no kyoi* [The Thread of China as it Becomes a Great Military Power], (Tokyo: Jiji Press, 1995) p. 164.

13 Ministry of Defense, *Boei Hakusyo* [*Defense of Japan*].

14 Ministry of Defense, *Boei Hakusyo* (2001) p. 60.

15 Cabinet Office Public Relations Office, *Seron Chosa Zu 10 Chugoku ni Taisuru Shinkinkan* [Public Opinion Poll Figure 10 Feeling of Friendliness Towards China], https://survey.gov-online.go.jp/h25/h25-gaiko/zh/z10.html (Accessed 29 May 2018).

security as well as economics, including increasing defense exchanges between them and agreeing to quickly realizing mutual visits of military vessels. Even with the gradually increasing theory of a "Chinese threat" from the second half of the 1990s, centered in the United States, many Japanese experts were skeptical of such a theory.[16] There were even former senior officials of the Japan Defense Agency who objected to the Bush administration's hard line vis-à-vis China.[17]

There is no doubt that the rise of China posed a long-term strategic problem to the United States and its allies. However, based on official announcements, contemporary Chinese defense spending was barely one tenth that of the United States, and as long as Japan maintained a close allied relationship with the United States, it was possible to respond to China's maritime expansion. Above all, at the time the main military threat to Japan was not China but North Korea, which was proceeding with missile and nuclear development. Consequently, in the first half of the 2000s, when the Bush administration presented a plan to Japan that prioritized deterring China, involving the transformation of the United States military, Japanese policy makers could not hide their confusion.[18]

The Australian perception of China differed even more greatly to that of the United States, and also to that of Japan. At the time, Australia did not see the rise of China as even a potential threat to its own safety. For example, the Defence White Paper published in 2000 did not refer to the modernization of China's military strength or its activities. Although the white paper identified irregular warfare and non-traditional security threats, it estimated that the possibility of China being a direct threat to Australia in the near future was very low.[19] In fact, the white paper presented a policy of deepening and developing dialogues with China in relation to strategic issues, from the perspective that China, which was rapidly increasing its influence on regional security, would become an increasingly important strategic interlocutor to Australia.[20]

Notably, Prime Minister John Howard, a conservative who stressed economic relations with China, proactively developed diplomacy with China to improve the relationship between the two countries, which had worsened since the 1996 Taiwan Strait Crisis. As a result, Jiang Zemin visited Australia for the first time as President of China in September 1999, and agreed not only to strengthen economic ties, but also to hold annual meetings between both countries' leaders and foreign ministers. In the same year, eight Australian cabinet ministers, including the Minister for Foreign Affairs and the Minister for Defence, visited China, and senior government officials from both countries strengthened dialogues concerning diplomacy and security. Economically, trade with China grew rapidly through the '90s in both imports and exports, and in the first half of the

---

16 For example, see Satoshi Amako (ed.), *Chugoku wa Kyoi ka* [Is China a Threat?] (Tokyo: Keiso Shobo, 1997). For the differences in Japan, the United States, and Australia's perception of China (as a threat) in the '90s, detail is available in Hideo Sato, "Japan's China Perceptions and its Policies in the Alliance with the United States", September 1998, available at file:///Users/sataketomohiko/Library/Mobile%20Documents/com~apple~CloudDocs/Sato_final_PM.pdf.

17 For example, Masahiro Akiyama, *Nichibei no Senryakutaiwa ga Hajimatta: Anpo Saitengi no Butai-ura* [Japanese-American Strategic Dialogues have Started: Behind the Scenes of Redefining Security] (Tokyo: Akishobo, 2002), p. 298.

18 Hiroyuki Akita, *Anryu: Beichunichi Gaiko San-kokushi* [Undercurrents: Diplomacy of The Three Kingdoms of the United States, China, and Japan] (Tokyo: Nikkei Inc., 2008), p. 53.

19 Department of Defence, *Defence 2000: Our Future Defence Force* (2000 Defence White Paper) (Canberra: Commonwealth of Australia, 2000), pp. 23-24.

20 Ibid., p. 37.

2000s China became Australia's number three trading partner after the United States and Japan.[21] In this context, Howard saw Australia's role as one that would stimulate "calm and constructive dialogue" between the United States and China, rather than support the hard-line American attitude towards China[22].

Of course, this did not mean that Australian policy makers were indifferent to the rise of China. For example, the abovementioned Defence White Paper includes detailed references to the rise of China and the changes in the relationship of power between China and the United States that this would bring about, including pointing out the possibility of a worsening security environment in the Asia Pacific in the next 20 years due to the course of the relationships between the major nations, especially Chinese-American and Chinese-Japanese relations.[23] The pressing issue for Australia was that there was increasing probability of conflict between China and the United States, such as the Taiwan Strait Crisis, and due to this Australia may have no choice but to involve itself in disputes through its alliance with the United States.[24] In fact, Richard Armitage, the United States Deputy Secretary of State, stated in 2001 that he wished Australia to support the United States should a Taiwan Strait Crisis occur.[25] China was not a direct threat to Australia, but at the same time it raised "strategic challenges."[26]

The important thing here was to maintain the status quo in which "no other country or group of countries will be able to challenge the United States' overall capacity to shape the global environment,"[27] rather than Australia itself directly opposing China. In so doing, Australia maintained its close relationship with the United States, while making it possible to strengthen its relationship with China at the same time. In this sense, Australia's relationship with Japan, which faced China geographically and was also where the largest American military presence in the region was located, was also extremely important. In particular, Japan expanding its role in the region would provide a counterbalance to China, as well as leading to maintaining and strengthening America's presence in the region by strengthening the American-Japanese alliance.[28] Post-Cold War Australia's basic policy towards Japan, which encouraged Japan's role in security, became all the more strategically important as the rise of China became a reality.

(2) The Establishment of Japan-United States-Australia Strategic Dialogues

Strengthening security cooperation between Japan, the United States, and Australia was proposed by Australia based on the aforementioned strategic requirements. In the ASEAN Regional Forum (ARF) held in July 2001, the Australian Minister for Foreign Affairs Alexander Downer proposed strategic dialogues between Japan, the United States, and Australia at vice-ministerial level to his

---

21 Department of Foreign Affairs and Trade, *Advancing National Interest* (Canberra: Commonwealth of Australia 2003), p. 142

22 Shannon Tow, *Independent Ally: Australia in an Age of Power Transition* (Melbourne: Melbourne U. Press, 2017) (Kindle Edition), No.5954-5956.

23 Department of Defence, *Defence 2000*, p. 18.

24 Stuart Harris, "China-US relations: A difficult balancing act for Australia?", *Global Change, Peace & Security*, Vol. 17, No. 3 (2005), p. 237.

25 Hamish McDonald, "Downer flags China shift", *The Age*, August 18, 2004.

26 Tow, *Independent Ally*, No. 5717.

27 Department of Foreign Affairs and Trade, *Advancing National Interest*, p. 21.

28 White, "Trilateralism and Australia", p. 104.

fellow foreign ministers.[29] It is said that it was Australian Secretary of the Department of Foreign Affairs and Trade Ashton Calvert who first suggested working-level trilateral security dialogues. Calvert had experience staying in Japan as an ambassador in the '90s, and was acquainted with Ambassador Ryozo Kato, who had served as Ambassador Extraordinary and Plenipotentiary of Japan to the U.S. in September 2001. Kato had a close relationship with Armitage and Australian Ambassador to the United States Michael Thawley, and it is said that these personal connections greatly contributed to the establishment of the TSD.[30]

Kato had felt that Australia had strategic value to Japan in more than the field of economics since he had served as First Secretary in the Embassy of Japan in Australia from 1975 to '78. In 1981 Kato, who had become the Director of the National Security Affairs Division in the North American Affairs Bureau, felt the need for Japan to bring out Australia's role in international society, which was as yet untried, including its role from the perspective of sea lane defense, a contemporary issue.[31] On the other hand, Kato recognized the limits of security cooperation between just Japan and Australia that resulted from the geographical distance between the two, the difference in their relationships with China, both countries' capabilities, and other factors. To Kato, the aim of Japanese-Australian security cooperation was above all for the two countries to "supplement" the American presence in the region, based on the Japan-United States alliance, and trilateral security cooperation was significant in stimulating this cooperation.[32]

With the rise of China in the background, this proposal from an allied country agreed with the United States' plan of encouraging collaboration between its allies. As a result, the first unofficial TSD meetings at vice-ministerial level took place as a sideline of discussions between American and Australian ministers in July 2002. According to Michael Green, who was the Director of Asian Affairs in the National Security Council (NSC) under the Bush administration, the first trilateral meeting discussed regional architecture rather than the problem of China. Australia in particular was concerned that the United States had shown little interests in regional architecture since President Bush was inaugurated, and together with Japan it requested that the United States regularly participate in the Asia-Pacific Economic Cooperation (APEC) and ARF. Of course, China's presence was there in the background, but military problems were not really discussed.[33] The vice-ministerial TSDs were held every year until 2005, and discussed a wide range of issues in the region, including North Korea's nuclear missile development, the issue of the non-proliferation of weapons of mass destruction, and cooperation in counterterrorism.[34] Although the rise of China was the main factor, the TSD was established as a body for relaxed consultations in which Japan, the United States, and Australia discussed general security issues in the region.

---

29 Alexander Downer, "Bias ignores years of hard work on foreign policy", *The Sydney Morning Herald*, 11 July, 2008.

30 John Hemmings, *Quasi-Alliances, Managing the Rise of China, and Domestic Politics: The US-Japan-Australia Trilateral*, thesis submitted to the Department of International Relations of the London School of Economics and Political Science for the degree of Doctor of Philosophy. London (January 2017), pp. 134-135.

31 Interview with Ryozo Kato, 6 April 2018.

32 Ibid.

33 Interview with Michael Green, 22 February 2017.

34 James L. Schoff, "The Evolution of US-Japan-Australia Security Cooperation", in Yuki Tatsumi (eds.), *US-Japan-Australia Security Cooperation: Prospects and Challenges* (Washington DC: Stimson Institute, 2015). P. 40.

2. From Exchange to Cooperation

(1) The 9/11 Terrorist Attacks

When the terrorist attacks occurred on September 11, 2001, Japan and Australia actively supported the "Global War on Terrorism." There is already a great deal of literature with detailed accounts of the support given to the United States by both Japan and Australia, so it will not be discussed at length in this paper.[35] The important point is that both Japanese and Australian policy makers became much more strongly cognizant of the necessity of supporting the United States' leadership and its role in the region in the wake of 9/11. For example, when Prime Minister Koizumi announced support for the United States in the Iraq War, his final decision was made with expectations of maintaining the relationship of mutual trust between the leaders of the US-Japan alliance, and that a strong alliance between Japan and the United States based on this relationship of mutual trust would bring about the power to deter North Korea.[36] To Japan, a decline in American prestige caused by failures in the Iraq War would lead to even more provocative action from North Korea. To avoid this situation, Japan thought it important to prevent the United States' commitment to isolationism and secure its presence in the region by proactively supporting American action.[37]

Similarly, when it came to participation in the Iraq War, Howard repeatedly emphasized the importance of supporting the United States in addition to the threat of weapons of mass destruction (WMD).[38] Here, the importance of the alliance with the United States meant self-defense for Australia as well as "maintain[ing] the involvement of the United States in our own region" through the alliance.[39] Although it was true that no direct threat (equivalent to that of North Korea to Japan) to Australia existed, preventing the United States' growing isolationism and maintaining its presence in the region was indispensable to Australia when it came to maintaining a favorable security environment, including its relationship with China. To this end, Australia had to demonstrate to the American people that "they did not have to undertake a very difficult task alone" by supporting the United States.[40] It was for this reason that Howard made the decision to participate in the Iraq war, overcoming the opposition who were against sending troops and even the majority public opinion. Like Japan, Australia understood American participation in the region

---

35 For information about the Japanese side, see e.g. Tomohito Shinoda, *Nichibei Domei to iu Riarizumu* [The Realism of the Japan-United States Alliance] (Tokyo: Chikura Publishing Company, 2007) and Tomohiko Satake, "*Nichibei Domei no 'Guroobaruka' to Sono Yukue* [The Globalization of the Japanese-American Alliance and its Course]", Yoshihide Soeya (ed.), *Chitsujo Hendo to Nihon Gaiko: Kakudai to Shushuku no 70 Nen* [The Changing Order and Japanese Diplomacy: 70 years of Expansion and Contraction]" (Tokyo: Keio University Press, 2016); on the Australian side, see e.g. Robert Garran, *True Believer: John Howard, George Bush & the American Alliance* (Sydney: Allen & Unwin, 2004) and Greg Sheridan, *The Partnership: The Inside Story of the US-Australian Alliance under Howard and Bush* (Sydney: University of New South Wales Press, 2005).

36 *Asahi Shimbun*, referencing an interview with former Chief Cabinet Secretary Fukuda on 20 March 2013.

37 Makoto Iokibe, Motoshige Ito, and Katsuyuki Yakushiji (eds.), *90 Nendai no Shogen Okamoto Yukio: Genbashugi wo Tsuranuita Gaikokan* [Testimony from the '90s Yukio Okamoto: The Diplomat Who Used a Hands-on Approach] (Tokyo: Asahi Shimbun Publications, 2008), p. 298. Okamoto was a Special Advisor to the Cabinet at the time.

38 Hugh White, "Security, Defence, and Terrorism", in James Cotton and John Ravenhill (eds.), *Trading on Alliance Security: Australia in World Affairs 2001-2005* (New York: Oxford University Press. 2006), p. 180.

39 "Transcript of the Prime Minister, the Hon. John Howard MP, Address to the Nation", 20 March 2003.

40 Sheridan, *The Partnership*, p. 65.

and supporting the United States on a global level to be inextricably linked.[41]

In light of these circumstances, Japan and Australia had a common goal of maintaining the United States' presence in the region, and it can be said that increasing cooperation in the fields of counterterrorism and non-proliferation, especially after 9/11, was the natural course. For example, the "Australia-Japan Creative Partnership" announced in May 2002 after talks between the Japanese and Australian Prime Ministers and the related action plan included agreement to high-level consultations on counter-terrorism, based on Japan and Australia's respective contributions to the fight against terrorism.[42] In August 2002, former Director-General of the Defense Agency Nakatani visited Australia for the first time in four years in this role; in dialogue with Minister for Defence Robert Hill, he agreed to implement an action plan aimed at strengthening security cooperation between the two countries, starting with counterterrorism, and to begin discussions between those ranked as heads of foreign and defense bureaus.[43] Moreover, in July 2003 the leaders of both countries signed the "Australia-Japan Joint Statement on Cooperation to Combat International Terrorism," setting out to strengthen cooperation in supporting the improvement of the counterterrorism capabilities of countries in Southeast Asia in particular, and formulating a concrete action plan.[44] In September the same year, the first Memorandum of Defense Exchange was agreed. Furthermore, the United States announced the Proliferation Security Initiative (PSI) in May 2003; both Japan and Australia proactively contributed to its activities, with Australia hosting PSI marine training in September 2003 and Japan doing so in October the following year.

At the same time, the occurrence of the 9/11 terrorist attacks prompted both Japan and Australia to strengthen cooperation in areas other than counterterrorism. One example is the cooperation between both countries in the East Timor PKO. When conflict broke out in 1999, triggered by an East Timor separatist independence movement, Australia organized the International Force East Timor (INTERFET), playing a leading role in calming the conflict. When they intervened, it was reported that Prime Minister Howard proposed that Australia would take responsibility for stabilizing the region as the "deputy sheriff" of the United States, the police of the world.[45] Although Howard later denied using the words "deputy sheriff," it can be said that they clearly captured Australia's role. In fact, while the United States played a key role in information gathering and logistical support, it did not supply any infantry to INTERFET because it was involved in conflict in Europe. There is also research with examples of the success of allied "division of labor"

---

41 Paul Kelly, "The Australian-American Alliance: Towards a Revitalization", in Jeffrey D. McCausland, Douglas T. Stuart, William T. Tow, and Michael Wesley, (eds.), *The Other Special Relationship: The United States and Australia at the Start of the 21st Century* (Canberra: Strategic Studies Institute, 2007), p. 59.

42 Ministry of Foreign Affairs of Japan, *Nichigo Shuno Kaidan Kyodo Puresu Suteetomento "Nichigo no Zozoteki Paatonaashippu" (Kayaku)* [Joint Press Statement by Prime Minister John Howard and Prime Minister Junichiro Koizumi "Australia-Japan Creative Partnership"], 1 May 2002, http://www.mofa.go.jp/mofaj/kaidan/s_koi/asi_pac02/australia_st.html.

43 Desmond Ball *"Nichigo Anzen Hosho Kankei no Yukue* [The Course of the Japan-Australia Security Relationship]", Michael Seigel and Joseph Camilleri (eds.), *Takokukanshugi to Domei no Hazama: Kiro ni Tatsu Nippon to Oosutoraria* [Caught Between Multilateralism and Alliance: Japan and Australia at a Crossroads] (Tokyo: Kokusai Shoin, 2006), p. 38.

44 Ministry of Foreign Affairs of Japan, *Kokusai Terorizumu to no Tatakai ni Kansuru Kyoryoku ni tsuite no Nichigo Kyodo Seimei (Kayaku)* [Australia-Japan Joint Statement on Cooperation to Combat International Terrorism], 16 July 2003, http://www.mofa.go.jp/mofaj/area/australia/ja_terro_s.html.

45 Fred Brenchley, "The Howard Defence Doctrine", *The Bulletin*, Vol. 28, September 1999, p. 22.

for crisis management in the region based on American-Australian cooperation.[46]

Australia also requested Japanese support, including deployment of its Self-Defense Forces (SDF) to East Timor, from the start. In response to this, Japan provided financial and humanitarian assistance, but refrained from deploying the SDF due to the five basic principles of PKO. Nonetheless, after the conflict was resolved, and as Japan had increasing pressure from the United States to contribute personnel after the 9/11 terrorist attacks, the possibility of SDF deployment resurfaced. According to media coverage by the Asahi Shimbun, the reason the SDF Ground Staff Office was especially proactive in the East Timor deployment was due to the judgement that, "Since it would be difficult to support the United States with 'boots on the ground' in Afghanistan and the surrounding areas, there is no choice but to supplement, even indirectly, the American military's endeavors for international security, which are developing on a global scale."[47] As a result, in March 2002 the Japanese government deployed an SDF engineering unit of 690 people, the largest ever for a PKO, to East Timor. Like Australia, Japan understood contributing to East Timor PKO as part of supporting the United States.

It has been acknowledged that at the time Australia was "isolated" in Asia due to this issue, and struggling as to ways to involve countries in the region, including Japan.[48] In these circumstances, Australia valued the decision to deploy the SDF, and expressed strong gratitude. Australia's foreign and trade policy white paper published in 2003 noted the rapid Japanese response since 9/11, as well as stating that Japanese-Australian contributions to East Timor PKO were evidence that "we can work together to enhance our mutual security and that of the region."[49] To both Japan and Australia, this cooperation was more than the independent contributions of countries in the region to maintain the regional order; it was also built upon Japan and Australia's common strategic aims of collaborating to supplement the role of the United States, which had been fully committed to the global war against terrorism since 9/11, and of maintaining the United States' presence in the region, based on a stable alliance system.

(2) Cooperation in Supporting Reconstruction in Iraq

Cooperation in supporting Iraqi reconstruction strengthened the relationship between the SDF and the Australian military even more. In February 2005, Prime Minister Howard held a press conference in Canberra and announced a plan to send reinforcements of 450 Australian military personnel to "ensure the safety of the SDF" in southern Iraq, where the Ground Self-Defense Forces (GSDF) were stationed. Before the election that took place in October the previous year, Howard had refused to send reinforcements to Iraq, and he was censured by the opposition, including the Labor Party. Public opinion polls indicated that this was a decision made amid opposition to sending reinforcements to Iraq from the majority of people.[50] The SDF had liaison officers stay at

---

46 Coral Bell, "East Timor, Canberra and Washington: A Case Study in Crisis Management", *Australian Journal of International Affairs*, Vol. 54, No. 2, pp. 171-176.

47 Asahi Shimbun "SDF 50 Years" reporting crew *Jieitai Shirarezaru Henyo* [The Self-Defense Force The Unknown Transformation](Tokyo: The Asahi Shimbun, 2005) p. 41.

48 Duncan Campbell, "Invisible friends are no comfort / Diplomacy at the Crossroads", *The Australian*, 15 September 1999.

49 Department of Foreign Affairs and Trade, *Advancing National Interest*, p. 78.

50 Michelle Hespe, "Polls show new Australian opposition to protecting Japanese in Iraq", *Kyodo News*, 15 March 2005.

Camp Smitty, where the British and Australian troops were stationed, and gather information and coordinate joint training. The Australian military offered a range of support to the activities of the SDF, including ensuring their safety, which were appreciated by the Japanese.[51]

Howard later made it clear that his decision to send Australian troops meant providing a strategic aspect to the Japan-Australia relationship, which had conventionally centered on economics.[52] Notably, there were internal sensitive constitutional issues relating to deploying the SDF to Iraq, and due to this Australia was concerned about a "very serious blow" striking the efforts of the allied forces should the SDF pull out, following the Dutch troops, due to safety issues.[53] Australia recognized the Japanese contribution to boots on the ground in Iraq as a litmus test indicating the country's greater commitment to other issues, such as Islamic fundamentalism and the spread of WMD.[54] Supporting the SDF activities in Iraq allowed the success of the American-led "war on terror," as well as meeting Australia's strategic aim of expanding Japan's role in security on a regional and global level.

Through this cooperation in Iraq, the Japanese perception of Australia greatly improved. Some Australian experts have voiced the opinion that without the deployment, it was "highly unlikely" that the 2007 Japan-Australia Joint Declaration on Security Cooperation would have been signed.[55] In an interview for the Australian media before Howard's visit to Japan in April 2005, Prime Minister Koizumi announced a gesture of apology for the conduct of the Japanese army during WWII, as well as his intent to consider the possibility of a bilateral free trade agreement (FTA), for which Australia was strongly pushing at that time; he also later agreed to the establishment of an FTA research group.[56] Takashi Terada analyzes that when it came to Koizumi's decision to consider an FTA with Australia, the national agreement to which would be difficult to obtain, "Koizumi's wish to take gains from Australian trade more seriously was reflected as an expression of gratitude to Australia, which had sent in troops to Iraq for the security of the SDF."[57]

The practical cooperation between Japan, the United States, and Australia also moved forwards in the field of disaster relief. When the Indian Ocean Earthquake and Tsunami took place on December 26, 2004, Japan sent three Maritime Self-Defense Force (MSDF) ships as well as two Air Self-Defense Force (ASDF) transportation aircraft and the GSDF Seventh Division (230 people) to Aceh Province in Indonesia, together with 800-900 SDF troops, and 500 million dollars of financial aid. Around the same time, Australia also sent four C130 transport aircraft and

---

51 For example, see Iraq Reconstruction and Support Group "Iraku Fukko Shien Katsudo Hokoku [Iraq Reconstruction and Support Group Activity Report]", 21 February 2006, https://www.asahicom.jp/news/esi/ichikijiatesi/iraq-nippo-list/20180416/370/060221.pdf, p. 15.

52 John Howard, *Lazarus Rising: A Personal and Political Autobiography* (Sydney: HarperCollins Publishers, 2010), p. 458.

53 Steve Lewis and Patrick Walters, "PM doubles troops to Iraq - 450 more Aussie soldiers to protect 850 Japanese engineers", *The Australian*, 23 February 2005.

54 Tom Allard, "Decision hinged on the result of two elections", *The Sydney Morning Herald*, 23 February 2005.

55 Malcolm Cook and Andrew Shearer, "Gooingu Guroobaru: Takokukan Kyoryoku no tame no Nichigo Ryokoku no Aratana Ajenda [Going global: A new Australia-Japan agenda for multilateral cooperation]", Lowy Institute, April 2009, p. 12.

56 "Japan PM Koizumi open to WWII apology", *Australian Associated Press Financial News Wire*, 19 April 2005.

57 Takashi Terada, "Nichigo Anzen Hosho Paatonaashippu no Shinten: Beichu no Yakuwari to Kokusai Kozo Henka [The Development of the Japan-Australia Security Partnership: The Role of the United States and China and Changes in International Structures]", Shotaro Yachi (ed.), *Ronshu: Nihon no Gaiko to Sogoteki Anzen Hosho* [Essay Collection: Japanese Diplomacy and Comprehensive Security] (Tokyo: Wedge, 2013), p. 282.

a ship from its naval fleet for rescue purposes; it also announced it would give an unprecedentedly large 765 million dollars in aid. Japan and Australia, together with India, played central roles alongside the United States in the international support system, participating in an integrated task force formed by the United States Asia-Pacific Command and the United States Marine Corps to aid disaster victims. Deputy Secretary of State Armitage praised these actions, saying to Vice-Minister for Foreign Affairs Yukio Takeuchi that they had strongly promoted closer cooperation with Australia.[58]

In this way, field-level cooperation between the SDF and the Australian military had moved to a regional and global level since the 9/11 terrorist attacks. By chance, the Japan-United States-Australia strategic dialogues that had been established before 9/11 came to provide a framework to coordinate trilateral cooperation after 9/11. Of course, security cooperation between Japan, the United States, and Australia may have moved forward even without 9/11, but these terrorist attacks were a challenge to the international order led by the United States, and it seems clear that this challenge accelerated the cooperation between these three countries. In particular, the Japanese-Australian cooperation in stabilizing East Timor and supporting the reconstruction of Iraq directly indicated an aim of maintaining and strengthening the United States' presence in the region based on stable allied relationships, by "supplementing" the United States' regional and global role through the cooperation of its allies. As a result, Japanese-Australian defense exchanges evolved into more practical cooperation, including cooperation in the field.

3. Institutionalizing Security Cooperation

(1) The Establishment of TSD Ministerial-Level Discussions and the Japan-Australia Joint Declaration on Security Cooperation

In a trilateral meeting of the foreign ministers of Japan, the United States, and Australia in May 2005, it was decided to elevate the TSD to ministerial-level discussions. The direct catalyst for this was the change in the American Deputy Secretary of State in February 2005. In contrast to Armitage, who had pushed for trilateral security cooperation, it is said that while the newly appointed Robert Zoellick saw China as a "responsible stakeholder" and emphasized American-Chinese relations, he did not show so much interest in the TSD. American and Australian government officials felt a growing sense of crisis in these circumstances, and ensured ministerial-level TSD by appealing to both American Secretary of State Rice and the Australian Minister for Foreign Affairs Downer, trying to maintain the momentum of trilateral cooperation.[59] As a result, in March 2006 the first ministerial-level TSD discussions were held in Sydney. In a joint statement after the meeting, it was publicly announced that the three countries would enhance their sharing of information and strategic assessments relating to international and regional security issues to strengthen cooperation between Japan, the United States, and Australia.[60]

Furthermore, in addition to the TSD process centered on foreign affairs departments, a framework for cooperation centered on national defense divisions was also strengthened. In

---

58 Shinoda, *Nichibei Domei to iu Riarizumu*, p. 234.

59 Hemmings, *Quasi-Alliances, Managing the Rise of China, and Domestic Politics*, pp. 146-147.

60 Ministry of Foreign Affairs of Japan, *Nichibeigo Senryaku Daiwa Kyodo Suteetomento (Kayaku)* [Trilateral Strategic Dialogue Joint Statement Australia-Japan-United States]", 18 March 2006, https://www.mofa.go.jp/mofaj/kaidan/g_aso/australia_06/jua_smt.html.

2006 the United States Department of Defense proposed cooperation between national defense departments through a framework separate from the TSD, and as a result the relevant parties agreed to establish the U.S.-Japan-Australia Security and Defense Cooperation Forum (SDCF) in February the following year, with the first forum held in Tokyo in April. Uniformed personnel and officials from the three countries' national defense departments and state (foreign affairs) departments participated in the SDCF; its initial agenda included disaster relief, missile defense, counter-piracy operations, previous training in bilateral exercises and non-proliferation, interoperability, and information sharing.[61] In June the same year, the first meeting between the three countries' ministers for defense was held in Singapore.

In this way, as trilateral cooperation between Japan, the United States, and Australia developed, the security relationship between Japan and Australia, the "weakest link," also became stronger. Notably, the opportunities for Japanese and Australian cabinet ministers and policy makers to meet regularly through the framework of the TSD played a major role in making security cooperation between the two countries more substantive.[62] Consequently, in March 2007, Prime Minister Abe and Australian Prime Minister Howard adopted the Japan-Australia Joint Declaration on Security Cooperation. As Teruhiko Fukushima points out, "Rather than setting out a new kind of collaboration, [the declaration was] an agreement characterized by confirming security cooperation to date, and wishing to confirm the intent to enhance cooperation between the two countries in the future."[63] It was, in fact, akin to a "skeleton" for enhancing cooperation, and did not contain practical details.

However, this "skeleton" would later be "fleshed out" through more practical cooperation. In June 2007, the Australian Minister for Defence Nelson visited Japan, the first visit in approximately four years by an Australian Minister of Defence. Nelson met with Defense Minister Kyuma in Tokyo, and subsequently the first 2+2 was held. Moreover, in September the same year, the Action Plan to implement the Japan-Australia Joint Declaration on Security Cooperation was issued, presenting a concrete road map to put the declaration into effect. This roadmap not only listed bilateral defense cooperation, it also included a wide range of points for cooperation, such as United Nations reforms, law enforcement, national border security, counterterrorism, disarmament and non-proliferation, PKO, and disaster relief.[64]

It is said that at first the Australian side assumed that the Japan-Australia Joint Declaration on Security Cooperation would be an agreement similar to the security framework agreement signed in November that year with Indonesia (the Lombok Treaty), but the Japanese side was concerned that a formal agreement would become the subject of parliamentary debate, and so it

---

61 Schoff, "The Evolution of US-Japan-Australia Security Cooperation", pp. 42-43.

62 Ibid.

63 Teruhiko Fukushima, "Nihon Gaiko ni okeru Tai Oosutoraria Kankei no Imi: Sengo Nichigo Kankei no Hatten Kankei [The Meaning of the Relationship with Australia in Japanese Diplomacy: The Development Course of the Post-war Japanese-Australian Relationship]", Kanazawa Institute of Technology, Institute for International Studies (ed.), *Nihon Gaiko to Kokusai Kankei* [Japanese Diplomacy and International Relationships], (Tokyo: Naigai Publishing, 2009) p. 209.

64 Ministry of Foreign Affairs of Japan, *Anzen Hosho Kyoryoku ni Kansuru Nichigo Kyodo Sengen wo Jisshisuru tame no Kodokeikaku no Shuyona Yoso (Kayaku)* [Major elements of the Action Plan to implement the Japan-Australia Joint Declaration on Security Cooperation]", September 2007, http://www.mofa.go.jp/mofaj/area/australia/0709_kk.html.

took the form of a joint declaration.[65] An alternate perspective is that the Japanese and Australian negotiators expected the announcement of the joint declaration to be a stepping stone towards the signing of a future formal security treaty.[66] In any case, at the very least there was no consensus with regard to concluding a formal security agreement together with a treaty with the Japanese side within the Australian government of the time. In particular, it has been said that there were very few parties that supported a treaty with fixed mutual defense obligations against attack from a third country.[67] Furthermore, although it is held that the Abe administration was initially eager for a formal agreement, when the joint declaration was announced the administration's approval rating had dropped due to verbal gaffes from cabinet ministers and scandals, and there was growing criticism in the absence of WMD in Iraq; to expect to sign a security treaty with Australia, which involved political risk, was not realistic for the Japanese side.

(2) The Rise of China?

As discussed in the previous section, close cooperation on a practical level between Japan, the United States, and Australia after 9/11, as well as the rise of China, lay behind the advancing institutionalization of Japan-American-Australian security cooperation from the mid-2000s. Although the Chinese-American relationship temporarily improved post-9/11, an antagonistic mood between the two countries was once again growing in relation to reforms to the renminbi, human rights issues, and the problem of nuclear development in North Korea and Iran. The February 2006 American Quadrennial Defense Review (QDR) expressed an extremely harsh view of China, saying "Of the major and emerging powers, China has the greatest potential to compete militarily with the United States." The QDR also made it clear that the United States was to strengthen integrated operations and information cooperation with its partners in deepening bilateral and multilateral participation and in dealing with common security issues, naming Japan, the Republic of Korea, Australia, and India.[68]

Going into the 2000s, Japan also increased ASDF scrambles in response to Chinese warplanes, and raised its guard against Chinese military activity due to repeated intrusions into Japanese territorial waters and the Exclusive Economic Zone by the Chinese navy, and other actions. The new National Defense Program Guidelines published in 2004 made reference to China's progressing modernization of nuclear and missile forces and marine and air power, and the expanding scope of its marine activities; it also considered a "response to an invasion of the islands" to be the first role of national defense capabilities.[69] In September 2005, an incident occurred in which a Chinese naval ship aimed a 100 mm gun at an MSDF P-3C patrol plane near

---

65 Fukushima, "Nihon Gaiko ni okeru Tai Oosutoraria Kankei no Imi: Sengo Nichigo Kankei no Hatten Kankei", p. 209.

66 Greg Sheridan, "Security treaty rejected by Tokyo", *The Australian*, March 12, 2007.

67 Interview with Murray McLean, former Ambassador to Japan, 11 October 2017.

68 United States Department of Defense, *Quadrennial Defense Review Report*, February 6, 2006, p. 88.

69 Prime Minister's Office of Japan, *Heisei 17 Nen Iko ni Kakaru Boei Keikaku no Taiko ni tsuite* [Outline of Defense Plans from 2005], 10 December 2004, https://www.kantei.go.jp/jp/kakugikettei/2004/1210taikou.html (accessed 31 May 2018).

gas fields in the East China Sea.[70] Moreover, the political relationship between Japan and China had cooled due to, for example, Prime Minister Koizumi's visit to Yasukuni Shrine, and in this context the Japanese people's perception of China became all the more hostile. According to a public opinion poll conducted in November 2005, 72% of respondents replied that they "cannot trust China," and 76% answered that they "feel a threat" from China.[71]

At the same time, Australia was also gradually raising its guard against the rise of China. A Defence Update, a report from the Department of Defence published in 2003, took the view that while the Chinese-American relationship was more stable than before, there was a continuing possibility of mutual misperceptions regarding both countries' strategic competition and the issue of Taiwan.[72] The 2005 version of this report made reference to the point that the pace and scale of China's defense modernization was giving rise to the possibility of misperceptions, and called for increased transparency concerning China's military and for the development of capabilities according to legitimate security needs.[73] A further report, published two years later, noted the possibility that enhancing the new capabilities of the Chinese military would lead not just to misperceptions but could damage stability in the region, referencing the antisatellite weapons that China had tested in January 2007.[74]

However, even at this stage, it can be said that there was still a huge gap between Tokyo and Canberra in terms of their perceptions of China as a threat.[75] Notably, as a result of the strengthening of Australia's relationship with China under the Howard administration, Australian exports to China from 1996 to 2006 averaged 18% per year, and increased by a total of 626%.[76] In 2007 China became Australia's largest trading partner other than Japan. On the security side, in October 2004 the first joint marine training exercise between the Australian military and the People's Liberation Army took place; although these were limited, they developed a relationship between the militaries.[77] In August 2004 Minister for Foreign Affairs Downer visited China and provoked controversy when he stated the point of view that military movements against countries or regions other than the United States or Australia would not automatically invoke the ANZUS Treaty, in response to a question about Australia's obligation to defend Taiwan via the Australia-

---

70 Richard J. Samuels (translation supervisor Takashi Shiraishi), *Nihon Boei no Daisenryaku: Fukoku Kyohei kara Gorudirokkusu Consensasu made* [Securing Japan: Tokyo's Grand Strategy and the Future of East Asia] (Tokyo: Nikkei Publishing Inc., 2009), p. 238.

71 Yasuhiro Matsuda, "Dai 6 Sho Anzen Hosho Kankei no Tenkai [Chapter 6 The Development of a Security Relationship]", Ryoko Iechika, Yasuhiro Matsuda, and Zuiso Dan (eds.), *(Kaiteiban) Kiro ni Tatsu Nitchu Kankei: Kako to no Taiwa, Mirai e no Mosaku* [The Japan-China Relationship at a Crossroads: Dialogues with the Past, Exploring the Future (Revised Edition)] (Tokyo: Koyo Shobo Publisher, 2012), p. 145.

72 Australian Department of Defence, *Defence Update 2003* (Canberra: Commonwealth of Australia, 2003), p. 8.

73 Australian Department of Defence, *Defence Update 2005* (Canberra: Commonwealth of Australia, 2005), pp. 6-7.

74 Australian Department of Defence, *Defence Update 2007* (Canberra: Commonwealth of Australia, 2007), p. 20.

75 For information about perceptions of China in Australian public opinion during this period, see e.g. Ivan Cook, *The Lowy Institute Poll: Australians Speak Public Opinion and Foreign Policy* (Canberra: Lowy Institute for International Policy, 2005), p. 1.

76 Allan Gyngell, *Fear of Abandonment: Australia in the World since 1942* (Melbourne: La Trobe University Press, 2017) (Kindle Edition), No.6166-6168.

77 Stuart Harris, "China–US relations: A difficult balancing act for Australia?", *Global Change, Peace & Security*, Vol. 17, No. 3, 2005, p. 235.

United States alliance.[78] Moreover, in February 2005 the United States and Japan requested that the EU continue the restrictions on arms exports to China; Australia did not participate in this pressuring. It is said that Japanese and American policy makers were extremely concerned over the Australian attitude towards China. One viewpoint holds that the United States raised the TSD to foreign-ministerial level to "pull" Australia to their side.[79]

In this way, although Australia's attitude towards China differed from those of the United States and Japan, Australia's response to stepping up the TSD included the goal of maintaining the United States' presence in the region, as already touched upon, and the expectation of expanding Japan's role in the region (in a way that would not irritate China) through the TSD framework. Australia's policy makers in particular were unsatisfied with the slow speed of the development of security cooperation between Japan and Australia due to a lack of bureaucracy and leadership in Japan since the '90s.[80] It can be said that the TSD and SDCF provided a suitable place for the United States and Australia to encourage Japan to deepen its commitment to regional defense and security issues. It is thought that the Australian side in particular wished for Japan to take on responsibility for part of these activities as, in addition to the war on terror at the time, it was sending a succession of forces overseas for PKO in East Timor and other locations.[81]

In fact, according to James Schoff, who attended the SDCF as staff of the American Department of Defense, China was mentioned during the forum but most of the time this was "only in the context of framing the strategic environment: directly when officials noted North Korea's growing missile and nuclear threats or complained about China's lack of military transparency."[82] The TSD also formed working groups on a professional level under the officials' discussions; the fields covered were humanitarian aid and disaster relief, counter terrorism, information sharing, non-proliferation, and issues and areas relating to the general regional order of the Pacific islands and Southeast Asia. Rather than directly opposing the Chinese military threat, it can be said that the issues raised here were brought up from the perspective of how to stabilize the existing regional order by maintaining an American presence and expanding the Japanese role.

This explains why the strategic dialogue between Japan, the United States, Australia, and India that was suggested around the same time suffered from setbacks while the US-Japan-Australia trilateral dialogues advanced. The quadrilateral security dialogue was proposed by US policy makers and Japanese Prime Minister Shinzo Abe, and an informal meeting was held between representatives of the four counties in May 2005. However, following this China made objections to the three countries through official routes, and the momentum for quadrilateral cooperation was diminished. At a joint press conference with the Chinese foreign minister in February 2008, Minister for Foreign Affairs Steven Smith of the Kevin Rudd administration (which followed the Howard administration) stated that Australia had no intention of participating in quadrilateral strategic dialogues.[83] It is said that Yasuo Fukuda, who succeeded Abe as prime minister, expressed

---

78 Hamish McDonald and Mark Forbes, "Downer flags China shift", *The Age*, August 18, 2004.

79 White, "Trilateralism and Australia", p. 109.

80 Ibid., p. 104.

81 "Yakuwari Kawaru Nichibei Domei Sekai no Chitsujo Iji/Kochiku Shifuto wo [The Changing Role of the Japan-United States Alliance: A Shift in Maintaining and Building a World Order]", *Asahi Shimbun*, 21 March 2007.

82 Schoff, "The Evolution of US-Japan-Australia Security Cooperation", pp. 42-43.

83 Indrani Bagchi, "Australia to pull out of 'quad' that excludes China", *The Times of India*, February 6, 2008.

barely any interest in quadrilateral security cooperation.[84] At any rate, in the 2000s there was no consensus in Japan, let alone in Australia, regarding formalizing cooperation with India, a country not allied with the United States, to the extent of risking irritating China.

Conclusion

As can be seen above, security cooperation between Japan and Australia, and Japan, the United States, and Australia grew stronger in the 2000s. This occurred to a large extent as an extension of Japan and Australia's relationship with the United States. The fundamental issue concerning Japanese-Australian cooperation was how to maintain and strengthen the United States' presence in the region, keeping in mind the rise of China and the threat of North Korea. Australia in particular sought to maintain the United States' strategic predominance in a form that would not damage its relationship with China, even as it was vigilant of China's rise. To do so, Australia worked hard to strengthen its bilateral alliance with the United States, expand Japan's role in security, and to strengthen US-Japan-Australia security cooperation, which would encourage both of these outcomes. Although China was the main "factor" in stimulating stronger security cooperation between Japan, the United States, and Australia, it was not the direct "target" of this cooperation.

In this sense, it can be said that both Japan and Australia in the 2000s held quite different strategic perceptions to the United States' strategic goal of forming a "federated network" and "external balancing" vis-à-vis China by strengthening its relationships with its allies (and between its allies). At the very least, as long as the United States maintained its strategic predominance in the region, formalizing allied relationships and strengthening US-Japan-Australia-India cooperation, which could irritate China, were not an urgent issue to either country. From Australia's perspective in particular, which placed importance on its relationship with China, a policy of external balancing with China, including potentially entering into an allied relationship with Japan, caused a dual risk—not only risking irritating China but also in the sense of increasing the risk of becoming caught up in the conflict between Japan and China. Rather than an explicit external balancing with China, the optimum solution for both Japan and Australia lay in maintaining and strengthening the United States' presence in the region based on the hub and spokes system. This was achievable through collaboration between Australia and Japan to supplement the United States' local and global role. From this perspective, one can see subtle differences between the United States (in conflict with China over regional hegemony) and its "junior partners," Japan and Australia, in terms of their standpoints vis-à-vis the rise of China.

[84] Terada, "Nichigo Anzen Hosho Paatonaashippu no Shinten: Beichu no Yakuwari to Kokusai Kozo Henka", p. 229.

Strengthening Public-Private Partnership in Cyber Defense: A Comparison with the Republic of Estonia*

YAMAGUCHI Yoshihiro[1]**

Abstract

This paper looks at Japan's cybersecurity policies while placing the focus on the defense of critical infrastructure that is directly related to national security, and examines the measures that need to be put in place going forward in regard to public-private partnership initiatives. Firstly, it takes a broad overview of Japan's policies followed by an overview of the cybersecurity policies of the Republic of Estonia, and carries out a comparison with Japan based on the following six classifications: cybersecurity strategy, legal systems, public-private partnership organizations and information-sharing systems, risk analysis and business continuity plans, cyber exercises, and national defense strategy and organizations. Then, the feasibility of implementation in Japan is considered. Finally, it makes the following recommendations: (1) Positioning the protection of critical infrastructure as the most important issue in the cybersecurity strategy; (2) Reviewing the legal system and strengthening the supervision and guidance of critical information infrastructure (CII) operators; (3) Strengthening the authority of the National center of Incident readiness and Strategy for Cybersecurity (NISC), and enhancing its functions; (4) Implementing exercises in preparation for a large-scale cyberattack at the national level; (5) Building a framework that enables civilians with advanced skills to participate in national defense in cyberspace.

Introduction

Late at night on April 27, 2007, a cyberattack was launched on the websites of the Estonian government and media organizations in the private sector. Initially, this had been a Denial of Service (DoS) attack that employed the simple method of sending ping commands in a concentrated attack to the target server. However, the methods used became increasingly sophisticated. The domain name system (DNS) of Estonia's leading Internet service provider (ISP) became targets of the attacks, and Distributed Denial of Service (DDoS) attacks were carried out simultaneously from

* Originally published in Japanese in *Boei Kenkyusho Kiyo* [NIDS Security Studies], vol.21, no.1, December 2018. Some parts have been updated.

** Information and Communications Section, Defense and Operations Division, Air Staff Office

1 This paper contains additions and revisions made to a paper submitted for the 65th General Course (Graduate School Partnership Program) of the National Institute for Defense Studies (NIDS). The views expressed in this paper are those of the author and do not represent the views of the author's organization. The author would like to thank Prof. Yasuaki Hashimoto, Director, Policy Studies Department, NIDS, Prof. Atsushi Sunami, Executive Advisor to the President, National Graduate Institute for Policy Studies (GRIPS), and Prof. Narushige Michishita, GRIPS, for their guidance in preparing this paper and NIDS for providing research space.

multiple botnets. As a result, Internet communications were interrupted intermittently.

From midnight of May 9 (Moscow time), which is also Russia's Victory Day, to May 10, the DDoS attacks reached their peak, and the operation of 58 websites including those of government agencies was simultaneously interrupted, forcing many banks to suspend their business operations. By May 18 when the attacks subsided, the Congress, government ministries and agencies, ISP, telephone networks, mass media, banks, and credit card companies were among the organizations that had been targeted. The attacks included DDoS attacks, tampering with webpages, attacks on DNS servers, and the jamming of communications through mass spam mails.[2]

During the cyberattack that lasted approximately three weeks, the Computer Emergency Response Team-Estonia (CERT-EE) provided 24-hour response and support for the large-scale cyberattack, while receiving assistance from volunteer cybersecurity experts from Estonia and abroad. With regard to the DDoS attacks, CERT-EE worked in cooperation with communications carriers and security companies to expand bandwidth for governmental networks and reinforce server processing capability, as well as install firewalls. At the same time, through analyses on the patterns of the attack, it successfully interrupted many attacks by establishing effective filtering rules for the ISPs.[3]

This large-scale cyberattack had been triggered by the Estonian government's decision to remove all monuments erected during the Soviet occupation. An old bronze statue of a Soviet soldier installed in the capital city of Tallinn had been erected to commemorate the victory of the Soviet army against Nazi Germany during the Second World War. For Estonians who were ethnic Russians, this statue was a symbol of a victory won by their motherland, Russia.

Figure 1 Bronze statue of a Soviet soldier and monument, prior to its relocation[4]

Source: Extracted from BBC news report (April 27, 2017)

However, this bronze statue was gradually transformed into a site of nationalism conflict as the result of a violent incident by Russian Estonians against non-Russian Estonians that took place near the bronze statue on May 9, 2006, Russia's Victory Day. The Estonian government, with a sense of crisis, announced in March 2007 that the bronze statue would be relocated to a cemetery for the war dead in the suburbs of Tallinn. On April 26, 2007, after the government erected a fence in the area in preparation for the relocation of the statue, Russian Estonians gathered in opposition

2 Tikk, E., Kaska, K., Vihul, L., *International Cyber Incidents: Legal Consideration* (NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010), pp. 18-22.

3 Ibid., p. 24.

4 Damien McGuinness, How a cyber attack transformed Estonia, BBC News 27 April 2017, http://www.bbc.com/news/39655415.

of the move. This erupted into a riot that included acts of vandalism on the surrounding facilities. This riot resulted in one death, several hundred injured persons, and the arrest of about 1,300 people. Furthermore, an opposition demonstration unfolded in front of the Estonian embassy in Moscow, and even led to the assault of the Ambassador of Estonia to Russia.[5]

The large-scale cyberattack on Estonia occurred under these circumstances, and became known as the first attack in history carried out against a nation in cyberspace.[6]

Cyberspace has long been described as the "fifth domain of war" after land, sea, air, and space. Cyberattacks have developed to become one of the means of achieving the goals in political and diplomatic disputes between countries, as demonstrated by the examples of attacks in Estonia and Georgia, as well as the Stuxnet virus attack on Iran. Countries around the world view large-scale cyberattacks as an important national security issue; alongside with advancing cybersecurity policies at the national level, they have also established dedicated cyberwar units in their armies, such as the newly set up United States Cyber Command and the People's Liberation Army Strategic Support Force of China, and are moving forward on preparations for the cyberwars that are expected to happen in the near future. Japan, too, is steadily advancing cybersecurity measures at the national level. Within the Ministry of Defense and Self-Defense Forces, it has established a new Cyber Defense Group and is working to strengthen its coping mechanism.

In Japan, although there are incidents of information leakage, theft of corporate information, and hacking for financial profit, large-scale cyberattacks that cause serious damage to critical infrastructure have never occurred to date. Japan has problems such as territorial issues with neighboring countries and its perception of history, which can potentially trigger political and diplomatic disputes. It has also adopted a hardline stance with regard to North Korea's nuclear missile development issue, and is continuing to apply pressure primarily through economic sanctions. The Rugby World Cup and Tokyo Olympic and Paralympic Games will be held in Japan in 2019 and 2020 respectively. In view of these factors, it is likely that large-scale cyberattacks with political or diplomatic motives and cyberattacks that are used as a means of terrorism may be carried out on Japan's critical infrastructure. The means of carrying out cyberattacks are growing increasingly sophisticated year after year. In the event that a large-scale cyberattack is carried out using methods that are more complex and sophisticated than that of the Estonian incident that occurred about 10 years ago, will Japan be able to put in place effective response measures?

The purpose of this paper is to establish how public-private partnership initiatives have progressed with regard to the cybersecurity policies that Japan has been implementing to date, which are the measures that are superior to those of other countries, which are the areas that are lagging behind in its countermeasures, and what measures need to be put in place going forward. Among the extensive and wide-ranging cybersecurity policies, the analysis in this paper places the focus on the protection of critical infrastructure that is directly linked to national security.

The discussion in this paper is set out as follows. Firstly, section 1 establishes the importance of joint efforts by the public and private sectors to build a cyber defense system from the perspective of deterrence and the characteristics of cyberspace, and taking into account the current situation surrounding cyberattacks.

---

5 Tikk, *International Cyber Incidents: Legal Consideration*, p. 16.

6 Hiroshi Itoh, *"Daigo no Senjo: Saibasen no Kyoi"* [The Fifth Domain of War: The Threat of Cyberwar)], (Shodensha Shinsho, 2012), p. 142.

Next, section 2 verifies the current situation with regard to public-private partnership initiatives in the area of cyber defense in Japan, while Section 3 provides an overview of the various policies that the Republic of Estonia (hereafter, "Estonia") is implementing in its active efforts to advance public-private partnership on cyber defense for critical services, followed by a comparison with Japan and a review of the feasibility of implementing such policies in Japan. In comparing the respective policies of Estonia and Japan, this paper places particular focus on public-private partnership in the protection of critical infrastructure, and carries out its analysis based on the following six classifications: cybersecurity strategy, legal systems, public-private partnership organizations and information sharing systems, risk analysis and business continuity plans, cyber exercises, and national defense strategy and organizations.

Finally, in section 4, this paper offers recommendations of several policies aimed at promoting public-private partnership in cyber defense in Japan.

1. The Importance of Public-Private Partnership in Cyber Defense

Why is public-private partnership necessary in order to realize the defense of cyberspace? The answer to this question can be summarized in the following two points: (1) Cyberspace itself and much of the country's critical infrastructure is operated by the private sector; and, (2) To secure deterrent power in cyberspace, it is vital for the government to gain the cooperation of private-sector operators.

(1) Characteristics of cyberspace

Cyberspace, unlike the domains of land, sea, air, and space, is unique in the sense that it is a man-made domain. Cyberspace is composed of terminal equipment such as computers, smartphones, and network cameras, networks such as Local Area Network (LAN) cables, optical lines, Wi-Fi (wireless LAN), mobile phone networks, international submarine cables, and satellite communication lines, various software and applications that are installed in the terminals, and communications protocols such as TCP/IP (Transmission Control Protocol/Internet Protocol), HTTP (Hypertext Transfer Protocol), and SMTP (Simple Mail Transfer Protocol). All of these components are primarily maintained and operated by private-sector operators. Furthermore, with the rapid advancement of information and communications technology, all the systems that make up society have become networked, and Internet technology is now actively applied to the critical infrastructure of a country such as electricity, communications, water, gas, transportation, railroads, and finance, with the purposes of improving the efficiency of maintenance and management as well as saving manpower. A large-scale cyberattack on such critical infrastructure could paralyze the functions of a country and have a serious impact on citizens' lives and economic and social activities. Regardless of that, the majority of a country's critical infrastructure is maintained and operated by operators in the private sector.

As seen in the cases of Estonia, Syria, Georgia, and Ukraine, cyberattacks that are linked to military operations are being carried out in reality. In international armed conflicts, there is a strong likelihood for cyberattacks to be carried out not only on the central leadership of a country and its military organizations, but also on its critical infrastructure, in tandem with military operations conducted through conventional military forces or as a part of a surprise attack. Taking into consideration such characteristics of cyberspace and the dependence of critical infrastructure on the private sector, unlike the domains of land, sea, air, and space, it is difficult for the cyber defense unit

of a country's military force to defend the country alone. Rather, it is important to cooperate with many private-sector actors such as communications carriers, ISPs, manufacturers of information and communications equipment and software companies, security enterprises, and CII operators.

(2) Deterrence in cyberspace

Next, I would like to consider public-private partnership from the perspective of deterrence. The concept of deterrence is often categorized generally into deterrence by punishment and deterrence by denial. Deterrence by punishment involves applying pressure on the enemy's cost calculations based on the threat of delivering an unbearable blow, in order to make the enemy give up the idea of launching an attack. Deterrence by denial involves applying pressure on the enemy's calculations of the possibility of achieving its goal, based on the ability to physically deter specific offensive action, in order to make the enemy give up the idea of launching an attack.[7] In cyberspace, however, it is difficult for either deterrence by punishment or deterrence by denial to fulfill their functions.

Attackers in cyberspace carry out their attacks by using the terminals of a third-party as the jump server, and attempt to escape discovery or identification by disguising these third-party terminals as the source of the attack. The defenders have to analyze these acts of disguise and concealment in order to identify the attackers. To achieve that, it is necessary to obtain various information and carry out analyses, such as the analysis of various communication logs and the terminals used as the jump server, as well as the tracking of the command and control servers that issued the commands to the botnet. However, it takes advanced technology, time, and effort to collect and analyze such information, and it is extremely difficult to identify the attackers. This is what is known as the attribution problem. Even if the defenders were to attempt to carry out a retaliatory attack on the source of the attack, it is difficult to determine if the target is the actual attacker or the third-party used as a jump server. Moreover, it is also difficult to project the effectiveness of the counterattack. Hence, the defenders cannot help but hesitate to execute a retaliatory attack. For this reason, while it is possible for attackers to launch a one-sided attack without fear of reprisal, it is difficult for defenders to identify the source of attack and retaliate. In this sense, it is difficult to strike an overwhelming and unbearable attack on the attackers, making it difficult for deterrence by punishment to function in cyberspace. Vulnerabilities that are caused by software security flaws and which are generally unknown, are called "zero-day vulnerabilities," and it is impossible to completely eliminate such vulnerabilities. Any attempts by the defenders to completely eliminate zero-day vulnerabilities, strengthen security and realize complete defense would incur an infinite cost. While the attackers can select a vulnerability to launch an attack on, it is extremely difficult for the defenders to address and resolve all vulnerabilities. As such, it is also difficult for deterrence by denial to function.

Deterrence through resilience is now drawing attention as a means of overcoming the difficulties of applying the aforementioned conventional theories of deterrence to cyberspace. Deterrence through resilience involves putting in place measures based on the premise of the defender suffering damage as a result of a cyberattack. The approach is to weaken the attacker's will to attack by ensuring that operations continue even when damage has been sustained as

[7] Ministry of Defense, "(Kaisetsu) Yokushi ni Tsuite" [{Explanation} About deterrence], http://www.clearing.mod.go.jp/hakusho_data/2010/2010/html/mc323000.html.

a result of repeated attacks, and that restoration back to the normal status is achieved quickly. Resilience is achieved by estimating the damage based on a detailed risk analysis, drawing up a business continuity plan beforehand according to the respective scenarios, and verifying as well as conducting training and exercises based on these plans, while at the same time, when damage is sustained, ensuring that IT systems continue to operate through means such as migrating to backup systems and enabling fallback operations, maintaining the provision of services at a minimal level, and implementing recovery measures quickly to restore operations to the normal status. The U.S. Department of Defense Cyber Strategy also establishes resilience as a means of deterrence in cyberspace in addition to "response" (deterrence by punishment) and "denial" (deterrence by denial). In addition, it also explains that in order to ensure that resilience functions effectively as a means of deterrence, it is necessary to cooperate with other ministries and agencies, as well as with private-sector actors including CII operators.[8] Efforts by the respective organizational units form the basis of the approach to cyber-resilience; however, when viewed from the perspective of national security, it is effective for the public and private sectors to join hands and for the country to work as one. In order to acquire deterrent capability through resilience, it is important to enhance restoration capacity in the event that damage is sustained in a large-scale cyberattack, through means such as building information-sharing systems for threat information and other data through public-private partnerships, and utilizing cyber exercises as an opportunity for establishing the procedures for measures implemented through public-private partnerships.

(3) The importance of public-private partnerships

As such, from the two perspectives of the characteristics of cyberspace and deterrence, we can see that in cyberspace, unlike the domains of land, sea, air, and space, private-sector actors play an extremely important role. Paradoxically, the more important private-sector actors are in cyberspace, the greater the importance of the role that state leadership fulfills in security in order to unify the direction of efforts by diverse private-sector actors toward ensuring security. In light of the fact that cyberwars are becoming a domain of battle between countries, and that the critical infrastructure of countries have become a perfect target for attacks, governments should not expect private-sector operators to work alone to defend critical infrastructure. For battles in cyberspace, the attackers who have the freedom of selecting the target, means, and timing of the attack, have an overwhelming advantage. To counter the attackers effectively, it is important for the various actors in the public and private sectors to cooperate and work as one to establish a system for coping with attacks, rather than for the defenders to respond individually to attacks.

2. Overview of Public-Private Partnership Systems for Cyber Defense in Japan

(1) Public-private partnership initiatives by the national government

(i) Japan's government-wide security policy promotion system and basic strategy

Japan's security policy was launched in 2000, triggered by the Y2K problem and the continued tampering with and hacking of the websites of central government ministries and agencies,[9] which

---

8 The Department of Defense, *The DoD Cyber Strategy*, (The Department of Defense, 2015), p. 11.

9 JPCERT Coordination Center, "Intanetto Sekyuriti no Rekishi, Dai 5 Kai 'Chuo Shocho Web Peji Kaizan Jiken'" [History of Internet Security, 5th session "Hacking of the websites of central government ministries and agencies"], http://www.jpcert.or.jp/tips/2007/wr071801.html.

occurred immediately after that. The government established the IT Security Office[10] under the auspices of the Cabinet Secretariat to perform the government's core function of implementing information security measures, and also developed a system for promoting government-wide cybersecurity policies. After that, it established the Information Security Policy Council[11] and the National Information Security Center (NISC)[12] in 2005. Furthermore, in January 2015, the Cyber Security Strategy Headquarters was established based on the Basic Act on Cybersecurity, while the former NISC was reorganized as the National center of Incident readiness and Strategy for Cybersecurity (NISC).

The First National Strategy on Information Security was drawn up in 2006 as the basic cybersecurity strategy for the country. This was followed by the Second National Strategy on Information Strategy drawn up in 2009, the Information Security Strategy for Protecting the Nation drawn up in 2010, and the Cybersecurity Strategy drawn up in 2013. The current Cybersecurity Strategy is based on the Basic Act on Cybersecurity enacted in 2014, and was approved by the Cabinet in July 2018.[13]

(ii) Initiatives related to the protection of critical infrastructure

(a) Overall

Information security measures for critical infrastructure began in 2000 when full-scale government-wide initiatives were launched, and the Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure[14] was established. This plan, aimed at protecting critical infrastructure from all attacks that could have a serious impact on citizens' lives and social and economic activities that involve the use of telecommunication networks and information systems, identifies seven relevant categories of critical infrastructure (telecommunications, finance, aviation, railroads, electrical power, gas, and government and administrative services), and prescribes five cyber-terrorism countermeasures that involve public-private cooperation: preventing damage, establishing and enhancing communication and coordination systems between government and the private sector, detection of cyberattacks and emergency response through government and private sector cooperation, establishing foundations of information security, and international cooperation. The Action Plan on Information Security Measures for Critical Infrastructures was approved by the Information Security Policy Council in December 2005, after which the Second Action Plan was approved in 2009, the Third Action Plan was approved in 2014, and the Fourth Action Plan was approved in 2017.

---

10 Cabinet Secretariat, "Jyoho Sekyuriti Taisaku Suishin Kaigi no Secchi ni Tsuite" [Establishment of the IT Security Office], https://www.kantei.go.jp/jp/it/security/suisinkaigi/0229suisinkaigi.html/

11 National center of Incident readiness and Strategy for Cybersecurity (NISC), "Jyoho Sekyuriti Seisaku Kaigi no Secchi ni Tsuite" [Establishment of the Information Security Policy Council], http://www.nisc.go.jp/conference/seisaku/pdf/kitei.pdf.

12 National center of Incident readiness and Strategy for Cybersecurity (NISC), "Jyoho Sekyuriti Senta no Secchi ni Kansuru Kisoku" [Regulations on the Establishment of the Information Security Center], http://www.nisc.go.jp/about/pdf/050420-kisoku.pdf.

13 National center of Incident readiness and Strategy for Cybersecurity (NISC), "Saiba Sekyuriti Senryaku (Heisei 30 Nen 7 Gatsu 27 Nichi)" [Cybersecurity Strategy (July 27, 2018)], http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf.

14 Information Security Measure Promotion Meeting, "Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure," http://www.kantei.go.jp/jp/it/security/taisaku/2000_1215/pdfs/txt3.pdf.

The current Fourth Action Plan on Information Security Measures for Critical Infrastructures[15] sets out 13 fields of critical infrastructure (telecommunications, finance, aviation, railroads, electrical power, gas, government and administrative services, medicine, water, logistics, chemistry, credit, petroleum), and establishes five areas of information security measures to be addressed during the period of the plan. These are: developing safety standards, etc., strengthening information-sharing systems, strengthening failure response systems, establishing risk management and coping mechanisms, and strengthening the protection infrastructure. The respective measures are being promoted.

(b) Information-sharing systems related to the protection of critical infrastructure

In promoting the protection of critical infrastructure, it is extremely important to build a public-private information-sharing system, and to share information related to threats and information security measures. To establish an information-sharing system, the Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure of 2000 prescribed the establishment of Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR) as an organization to fulfill the functions of sharing and analyzing information for CII operators and others.[16] As of the end of September 2017, a total of 18 CEPTOARs are in operation for 13 critical infrastructure domains; industrial organizations and others serve as secretariats, and information is shared between the government and other stakeholders with the aim of preventing service failures for critical infrastructure, preventing the spread of damage, ensuring prompt restoration of services, and preventing recurrence. Furthermore, in order to promote information sharing, the CEPTOAR-Council, comprising representatives of CEPTOARs set up in the respective domains of critical infrastructure, was established in 2009. This Council is engaged in the coordination and management of systems for providing information that is closely related to CII operators and others.[17]

With regard to the flow of information-sharing related to cyberattacks and IT failures, information is shared by the operator in question within the CEPTOAR it is affiliated with. At the same time, the information is also reported to the competent ministries and agencies of the critical infrastructure in question via the CEPTOAR secretariat (or directly), and then disseminated by the CEPTOAR-Council to the CEPTOARs of other fields. The National center of Incident readiness and Strategy for Cybersecurity (NISC) obtains information about failures and other matters related to the critical infrastructure from the competent ministries and agencies of the critical infrastructure (or from the operator in question during an emergency), and shares this information with ministries and agencies involved in disaster risk reduction, case resolution, and information security. It also disseminates the information to business circles outside the field of the critical infrastructure in question.

Alongside with close information-sharing within each CEPTOAR, which are established

---

15 Cybersecurity Strategy Headquarters, "Fourth Action Plan on Information Security Measures for Critical Infrastructures," https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf.

16 Information Security Measure Promotion Meeting, "Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure," http://www.kantei.go.jp/jp/it/security/taisaku/2000_1215/pdfs/txt3.pdf.

17 National center of Incident readiness and Strategy for Cybersecurity (NISC), "Jyoho Kyoyu Taisei no Kyoka" [Strengthening Information-sharing Systems], https://www.nisc.go.jp/active/infra/ shisaku2.html.

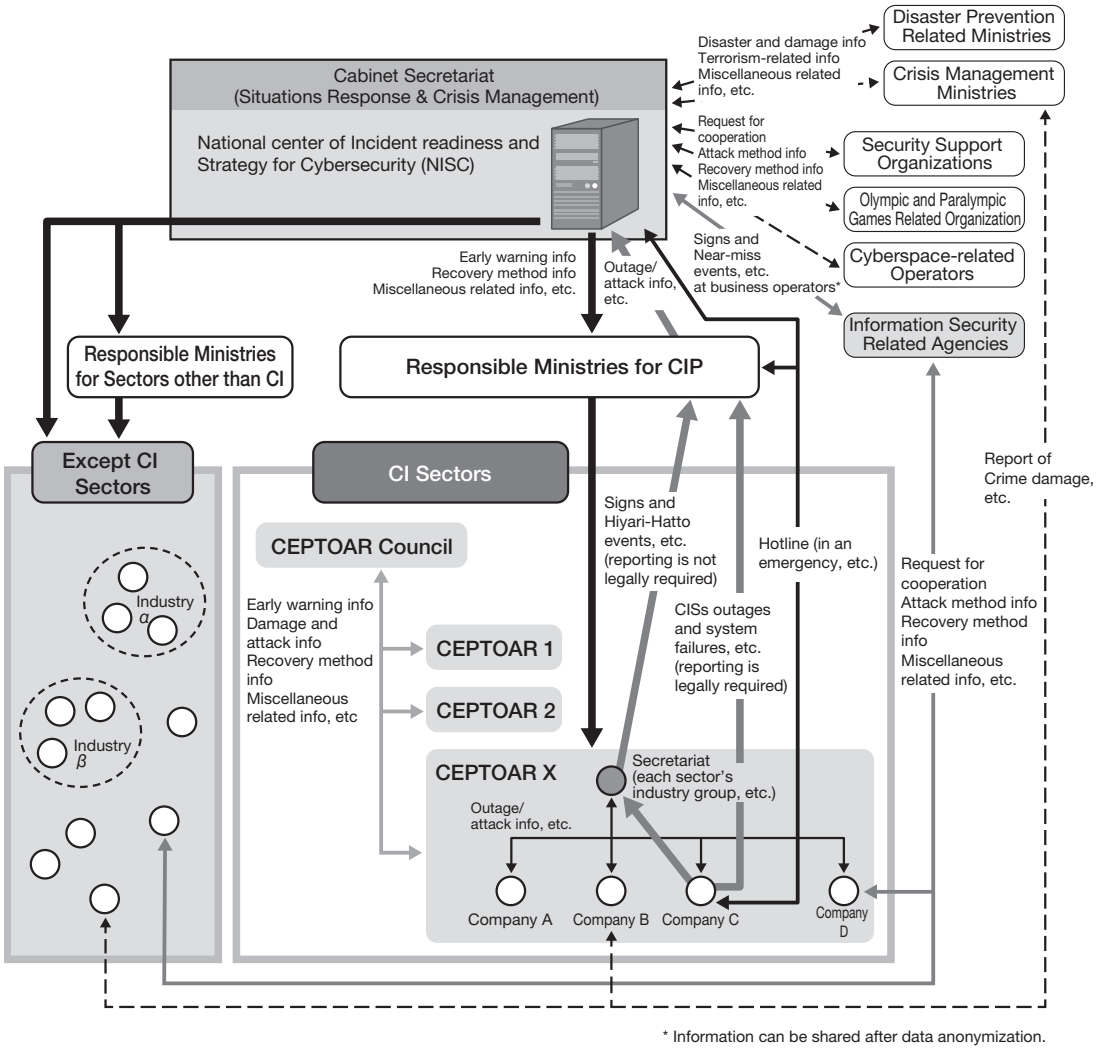
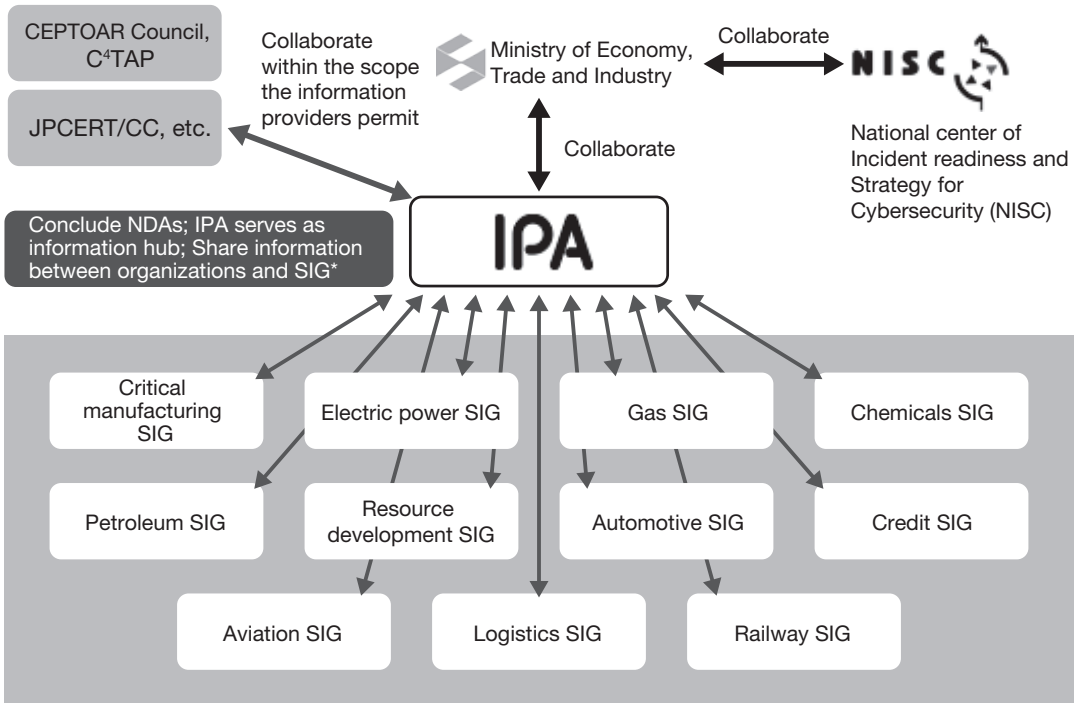


Figure 2 Information-sharing system centered around NISC

Source: Extracted from the Fourth Action Plan on Information Security Measures for Critical Infrastructures

along the lines of the various domains of critical infrastructure, the system is structured such that information is also consolidated by NISC according to the degree of importance and urgency, and disseminated to the relevant organizations.

The Information-technology Promotion Agency (IPA) launched the Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) in 2011 in cooperation with the Ministry of Economy, Trade and Industry (METI), with the aim of preventing the spread of damage in the event of a cyberattack. This initiative is intended to serve as a space for information-sharing and early response, centered around the manufacturers of equipment used for critical infrastructure. Under the initiative, an information-sharing system has been established by 227 participating organizations, creating 11 Special Interest Groups (SIG, collectives of members from similar industries). IPA has concluded non-disclosure agreements (NDA) with the participating



*SIG: Acronym for "Special Interest Group"

Figure 3 Information-sharing through the Initiative for Cyber Security Information sharing Partnership of Japan

Source: Extracted from the IPA website

organizations, and is engaged in the sharing of information on cyberattacks.[18]

Taking reference from the information Sharing and Analysis Center (ISAC), which is an industry-based information-sharing and analysis organization in the United States, Telecom-ISAC was launched in 2002 primarily for communications carriers, while the Financials ISAC was established in 2014. These organizations share information related to cyberspace in their respective fields.

(C) Implementation status of cross-sectoral exercises

To respond appropriately to IT failures and cyberattacks, it is vital to repeatedly validate the effectiveness of information-sharing systems, emergency response procedures, and business continuity plans, as well as to improve upon them, through exercises and training. From this perspective, cross-sectoral exercises were launched in FY2006 with the aim of improving the functions of public-private partnership systems related to the protection of critical infrastructure. In the inaugural exercise held in FY2006, "research-based exercises" and " tabletop exercises" were held, while annual "functional exercises" have been held since FY2007. The scenarios for the exercises are revised every year, and the difficulty of the scenarios has been raised gradually since

[18] Information-technology Promotion Agency (IPA), Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP), https://www.ipa.go.jp/ security/J-CSIP/.

the launch of the exercises, which have covered coping with a DDoS attack (FY2007), IT failure (FY2008), wide-area power outage (FY2009), large-scale telecommunications failure (FY2010), complex situations involving electricity and gas (FY2011), complex failures of electricity and telecommunications compounded by IT incidents (FY2012), and large-scale information security incidents (FY2013).[19, 20] About 90 representatives from about 10 domains of critical infrastructure participated[21] in the first "tabletop exercise" held in 2006. This has since expanded in scale to participation by about 2,600 people from 13 domains of critical infrastructure[22] at the 12th exercise held in FY2017.

The implementation of cross-sectoral exercises has produced significant results, bringing public- and private-sector stakeholders in public infrastructure together under one roof to conduct verification on the effectiveness of cooperation between the public and private sectors as well as between operators, and at the same time, strengthening response capability within the respective fields by facilitating a common recognition of cross-sectoral threats and understanding of the response situation in other fields, and producing ideas for measures aimed at effective information-sharing between the public and private sectors.

(2) Initiatives by the Ministry of Defense and Self-Defense Forces

The Ministry of Defense, alongside with the National Police Agency, Ministry of Internal Affairs and Communication, Ministry of Economy, Trade and Industry, and Ministry of Foreign Affairs, as members of the Cybersecurity Strategy Headquarters, are engaged in cross-governmental efforts led by the NISC, including participating in exercises on coping with cyberattacks, personnel exchanges, and information-sharing on cyberattacks. In addition, it dispatches personnel to the Cyber incident Mobile Assistance Team (CYMAT), which provides swift and flexible support through cooperation across government ministries and agencies, and contributes in other ways to government-wide initiatives.[23]

As a part of its own initiatives, the Ministry of Defense (MOD) and Self-Defense Forces (SDF) established a new Cyber Defense Group under the SDF Command Control Communication Computers Systems Command in March 2014, through which it operates a 24-hour posture for supporting the information and communications network of the Ministry of Defense and Self-Defense Forces and responding to cyberattacks. The respective Self-Defense Forces also monitor and protect their own information systems through the System Protection Unit of the Ground

---

19 National center of Incident readiness and Strategy for Cybersecurity (NISC), "2013 Nendo Jyuyo Infura no Bunya Odanteki Enshu ni kansuru Chosa no Kekka ni Tsuite" [Results of the Survey on the FY2013 Cross-Sectoral Exercise for Critical Infrastructure], https://www.nisc.go.jp/active/infra/pdf/bunyaoudan_2013.pdf.

20 National center of Incident readiness and Strategy for Cybersecurity (NISC), "Jyuyo Infura ni okeru Bunya Odanteki Enshu – [CIIREX 2010] no Jisshi ni Tsuite" [Cross-Sectoral Exercises for Critical Infrastructure – Implementation of CIIREX 2010], https://www.nisc.go.jp/press/pdf/ciirex2010_press.pdf.

21 National center of Incident readiness and Strategy for Cybersecurity (NISC), "2010 Nendo Jyuyo Infura no Bunya Odanteki Enshu ni kansuru Chosa no Kekka ni Tsuite" [Results of the Survey on the FY2010 Cross-Sectoral Exercise for Critical Infrastructure], https://www.nisc.go.jp/active/infra/pdf/bunyaoudan_2010.pdf.

22 National center of Incident readiness and Strategy for Cybersecurity (NISC), "Jyuyo Infura 13 Bunya wo Taisho ni Sabisu Shogai Taio no tame no Saiba Enshu wo Jisshi – 2017 Nendo Bunya Odanteki Enshu" [Implementation of Cyber Exercises for Responding to Service Outages in the 13 Critical Infrastructure Domains – FY2017 Cross-Sectoral Exercise], http://www.nisc.go.jp/active/infra/pdf/bunya_enshu2017gaiyou.pdf.

23 Ministry of Defense, *Defense of Japan 2017*, (Nikkei Printing Inc., 2017), p. 359.

Self-Defense Force, the Communication Security Group of the Maritime Self-Defense Force, and the Computer Security Evaluation Squadron of the Air Self-Defense Force. The MOD and SDF are working to enhance systems, including improving military facility to withstand attacks, strengthening information-gathering as well as research and analysis functions, and developing a training environment for actual combat, so as to cope effectively with cyberattacks on their information systems and networks.[24]

As for international initiatives, the MOD and SDF have established the Cyber Defense Policy Working Group (CDPWG) in partnership with Japan's ally, the United States, and hold conferences on topics such as promoting policy consultation, facilitating closer information-sharing, promoting joint exercises, and cooperating to develop and secure experts. They also engage in exchanges of opinions with countries such as the UK, Australia, and Estonia through the establishment of cyber-consultations among the defense authorities. At the same time, they have cooperated with NATO to set up NATO-Japan Cyber Defense Staff Talks, and are engaged in other efforts to build up its cooperative relationship with NATO, such as by participating as an observer in Cyber Coalition, Locked Shields and other cyber defense exercises organized by NATO.

In Japan, efforts are underway to improve the ability of the MOD and SDF, as well as the defense industry, to cope with cyberattacks, through initiatives such as joint exercises, and the establishment of the Cyber Defense Council in 2013, comprising about 10 companies with a deep interest in cyber security as its core members.[25]

(3) Summary

Japan's cybersecurity measures were launched in response to the Y2K problem. To date, a wide range of measures have been implemented steadily in the areas of governmental organizations, strategy formulation, and development of legal systems. These include the establishment of the Cybersecurity Strategy Headquarters and the National center of Incident readiness and Strategy for Cybersecurity, the formulation of cybersecurity strategies, and the enforcement of the Basic Act on Cybersecurity. With regard to initiatives related to the protection of critical infrastructure, it has also strengthened public-private partnership systems based on the respective action plans, through the establishment of information-sharing systems and cross-sectoral exercises. The MOD and SDF have established new dedicated cyber defense units and cooperated with the government as a whole on various initiatives, while at the same time building international cooperative relationships with allies and friendly countries such as the United States.

3. Estonia's Initiatives, Comparison with Japan, and Feasibility of Implementation in Japan

Since it gained independence from the Soviet Union in 1991, Estonia has advanced efforts to utilize information and communications technology at the national level with a view to realizing an e-government. The Estonian government has decided to concentrate its resources on information and communications technology in order to achieve economic growth in an efficient manner, in light of the country's limited natural resources. This approach is supported by the citizens. As the country needed to develop social infrastructure such as roads and schools in the early stages

[24] Ministry of Defense, "Jieitai no Saiba Kogeki e no Taio ni Tsuite" [SDF's Response to Cyberattacks], http://www.mod.go.jp/j/publication/net/shiritai/cyber/index.html#a2.

[25] Ministry of Defense, *Defense of Japan 2017*, p. 361.

of its independence, it poured its efforts into creating an environment for using the Internet. It has even been said that the introduction of computers was prioritized over the repair of roofs in schools.[26] From 1996 to 2000, it implemented the "Tiigrihüpe" ("Tiger Leap") project with the aim of overtaking developed countries through the use of information and communications technology. In addition to building environments to enable Internet use in all schools, it also promoted the use of the Internet across a wide range of public services and banking processes. In 2001, it built X-Road, a data exchange layer that serves as an information and communications infrastructure for governmental organizations, thereby enhancing efficiency in the exchange and sharing of information among government ministries and agencies. The eID card, which forms the basis for personal authentication and electronic signature, has been distributed to all citizens aged 15 and above since 2002. In 2005, Estonia became the first in the world to conduct local government elections through electronic voting on the Internet.[27] As a result of such intensive investment in information and communications technology, Estonia's global ranking for the penetration of information and communications technology rose from 33rd place in 1999[28] to 17th place in 2017.[29] (Estonia comes second after the Republic of Korea in the rate of increase of its ranking during this period of time.)

Against this background, Estonia was hit by a large-scale cyberattack on its critical infrastructure in April 2007. Drawing lessons from this incident, Estonia has taken strong steps to promote cybersecurity initiatives, and the various measures it has put in place are exceedingly advanced even among the NATO member countries. The Global Cybersecurity Index (GCI) 2017 report published by the International Telecommunication Union (ITU) positioned Estonia in the fifth place globally among 193 countries, and first in the Europe region.[30] (The GCI assesses countries based on the five pillars of legal measures, technical measures, organizational measures, capacity building, and cooperation. Globally, Singapore ranks first, the United States ranks second, and Japan ranks 11th.) In this GCI report, Estonia was highly rated for its efforts after the large-scale cyberattack of 2007 to develop its legal system so as to ensure the provision of a minimal level of services even when the Internet is shutdown, and to promote organizational measures for swift response to attacks.[31]

Estonia has also established a Cyber Command in its regular military forces, as well as a Cyber Defense Unit comprising volunteers from the private sector under the auspices of the Estonian Defense League, a paramilitary organization. With regard to national defense against cyberattacks, the country has developed a unique military-civilian partnership system that is not seen in any other country. Based on these facts, we can see that Estonia is a democracy that has put nationwide efforts toward the realization of an e-government through the use of the Internet,

---

26 Allikivi, Raul, and Yoji, Maeda, *Miraigata Kokka Estonia no Chosen – Denshi Seifu ga Hiraku Sekai* [Challenges Faced by the Future-Oriented State of Estonia – Opening Up a New World Through e-Government], (Impress R&D, 2016)

27 Ibid., pp. 52-53.

28 United Nations Conference on Trade and Development, *Information and Communication Technology (ICT) Development Indices*, (Geneva, UNCTAD Secretariat, 2003), p. 44.

29 International Telecommunication Union, *Measuring the Information Society Report 2017 Volume1*, (Geneva, ITU, 2017), p. 31.

30 International Telecommunications Union, *Global Cybersecurity Index (GCI) 2017*, p. 17.

31 Ibid., p. 36.

as well as a country that fell victim to a large-scale cyberattack that had a severe impact on the critical infrastructure of the country. It has strongly promoted various measures based on the lessons drawn, placing the focus of its cyber defense system on public-private and military-civilian partnerships rather than on the military and bureaucracy, and has been successful in developed a national cybersecurity system.

The population of Estonia is about 1.32 million, which is approximately one-hundredth of the population of Japan. From the perspective of national scale, there may be critics who feel that Estonia is not an appropriate subject in drawing a comparison of the cybersecurity policies with Japan. However, Estonia enjoys the merits of having few stakeholders who hold a stake, as well as ease of promoting new measures, because it is a country with a small population. It has taken advantage of these precise merits to promote e-government measures, and at the same time, advanced new cybersecurity policies. As these leading initiatives that take advantage of the merits of being a small country offer many implications, such as examples of successes as well as failed measures, they can be fully utilized when considering future initiatives for Japan's cybersecurity measures.

This section looks at Estonia's cyber defense initiatives, placing particular focus on public-private partnership in the protection of critical infrastructure, and provides an overview of the various measures based on the following six classifications: cybersecurity strategy, legal systems, public-private partnership organizations and information sharing systems, risk analysis and business continuity plans, cyber exercises, and national defense strategy and organizations. It carries out a comparison with Japan, and discusses the feasibility of implementing these measures in Japan.

In Estonia's laws and strategy documents, "vital service" is a term used in relation to the protection of critical infrastructure. Hence, in deference to the usage of the term in Estonia, this section will apply the term "vital service" in regard to the protection of critical infrastructure in Estonia.

(1) Cybersecurity strategy

(i) Estonia's national security strategy and cybersecurity strategy

The most important document related to Estonia's national security is the National Security Concept of Estonia, which was revised in 2010 base on lessons drawn from the large-scale cyberattack of 2007.[32, 33] With regard to the environment in Estonia, information and communications systems are becoming increasingly important in society, and vital services are also becoming increasingly dependent on information and communications systems; hence, a vital service outage will have severe impact on society. In light of this, the National Security Concept points to the importance of ensuring the security of information and communications systems, and positions the securing of

[32] Christian Czosseck, Rain Ottis and Anna-Maria Taliharm, Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security, (NATO CCD COE), p. 59. http://ccdcoe.org/articles/2011/Czosseck_Ottis_Taliharm_Estonia_After_the_2007_Cyber_Attacks.PDF

[33] Estonia published its revised National Security Concept of Estonia 2017 in October 2018 after this paper was written. http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017.pdf.

resilience for vital services as one of the important elements of national defense.[34] Furthermore, it also clearly sets out measures aimed at securing the resilience of vital services, including improving restoration capacity when damage is incurred, prior preparation of reserve supplies, formulation of action plans, and continued evaluation of risk analysis.[35]

After the large-scale cyberattack of 2007, the Estonian Ministry of Defense established the Cyber Security Strategy Committee through cooperation between the Ministry of Education and Research, Ministry of Justice, Ministry of Economic Affairs and Communications, Ministry of the Interior, and Ministry of Foreign Affairs, and promoted the formulation of a national Cyber Security Strategy. In May 2008, Cyber Security Strategy 2008 – 2013 was drawn up.[36] In 2011, the authority for the inter-agency coordination of cybersecurity policies was transferred from the Ministry of Defense to the Ministry of Economic Affairs and Communications, and the responsibility of preparing the cybersecurity policies of Estonia fell to the Ministry of Economic Affairs and Communications its subordinate organization, the Estonian Information System Authority ("Riigi Infosüsteemi Amet" or RIA. Discussed in detail later.)

The current Cyber Security Strategy is the Cyber Security Strategy 2014 – 2017, published by the Estonian Ministry of Economic Affairs and Communications, and it is positioned as the basic document covering cybersecurity in Estonia. This Strategy is structured as follows: Chapter 1: Analysis of current situation (Sectoral progress; Trends; Challenges), Chapter 2: Principles of ensuring cyber security, Chapter 3: General objective of the strategy for 2017; Chapter 4: Subgoals; Chapter 5: Parties related to the strategy. It places focus on the areas of maintaining vital services, effective response to cybercrimes, and progress of national defense capability.[37] The main goal of this Strategy is to secure safety in cyberspace by enhancing cybersecurity capability and raising awareness of cyber threats among the population.[38] This Strategy then sets out five subgoals for achieving the main goal: ensuring the protection of information systems underlying important services; enhancing of the fight against cybercrime; development of national cyber defence capabilities; managing evolving cyber security threats; and, developing cross-sectoral activities.[39]

The Cyber Security Strategy is characterized by the fact that it positions "Ensuring the protection of information systems underlying important services" as the issue of the highest priority. The Strategy lays out the following measures for achieving this subgoal: ensuring alternative solutions for important services, managing cross-dependency between important services, ensuring the security of ICT infrastructure and services, managing cyber threats to the public and private sector, introducing a national monitoring system for cyber security, ensuring digital continuity of the state, and promoting international cooperation in the protection of the infrastructure of critical information.

---

34 Parliament of Estonia, *National Security Concept of Estonia*, May 12, 2010, pp. 13-14. http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia.pdf

35 Ibid., p. 17.

36 Tikk, *International Cyber Incidents: Legal Consideration*, pp. 29-30.

37 Ministry of Economic Affairs and Communication, *Cyber Security Strategy 2014-2017*, 2014, p. 6.

38 Ibid., p. 8.

39 Ibid., p. 8.

(ii) Comparison with Japan's cybersecurity strategy

Comparing Estonia's Cyber Security Strategy 2014 – 2017 and Japan's Cybersecurity Strategy (approved by the Cabinet in July 2018), we can see that the two countries are generally in accord with regard to their recognition of the threats facing cyberspace, recognition of the benefits that cyberspace has given to society, and the aims and goals of the respective cybersecurity strategies. However, the two countries differ from the perspective of the priority they place on measures related to the protection of critical infrastructure.

Japan's Cybersecurity Strategy establishes the promotion of cybersecurity that underpins the creation of new values as the first measure within the four policy approaches (Enabling socio-economic vitality and sustainable development; Building a safe and secure society for the people; Contribution to the peace and stability of the international community and Japan's national security; Cross-cutting approaches to cybersecurity), and places the emphasis on enhancing socio-economic vitality and sustainable development in Japan alongside with the growing and widespread use of IoT systems.[40]

While Estonia's Cyber Security Strategy places "Ensuring the protection of information systems underlying important services" as the issue of top priority in the Cyber Security Strategy, Japan's Cybersecurity Strategy positions the protection of critical infrastructure as the fifth initiative[41] out of a total of 16 measures, and covers it alongside with other measures. It may be argued that the order of the measures set out in Japan's Cybersecurity Strategy does not reflect their degree of importance. However, we could say that Estonia differs greatly from Japan in that it clearly positions the protection of vital services as the top priority, and has established the protection of vital services at the center of its approach to cybersecurity.

Table 1 Comparison of cybersecurity strategies of Estonia and Japan

	Estonia	Japan
Most important issues	1. Ensuring the protection of information systems underlying important services 2. Enhancing of the fight against cybercrime 3. Development of national cyber defence capabilities 4. Managing evolving cyber security threats 5. Developing cross-sectoral activities	1. Enabling socio-economic vitality and sustainable development 2. Building a safe and secure society for the people 3. Contribution to the peace and stability of the international community and Japan's national security 4. Cross-cutting approaches to cybersecurity
Protection of critical infrastructure	Positioned as first item among five subgoals (first item among 22 measures)	Positioned as second item among four policy approaches (fifth item among 16 measures)
Order of priority for each measure	Description corresponding to degree of priority (explicit)	Description alongside with other policy approaches (not explicit)

Source: Drawn up based on the cybersecurity strategies of Estonia and Japan

40 *Cybersecurity Strategy*, approved by the Cabinet on July 27, 2018, pp. 13-42.

41 Ibid., pp. 13-42.

(iii) Feasibility of implementation in Japan

The formulation of Japan's Cybersecurity Strategy is mandatory in accordance with the provisions of Article 12 of the Basic Act on Cybersecurity, and the Strategy is drafted by the Cybersecurity Strategy Headquarters. While there are no specific provisions stipulating the contents to be included in the Cybersecurity Strategy, it is possible to explicitly set out the order of priority for the respective policy approaches in the same way as Estonia's Cyber Security Strategy.

The viewpoint of actively using cyberspace as a means for economic development is an important one. However, cyberspace is established through the maintenance of networks by communications carriers and a stable supply of electricity that underpins that. Accordingly, we could say that economic development based on the use of cyberspace is first realized through the stable operation of the country's critical infrastructure. As indicated by Estonia's Cyber Security Strategy, Japan's Cybersecurity Strategy should also position measures to protect critical infrastructure from large-scale cyberattacks as the issue of the highest priority.

(2) Legal systems

(i) Legal systems related to the protection of vital services in Estonia

In Estonia, there are no specific laws for cybersecurity like Japan's Basic Act on Cybersecurity.[42] Instead, the protection of vital services is clearly provided for under the Emergency Act. This Act, revised in 2009, clearly sets out 43 types of vital services and the competent ministries and agencies for these services.[43] The number of vital services, which far exceeds the 13 domains of critical infrastructure established by Japan, is due to the detailed categorization and listing of the respective vital services in Estonia, and there are many vital services in Estonia's list that have not been defined as critical infrastructure in Japan. (For example, ports, shipping traffic, roads, emergency aid messages, and environmental monitoring of radiation, atmosphere and oceans, to state a few.)

At the Cybersecurity Conference organized by the Estonian Information System Authority ("Riigi Infosüsteemi Amet" or RIA) in 2013, vital service providers were of the view that it is necessary to develop a clearly defined legal system for regulation corporations, such as the actions that vital service providers should take when a large-scale cyberattack occurs, and the minimum level of services that should be maintained by vital service providers in order to sustain social life in the event of an emergency. To that end, they recommended revision to the law. Consequently, the Emergency Act was revised in July 2017 and vital services were organized into 14 categories (electricity supply, gas supply, fuel supply, national roads, fixed-line telephones, mobile phones, data transmission services, digital identification and digital signing, emergency care, payment services, cash circulation, district heating, local roads, and water supply and sewage). At the same time, the responsibilities of the competent ministries and agencies as well as of the vital service providers were clearly defined.[44]

---

[42] Estonia enacted the Cybersecurity Act in May 2018, after this paper was written. Government of Estonia, Emergency Act passed 09.05.2018. https://www.riigiteataja.ee/en/eli/523052018003/consolide.

[43] Government of Estonia, *Emergency Act passed 15.06.2009, Art.34*, https://www.riigiteataja.ee/en/eli/525062014011/consolide.

[44] Government of Estonia, *Emergency Act passed 08.02.2017, Art.36*, https://www.riigiteataja.ee/en/eli/513062017001/consolide.

Article 38 of the Emergency Act sets out the following responsibilities of vital service providers: (1) Prepare the continuity risk assessment and plan of the vital service; (2) Implement measures that prevent interruptions of vital services; (3) Ensure the capability to guarantee the continuity of and to quickly restore the services; (4) Notify the authority organizing the continuity of the vital service in the event of an emergency; (5) Participate in resolving an emergency according to the emergency response plan; (6) Provide information to the competent authority and other relevant parties; (7) Organize exercises in order to verify the continuity of the vital service ; and others. Furthermore, Article 37 of the same law sets out the following responsibilities of the competent ministries and agencies of vital services: (1) Coordinate the ensuring of the continuity of the vital service; (2) Advise providers of vital services; (3) Exercise supervision over ensuring the continuity of vital services; (4) Approve the continuity risk analyses and plans of providers of vital services; (5) Coordinate the resolution of an emergency; (6) Prepare an emergency response plan; and others. It also clearly sets out the continuity requirements that the competent ministries and agencies demand of vital service providers in relation to the continuity of their vital service operations: (1) The contents of the vital services for which functions should be maintained; (2) Service levels that should be maintained; (3) Requirements for the prevention of interruption; (4) Time permitted for interruption; (5) Service failures that constitute an emergency; (6) Reporting when an emergency arises; and others.

(ii) Comparison with Japan's legal system

Japan's Basic Act on Cybersecurity sets out in Article 3 (Basic Principles) that "the promotion of the Cybersecurity policy must be carried out with the intent to produce active responses to threats against Cybersecurity through coordination among multiple stakeholders, including the national government, local governments, and critical information infrastructure (CII) Operators," and in Article 6 (Responsibility of CII Operators) that "In accordance with the Basic Principles and for the purpose of stable and appropriate provision of their services, CII Operators are to make an effort to: deepen their awareness and understanding of the critical value of Cybersecurity; ensure Cybersecurity voluntarily and proactively; and cooperate with the measures on Cybersecurity taken by the national government or local governments." Hence, the law only provides for efforts to cooperate with measures set out by the government. For this reason, although NISC promotes various measures by positioning the Action Plan on Information Security Measures for Critical Infrastructures as the basic document for information security measures related to critical infrastructure, CII operators are not legally obligated (legal duty) to be involved in these measures based on the Basic Act on Cybersecurity.

Estonia's Emergency Act clearly sets out the responsibilities of vital service providers, including risk analysis and formulation of business continuity plans, measures to prevent interruption to vital services, and reporting in the event of an emergency. It differs from Japan in the sense that it imposes a certain degree of legal duty on vital service providers to ensure cybersecurity. Moreover, there is a sense that vital service providers who are regulated by law are more involved in the enactment of legislation for vital service providers, such as criticizing the government for inadequacies in the Emergency Act and promoting revisions to the law.

Table 2 Comparison of legal systems of Estonia and Japan47

	Estonia	Japan
Legal framework	• Provided for in the Emergency Act * Discussions are ongoing about the need for a basic law on cybersecurity[45]	• Basic Act on Cybersecurity • Laws regulating the respective industries, etc.
Responsibilities of CII operators	• Prepare risk analysis and business continuity plan • Implement measures that prevent interruptions of vital services • Ensure the capability to ensure the continuity, etc. • Notify the competent authorities in the event of an emergency • Participate in resolving an emergency according to the emergency response plan • Provide information to the competent authority • Organize exercises to verify the business continuity plans	• Voluntarily and proactively put effort into ensuring cybersecurity • Cooperate on cybersecurity measures implemented by the government and other entities
Responsibilities of the government and competent ministries and agencies	• Coordinate the ensuring of the continuity of the vital service • Advise providers of vital services • Exercise supervision over ensuring the continuity of vital services • Approve the continuity risk analyses and plans • Coordinate the resolution of an emergency • Prepare an emergency response plan	• Promotion of the establishment of standards, exercises and training, sharing of information, and other voluntary initiatives related to cybersecurity by CII operators, as well as the implementation of other necessary measures.

Source: Drawn up based on Estonia's Emergency Act and Japan's Basic Act on Cybersecurity

(iii) Feasibility of implementation in Japan

With regard to regulations based on laws for ensuring the security of critical infrastructure, in addition to the Basic Act on Cybersecurity, it is possible to reexamine the regulations through revision to the laws governing the respective industries, which are under the jurisdiction of each competent ministry and agency of the critical infrastructure. As for the implementation of cybersecurity policies, strengthening regulations on all matters through the application of the law could hinder free and flexible activities by corporations, and may not necessarily be the right thing to do. In particular, the frameworks for sharing of information between the public and private sectors in Japan have developed without the enforcement of any legally binding force. Hence, it is not necessary to re-establish systems based on law to regulate such mature systems that have developed through voluntary efforts.

However, there is a need to develop law-based systems to mandate the implementation of risk analyses and formulation of business continuity plans by CII operators, so as to provide assurance for matters that form the foundation of the protection of critical infrastructure that could have a severe impact on citizens' lives and socio-economic activities, or in other words, to ensure the provision of the minimal level of services in the event of critical infrastructure outage, as well as to ensure the swift restoration of services when operations are interrupted.

45 The Cybersecurity Act was enacted in May 2018 after this paper was written.

(3) Public-private partnership organizations and information-sharing systems

(i) Estonia's public-private partnership organizations and information-sharing system

In 2009, the Cyber Security Council was added to the Security Committee of the Estonian government. It was tasked with promoting strategic cooperation between the ministries and agencies, and carrying out supervision to ensure that the goals set out in the Cyber Security Strategy were achieved. In 2010, the responsibility of formulating cybersecurity policies, which had until then been the job of the Ministry of Defense, was transferred to the Ministry of Economic Affairs and Communications. Alongside with this, the Estonian Information System Authority ("Riigi Infosüsteemi Amet" or RIA) was established as the agency responsible for the implementation of Estonia's cybersecurity policies.

The primary duties of the RIA[46] are as follows:

- To monitor the information systems of vital services and implement security measures
- To engage in organizational security activities on information systems of governmental organizations and critical infrastructure
- To deal with security incidents affecting computer networks in Estonia
- To supervise the situation of compliance with the standards of security measures for the information systems of governmental organizations
- To maintain and manage the information systems of governmental organizations and the information and communications infrastructure (X-Road)
- To carry out coordination in relation to maintaining the functions of the public key infrastructure (PKI)
- To carry out coordination in relation to the development of information systems for governmental organizations and participation in international projects
- To participate in the activities of the European Union (EU)
- To participate in various activities pertaining to the legal systems, policies, strategies, and development in relation to cybersecurity

RIA, in comparison with its predecessor, the former Estonian Informatics Center, has greater authority over the protection of the country's information and communications infrastructure, and is also responsible for supervision to ensure that information systems related to vital services are secure.[47] The Critical Information Infrastructure Protection (CIIP) is established within the RIA with the aim of protecting vital services. It is responsible for the protection of public and private information systems that are related to the maintenance of the functions of vital services.[48] CIIP is the main department in RIA that conducts general risk evaluation in relation to vital services, as well as formulates national emergency response plans in preparation for the event of a large-scale cyber incident. In 2010, it conducted a mutual dependency survey for vital services, and clearly established the security requirements for the critical information systems that are necessary for the country to function.[49] The supervision of all services in the respective fields of vital services comes under the charge of the competent ministries and agencies for the vital services, as before.

---

46 Information System Authority, https://www.ria.ee/en/about-estonian-information-system-authority.html.

47 Government of Estonia, *Status of the Information System Authority, Art.8*, https://www.ria.ee/public/RIA/Dokumendid/Statutes_of_RIA.pdf.

48 Critical Information Infrastructure Protection, https://www.ria.ee/en/ciip.html.

49 Ministry of Economic Affairs and Communication, Cyber Security Strategy 2014-2017, 2014, p. 2.

However, matters related to ensuring cybersecurity for information systems that make up the vital services are directly supervised by RIA. This system makes is possible to consolidate the various information on the information infrastructure that supports vital services, which had previously been scattered across the competent ministries and agencies, under the CIIP of RIA, making it possible to effectively and efficiently perform tasks that are related to the identification and supervision of vital service providers who are lagging behind in the implementation of security measures.

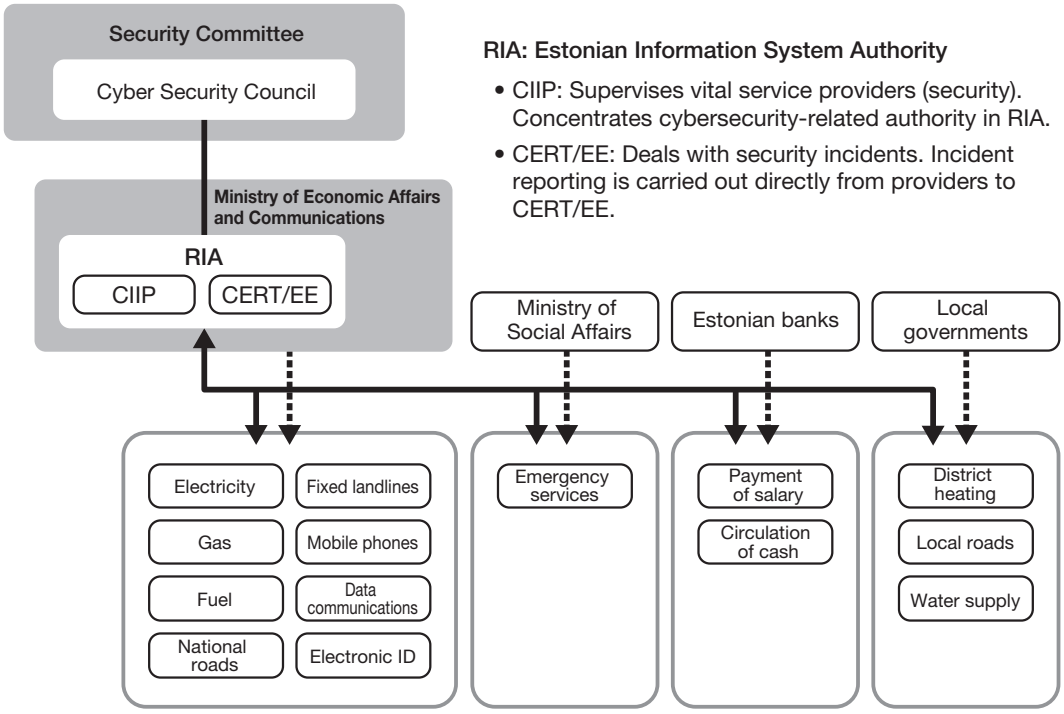


Figure 4 Relationship between RIA, the competent ministries and agencies of vital services, and vital service providers

Source: Drawn up based on the RIA website and the Emergency Act

With regard to the information-sharing system, the Estonian Computer Emergency Response Team (CERT-EE) is established within the RIA. Its scope of work includes incident handling for information systems related to vital services, notification of alert information, and providing support for the relevant organizations. The Security Measures for Information Systems of Vital Services and Related Information Assets[50] prescribes, as one of the enforcement rules of the Emergency Act, that in the event of a serious security incident, vital service providers are required to notify RIA and report on post-incident measures.

[50] Republic of Estonia Information System Authority, *Security measures for information systems of vital services and related information assets*, https://www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf.

(ii) Comparison with Japan's public-private partnership organizations and information-sharing systems

With regard to public-private partnership organizations, Japan's core organization is the NISC. Its responsibilities[51] are as follows:

- Monitoring and analysis of illegal activities on the information systems of all administrative departments
- Investigations to uncover the cause of serious events that could impede efforts to ensure cybersecurity in all administrative departments
- Offering the necessary advice, information, and other forms of assistance for ensuring cybersecurity in all administrative departments
- Carrying out the necessary audits in relation to ensuring cybersecurity in all administrative departments
- Other administrative work pertaining to the planning, drafting, and overall coordination needed for the standardized maintenance of measures for all administrative departments, in relation to ensuring cybersecurity

Table 3 Comparison of the public-private partnership organizations and information-sharing approaches of Estonia and Japan

	Estonia	Japan
Public-private partnership promotion organizations	Estonian Information System Authority ("Riigi Infosüsteemi Amet" or RIA), under the Ministry of Economic Affairs and Communications	National center of Incident readiness and Strategy for Cybersecurity (NISC)
Supervision of CII operators	Has direct supervision authority (Only for areas related to ensuring security)	Does not have supervision authority (Advice and overall coordination of competent ministries and agencies)
Responsibilities	• To monitor the information systems of vital services • To engage in organizational security activities on information systems of governmental organizations and critical infrastructure • To deal with security incidents • To supervise the situation of compliance with the standards of security measures for the information systems of governmental organizations • To maintain and manage the information systems of governmental organizations • To maintaining the functions of the public key infrastructure (PKI) • To participate in international projects and EU activities • To participate in various activities pertaining to the legal systems, policies, strategies, and development in relation to cybersecurity	• Monitoring and analysis of illegal activities on the information systems of all administrative departments • Investigations to uncover the cause of serious events that could impede efforts to ensure cybersecurity in all administrative departments • Offering the necessary advice, information, etc. for ensuring cybersecurity in all administrative departments • Carrying out the necessary audits in relation to ensuring cybersecurity in all administrative departments • Other administrative work pertaining to the planning, drafting, and overall coordination needed for the standardized maintenance of measures for all administrative departments, in relation to ensuring cybersecurity

Source: Drawn up based on the RIA website and the Order for the Organization of the Cabinet Secretariat

[51] National center of Incident readiness and Strategy for Cybersecurity (NISC), "Order for the Organization of the Cabinet Secretariat (Order No. 219 of 1957)," http://www.nisc.go.jp/law/pdf/soshikirei.pdf

As described above, NISC is engaged in planning and drafting work related to ensuring cybersecurity, and promotes measures through the overall coordination of the competent ministries and agencies of critical infrastructure. Under this system, the competent ministries and agencies of the respective critical infrastructure supervise CII operators based on the laws that govern the respective sectors.

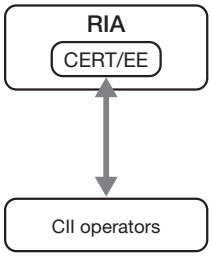
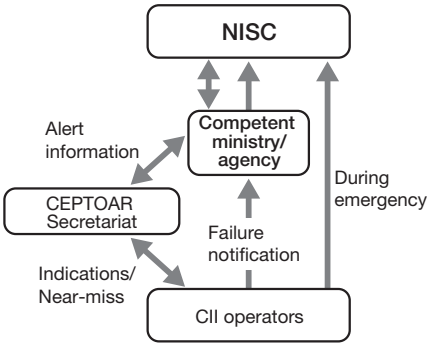
Comparing Japan's NISC and Estonia's RIA, we can see a significant difference in the sense that RIA has the authority to supervise vital service providers with regard to information systems, while NISC does not have direct authority to supervise CII operators.

With regard to the information-sharing systems, Japan has established a CEPTOAR for each domains of critical infrastructure to fulfill the functions of sharing and analyzing information in each of the domains. In contrast, Estonia does not have an organization for information-sharing and analysis for each domain of vital services; instead, this function is served primarily through the direct relationship between RIA and vital service providers. In Japan, as there are many corporations within each domain of critical infrastructure, there is a mature information-sharing and cooperation relationship between corporations within each CEPTOAR, followed by the maturing of the cooperative relationship between the public sector and the CEPTOARs. In Estonia, a country that is much smaller than Japan, there is a limited number of corporations for each domain of vital services. As such, the direct relationship between the public sector and corporations is considered to be mature.

As for information-sharing in the event of a security incident, in the case of Japan, CII operators notify NISC via the CEPTOAR Secretariat and the competent ministry or agency of the critical infrastructure. In the case of Estonia, however, the vital service providers notify CERT-EE under the RIA directly. Estonia surpasses Japan in the aspects of the volume of incident information that CERT has acquired and accumulated, as well as the need to report speedily.

Furthermore, the reporting of security incidents is mandated by law in Estonia, and companies cannot hesitate in making reports for fear that doing so may have a negative impact on their corporate image.

Table 4 Comparison of information-sharing systems of Estonia and Japan

	Estonia	Japan
Information-sharing system		

Source: Drawn up based on the RIA website and NISC website

(iii) Feasibility of implementation in Japan

It is necessary to resolve various issues of Japan's NISC is to take on the function of directly supervising CII operators on the implementation of cybersecurity policies in the same way as Estonia's RIA. Firstly, the supervision of all CII operators is difficult based on the current personnel strength in NISC. Hence, there is a need to either increase the number of personnel assigned to NISC, or to use other means such as outsourcing the work to a third-party organization. In addition, it will probably also be necessary to segregate work related to the field of cybersecurity, from among the tasks of supervising CII operators that the respective competent ministries and agencies of the respective critical infrastructure are responsible for.

With regard to the information-sharing systems, as there is a very large number of companies in each critical infrastructure domain in Japan as compared to Estonia, it would be difficult for the NISC to process the overwhelming volume of incident information if CII operators were to report directly to NISC. Hence, it would probably be preferable to maintain the current system of using CEPTOARs for each sector.

(4) Risk Analysis and Business Continuity Plans

(i) Estonia's risk analysis and business continuity plans for vital services

Drawing up a risk analysis for vital service outages and business continuity plans for service interruptions in advance is extremely important for the implementation of the necessary measures beforehand, as well as for the smooth implementation of restoration work in the event that damage is incurred. In Estonia, vital service operators are mandated under the Emergency Act to draw up risk analysis and business continuity plans for vital services, while the procedures for the formulation of these documents and their contents are prescribed by the Ministry of the Interior regulation, "Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan."[52] Upon its designation as a vital service provider, the business operator in question is required to conduct a risk analysis, formulate a business continuity plan, and submit these to the competent ministry or agency within a year. Risk analyses and business continuity plans must be updated at least once every two years, and every time there are significant changes to the threats or environment surrounding the vital services. When it is deemed unnecessary to change the contents of a previous risk analysis and business continuity plan based on the results of an analysis conducted for the update of the documents, the vital service provider is required to notify the competent ministry or agency.

Risk analyses are implemented in five stages. The first stage is to clarify why the service in question has been designated as a vital service, and to define who the users of the service are, the number of users, the service coverage area, minimum service provision level in the event of an emergency, and maximum tolerable period of disruption during an incident. The second stage is to identify the critical activities necessary for the vital service to function, and to analyze the degree of importance of these activities. It also involves the analysis of the resources necessary for the critical activities (staff, buildings and territory, IT, information, funds, other services, suppliers and collaborators). The third stage is to identify the threats that may impede the critical activities,

---

[52] Minister of the Interior, *Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan*, https://www.riigiteataja.ee/en/ eli/525092017001/ consolide.

identify multiple scenarios that could bring about a loss in the functions of the vital service, evaluate the likelihood of occurrence of the scenario (five-grade evaluation) and the extent of damage accompanying the occurrence of the scenario (five-grade evaluation), and calculate the class of risk (five-grade evaluation). The fourth stage is to analyze, in the event of the occurrence of the scenarios, the measures that should be implemented at the current point in time and the measures that should be implemented in order to reach the standards of maintaining the minimum service levels and the standards of maximum tolerable period of disruption within three years. Finally, to summarize the risk analysis, the fifth stage involves summarizing the instructions pertaining to: (1) List of order of priority for the critical activities; (2) List of scenarios ranked high for the class of risk; (3) Threats that have the potential to cause long-term disruption to the vital services in question; (4) Impact on citizens' lives; and (5) Guidelines for citizens in the event of a long-term disruption.

The business continuity plan carries out a review based on the results of the risk analysis, and prescribes a recovery plan that corresponds to scenarios in a class of high risk. The recovery plan should include the following: (1) Contact information of the representative in charge of incident response in the event of disruption to vital services and critical activities; (2) Contents of recovery activities; (3) Contact information of the deputy representative in charge of incident response and contents of activities; (4) Resources necessary for recovery activities; (5) Alternative measures if the recovery activities cannot be implemented effectively; (6) Measures to mitigate damage and the implementation procedures of these measures; (7) Guidelines for the provision of information to citizens; (8) Expected time required for the restoration of vital services.

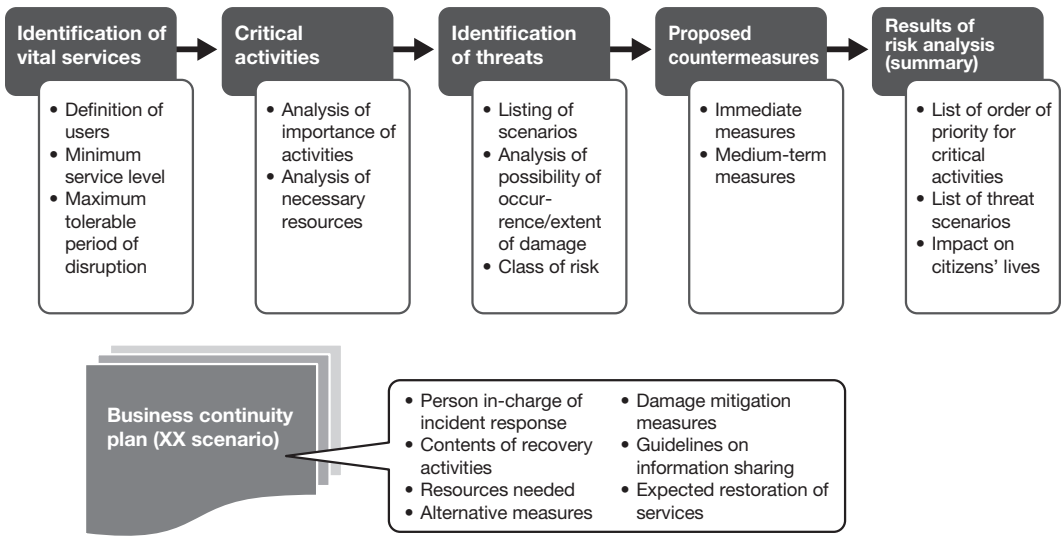


Figure 5 Overview of risk analysis procedures and business continuity plans

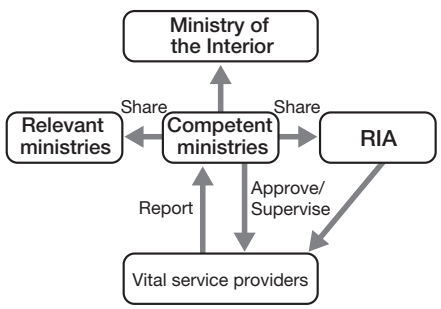
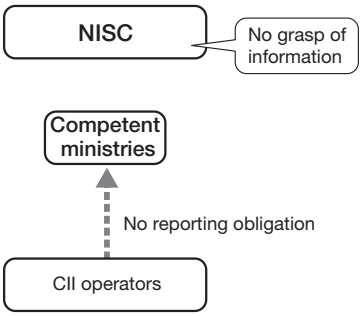
Source: Drawn up based on Estonia's "Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan"

(ii) Comparison with Japan's approach to risk analysis and business continuity plans

With regard to the risk analysis and formulation of business continuity plans for critical infrastructure in Japan, Japan implements similar initiatives as Estonia as a part of two policy approaches: the establishment and spread of safety standards, and risk management and establishment of a coping mechanism, which are set forth in the Fourth Action Plan on Information Security Measures for Critical Infrastructures. However, several differences can be found.

In Estonia, it is mandatory to conduct risk analyses and formulate business continuity plans for vital services, with legally binding force provided through the Emergency Act and other relevant domestic laws and ordinances. Under the Estonian system, the risk analyses and business continuity plans drawn up by vital service providers are submitted to the competent ministries and agencies for the vital services, and approved by these competent ministries and agencies. If there are any inadequacies with these risk analyses and business continuity plans, the competent ministries and agencies can provide the necessary supervision. Furthermore, the risk analyses and business continuity plans submitted to the competent ministries and agencies of the vital services are shared not only with the competent ministries and agencies in question, but also with all other relevant ministries and agencies. They are also consolidated at the Ministry of the Interior, which plays a leadership role in responding to emergency situations. Through this framework, the Ministry of the Interior is able to capture the risk analyses and business continuity plans drawn up by all vital service providers, and thereby obtain information beforehand on the response that providers should take if a crisis occurs in relation to vital services. Moreover, as the risk analyses and business continuity plans contain information that is related to the trade secrets of the service provider in question, the protection of these documents is provided for under the Emergency Act. On the other hand, the formulation of risk analyses and business continuity plans in Japan is encouraged as an effort to meet the goals set out in the Fourth Action Plan, but is not legally mandated for CII operators. According to a survey conducted by NISC in FY2016, only 57% of all CII operators have completed the formulation of a business continuity plan, while 23% of the CII

Table 4 Comparison of information-sharing systems of Estonia and Japan

	Estonia	Japan
Legally binding force	Yes Provided for under the Emergency Act	No Fourth Action Plan on Information Security Measures for Critical Infrastructures
Sharing of information with the government		

Source: Drawn up based on Estonia's Emergency Act and the Order for the Organization of the Cabinet Secretariat

operators have no plans to draw up a business continuity plan.[53] This clearly shows the negative effect of a measure that has no legally binding force. Furthermore, risk analyses and business continuity plans are kept internally by the CII operators that have drawn them up; these operators are not obligated to submit them to the competent ministries and agencies of critical infrastructure. For this reason, in Japan, the competent ministries and agencies do not have any means of carrying out supervision or providing instruction with regard to the response of CII operators in the event of a critical infrastructure-related crisis. On top of that, they are also unable to capture the contents of the plans beforehand.

(iii) Feasibility of implementation in Japan

In addition to minimizing the damage caused by cyberattacks, it is possible to enhance resilience with regard to the operation of critical infrastructure by swiftly implementing restoration and recovery procedures. The formulation of a risk analysis and business continuity plan is indispensable toward enhancing the cyber-resilience of critical infrastructure. Although NISC has played a central role in promoting the formulation of risk analysis and business continuity plan among CII operators, but response is progressing slowly.

In order to ensure that CII operators comply with the requirement of drawing up risk analyses and business continuity plans, it is necessary to make it legally mandatory. As explained in the previous section about legal systems, the Basic Act on Cybersecurity should be revised to make CII operators should be obligated to conduct risk analyses and draw up business continuity plans.

(5) Cyber Exercises

(i) Cyber exercises in Estonia

Estonia recognizes cyber exercises as an important means for promoting public-private partnership. Hence, the government takes the lead in organizing cyber exercises that are participated in by both the public and private sectors. It also participates actively in international cyber exercises.

Cyber exercises organized by the Estonian government include “Cyber Hedgehog”, which is based on the scenario of a cyberattack on the electronic voting system, as well as the tactical exercise on the protection of critical infrastructure and crisis management organized by the Ministry of Economic Affairs and Communications, both held in 2010. Cyber Fever, a command center exercise for cyber defense by the Estonian government, was held in 2012, during which the decision-making process in the government was confirmed.

The Cyber Defense Unit (to be discussed later) participates every year in Spring Storm, the military exercise conducted by the Estonian military, during which it participates in training on public-private partnership in emergencies. Since 2013, RIA has been organizing a technical training every year, which draws about 500 to 800 participants from the private sector annually, including vital service providers.

In 2015, the Ministry of Economic Affairs and Communications organized CONEX2015 in cooperation with the Ministry of the Interior. This exercise verified the response guidelines at the strategic level in the event of information leakage incidents and large-scale cyberattack on vital

[53] National center of Incident readiness and Strategy for Cybersecurity (NISC), “FY2016 Survey on the Status of Penetration of Safety Standards, etc. for Critical Infrastructure,” http://www.nisc.go.jp/conference/cs/ciip/dai10/pdf/10shiryou02.pdf.

services such as the eID card infrastructure and data exchange networks. Furthermore, Cyber Hedgehog 2015 held the same year provided validation based on the emergency response plan for large-scale cyberattacks, for matters such as the role of the respective organizations during an emergency, guidelines for public-private partnerships, response procedures in RIA, and guidelines for the sharing of information.

Based on the results of CONEX2015 and Cyber Hedgehog 2015, a review was carried out on the types of vital services covered under the Emergency Act, as well as the revision of regulations in the laws governing each sector. In 2017, the revised Emergency Act was enforced. In this way, cyber exercises conducted in Estonia do not only enhance participants' capacity and verify response procedures; rather, the results of the exercises are swiftly tied in with law revisions in order to ensure that the respective organizations respond securely when coping with an emergency. This is the characteristic of the Estonian system.

With regard to involvement in international cyber exercises, Estonia has participated in Cyber Europe organized by EU/ENISA (2010, 2012), the joint EU-US exercise Cyber Atlantic (2011), Cyber Coalition organized by NATO (2011), NATO's crisis management exercise CMX (2012), and Baltic Cyber Shields (2010) and Locked Shields (2012) organized by the NATO Cooperative Cyber Defence Centre of Excellence, to name a few. The Cyber Defense Unit participated in Cyber Coalition in 2009 as an observer, and has been participating every year since 2010. At Cyber Coalition held in 2012, employees of vital service providers in Estonia also provided their cooperation from the planning phase.[54] At the Locked Shields exercise held in 2013, the Estonian representative team, comprising vital service providers and key members of RIA, was highly appraised for its advanced technical skills and excellent teamwork, and placed second after the NATO representative team.[55] The 2013 Cyber Coalition exercise was hosted by Estonia. In addition to preparing the plans for the exercise through public-private cooperation, cyber experts from the private sector of Estonia led the exercise during its implementation, marking a first for an exercise organized by NATO.[56] From the beginning of 2014, Estonia has been even more actively involved in international cyber exercises. At the Cyber Europe exercise organized by EU, nine teams from Estonia composed jointly of members from the public and private sectors participated and confirmed guidelines for incident response, information-sharing, and inter-agency coordination. In addition, key personnel from RIA were also involved in the preparation of exercise plans, coordination of the exercise, and as key "red team" members. At Cyber Coalition, the Estonian representatives surprised the other participating countries by demonstrating their advanced skills in carrying out digital forensic investigation on android terminals that have been contaminated by malware. At Locked Shields, the Estonian team was ranked third overall, and first in the forensics category.[57] The Locked Shields exercise held in 2017 was hosted by Estonia, and was conducted based on the scenario of defending a virtual airbase network from cyberattacks on power networks, reconnaissance drones, the military's command and control system as well as fuel

---

54 Piret Pernik and Emmet Tuohy, *Interagency Cooperation on Cyber Security: The Estonian Model*, p. 9.

55 Republic of Estonia Information System Authority, *2013 Annual Report Cyber Security Branch of the Estonian Information System Authority,* p. 14.

56 Piret, *Interagency Cooperation on Cyber Security: The Estonian Model*, p. 9.

57 Republic of Estonia Information System Authority, *2014 Annual Report Cyber Security Branch of the Estonian Information System Authority*, p. 21.

supply infrastructure.

To date, Locked Shields had been an exercise focused primarily on the technical aspects. However, in the Locked Shields exercise hosted by Estonia, training was also conducted on decision-making processes for policymakers, with support provided by legal advisors. All the exercises are participated in by government organizations, Internet service providers, and practitioners from vital service providers, who present a high level of skills. These international cyber exercises are characterized by the active involvement of not only key government officials from Estonia, but also engineers from the private sector.

(ii) Comparison with Japan's approach to cyber exercises

In Japan, cross-sectoral exercises organized by the Cabinet Office have been held since FY2006 with the aim of improving public-private partnership in the field of critical infrastructure protection. The exercise scenarios have been becoming increasingly difficult, while the scale of the exercise has also been expanding, from about 90 participants in FY2006 to about 2,600 participants in FY2017. Each competent ministry and agency of critical infrastructure has also been conducting exercises on dealing with cyberattacks, with a focus on their respective areas of jurisdiction.

Although similar cyber exercises are also conducted in Estonia, the difference with Japan lies in the fact that Estonia's exercises provide training on the response by various governmental organizations to large-scale cyberattacks, and validate the effectiveness of the country's emergency response plans. Japan's cross-sectoral exercises, on the other hand, are focused on the sharing of information and collaboration between the critical infrastructure stakeholders, while exercises conducted by the competent ministries and agencies of critical infrastructure are aimed at enhancing the technical response capability of operators in their respective fields. Going forward, the respective ministries and agencies of the Japanese government should actively incorporate training that includes aspects such as response and decision-making, into their exercises.

It has to be said that Japan's involvement in international cyber exercises is relatively limited in comparison with Estonia. In the past, Japan had participated in Cyber Storm, a public-private joint exercise organized by the US Department of Homeland Security.[58] The government and CII operators have a poor track record for full-fledged participation in international cyber exercises. In September 2017, the Ministry of Economy, Trade and Industry held the first US-Japan ICS (Industrial Control System) Cybersecurity Joint Training in Japan.[59] Seven experts from the US Department of Homeland Security and ICS-CERT were invited, and an exercise on cybersecurity for industrial control systems was finally held. Estonia has attracted the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) into its country, and makes use of its geographical advantage to participate as a player in various international cyber exercises organized by NATO and EU. It is also involved in the preparation of exercise plans, prior coordination, leading the exercises, and as the "red team" (playing the role of the attackers). In addition to employees of governmental organizations, engineers of vital service providers also participate actively. In these respects, it differs greatly from Japan.

---

[58] Cabinet Secretariat, *"Jyoho Sekyuriti Seisaku no Gaiyo"* [Overview of Information Security Policy], p. 12. http://www.kantei.go.jp/jp/singi/shin-ampobouei2010/dai7/siryou2.pdf.

[59] Ministry of Economy, Trade and Industry, "Press Release: Japan's first US-Japan ICS (Industrial Control System) Cybersecurity Joint Training held," http://www.meti.go.jp/press/2017/09/20170927004/20170927004.html

Table 6 Comparison of Estonia and Japan in the area of cyber exercises

	Estonia	Japan
Domestic cyber exercises	• Government's decision-making exercise (CONEX) • Public-private cooperation exercise (Cyber Hedgehog) ⇒ Confirmation of request for emergency response, revision of law	• Cross-sectoral exercises ⇒ Confirmation of public-private cooperation guidelines
International cyber exercises	• Proactive involvement in cyber exercises organized by EU and NATO • Planning and leading of exercises as a host country • Self-directed involvement by the private sector, such as vital service providers, Internet service providers, etc.	• Participation in Cyber Storm (U.S.), etc. as observer • Organized US-Japan ICS Cybersecurity Joint Training (METI) (September 2017), seven participants from U.S.

Source: Drawn up based on the status of participation in cyber exercises by Estonia and Japan

(iii) Feasibility of implementation in Japan

In Estonia, cyber exercises are carried out based on the assumption of a large-scale cyberattack on vital services, and various matters are verified based on the emergency response plan, including the government's decision-making processes, the roles of the respective organizations in an emergency, guidelines for public-private cooperation, response procedures in RIA, and guidelines for information-sharing. In Japan as well, efforts are made to build the response capacity of vital service providers through cross-sectoral exercises. By making use of the framework of such cross-sectoral exercises, which are conducted based on the scenario of a large-scale cyberattack at the national level as explained in the previous section, it is possible to verify the emergency response plans drawn up by the government, the guidelines for strategic decision-making by policymakers, response by the respective ministries and agencies, and public-private partnership.

Involvement in international cyber exercises, which is actively promoted in Estonia, can also be fully introduced in Japan. Through the active participation of engineers from government organizations, CII operators, and cybersecurity operators in international cyber exercises held in Europe and America, Japan can acquire information about the latest cyberattack technology and defense technology, as well as develop friendly relations and human networks with the relevant countries. Furthermore, acquiring knowhow on organizing international cyber exercises can also facilitate the hosting of international cyber exercises by Japan in future.

(6) National Defense Strategy and Organizations

(a) Positioning of cyber defense and protection of vital services in the national defense strategy

(i) Estonia's national defense strategy and protection of vital services

Estonia is a small country with a small population. Its terrain is flat with few topographical barriers, and shares a border Russia, a potential adversary country. Hence, from the perspective of national defense, it has been placed in a very tough environment. For this reason, its national defense strategy is set out based on the premise of primarily confronting threats from Russia. The National Defense Strategy of Estonia published by the Estonian Ministry of Defense, sets out the decline of Estonia's international status through non-military means and the threat of the severance of friendly relations with allies as security risks faced by Estonia, and raises attacks on

energy-related infrastructure and information and communications systems as a potential threat to Estonia's survival.[60] It establishes "the Estonian population's strong will to defend their country" as the basis of Estonia's national defense, and emphasizes the principle of "total defense" as a means of countering the threat of war as well as non-military threats.[61] The National Defense Strategy sets out six main courses of action to ensure deterrence power as well as organized response for its national defense. These are: military defense; civil sector support to military defense; international efforts; ensuring internal security; ensuring the sustainability of vital services; psychological defense.

Of these six courses of action for its National Defense Strategy, the inclusion of "ensuring the sustainability of vital services" is a distinctive feature, and is consistent with the previously mentioned Cyber Security Strategy 2014 – 2017 and provisions of the Emergency Act. The National Defense Strategy sets out the guidelines for ensuring the sustainability of vital services in the event of a military attack. According to the Strategy, in the event of a military attack against Estonia, sustainability of vital services shall be continued within the same organizational frameworks as would be applied under peacetime circumstances. It then lists the competent ministries and agencies that govern the respective vital services. The Strategy also stipulates that the Estonian government identify the vital services that particular importance should be placed on from the perspective of national defense, that vital service providers take into consideration plans for responding to "military threat scenarios" when drawing up risk analyses and business continuity plans, and that the Ministry of the Interior consolidate these plans into an integrated document and submit it to the Riigikogu (parliament) of Estonia once every four years.

(ii) Comparison with Japan

With regard to the security environment surrounding Japan, the National Defense Program Guidelines for FY2014 and Beyond states that establishing the stable use of cyberspace as global commons is a significant security challenge for the international community, including Japan.[62] However, concerning public-private partnership in the field of cyberspace and the protection of critical infrastructure, these Guidelines stop short at stating that "in light of society's growing dependence on outer space and cyberspace, Japan will make effective use of the SDF's capabilities when endeavoring to strengthen collaboration with relevant organizations and clarify the division of roles, thereby contributing to comprehensive, government-wide initiatives."[63] It does not contain any particular reference to the protection of critical infrastructure in relation to cyber security. However, a document titled "Toward Stable and Effective Use of Cyberspace" published by the Ministry of Defense in 2012 states, under the section on "Contributions to National Efforts, including Partnership with the Private Sector," that as the Ministry of Defense and Self-Defense Forces rely on the private sector for the development and maintenance of social infrastructure and equipment, it is important to ensure the stable use of cyberspace across the whole of society. To that end, it states that Japan is engaged in efforts such as conducting cyber exercises, sharing

60 Estonian Ministry of Defence, "National Defence Strategy Estonia", 2011, p. 7.

61 Ibid., p. 8.

62 *National Defense Program Guidelines for FY2014 and Beyond*, approved by the Cabinet (December 17, 2013), p. 2.

63 Ibid., p. 13.

information, and dispatching human resources to government organizations.[64]

In comparing the defense strategies of Estonia and Japan, both countries demonstrate a similar recognition of the importance of cyber defense and the need for public-private partnership. However, while Estonia positions the protection of vital services as one of six courses of action in its national defense, Japan's Ministry of Defense and Self-Defense Forces adopt the position of contributing to government-wide initiatives. Hence, there appears to be a difference in the level of commitment to protecting critical infrastructure between the two countries.

(iii) Feasibility of implementation in Japan

The protection of vital services is positioned as one of the courses of action in the national defense strategy of Estonia, while Japan's Ministry of Defense and Self-Defense Forces adopt only a stance of contributing to comprehensive initiatives by the government as a whole without clearly establishing the functions of the Ministry of Defense and Self-Defense Forces in protecting critical infrastructure. If the protection of critical infrastructure were positioned as a new function of the Ministry of Defense and Self-Defense Forces as a part of Japan's national defense strategy, there would be a need to clarify the scope of their duties, and to enhance the personnel and equipment needed for them to perform these duties.

(b) National defense organizations

(i) Overview of the Estonian Defense Forces

The Estonian Defense Forces are composed of the regular land, sea, and air forces, as well as the Estonian Defense League (hereafter, "Defense League"). The strength of the regular military force during peace time is about 6,000 personnel, half of whom are personnel drafted in under the conscription system. The Defense League is a volunteer national defense organization that comprises about 15,000 personnel. During war time, it is expanded to a 60,000-strong force through the mobilization of reserve personnel who have completed their training under the conscription system.[65]

(ii) Cyber Command of the Estonian Defense Forces

The organization for cyber defense in the Estonian Defense Forces had comprised only personnel from the regular forces deployed to the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), and the Cyber Defense Unit of the Estonian Defense League (to be discussed later). However, on August 1, 2018, the Cyber Command was newly established as a subordinate organization under the Estonian Land Forces.

The main mission of the Cyber Command is to "carry out operations in cyberspace in order to provide command support for Ministry of Defense's area of responsibility," and its primary tasks are outlined as follows:

- Provide information and communication technology infrastructure and services.
- Provide cyber defense.
- Plan and execute cyber operations.

---

64 Ministry of Defense, *Toward Stable and Effective Use of Cyberspace*," pp. 8-9.

65 Estonian Defence Forces, http://www.mil.ee/en/defence-forces.

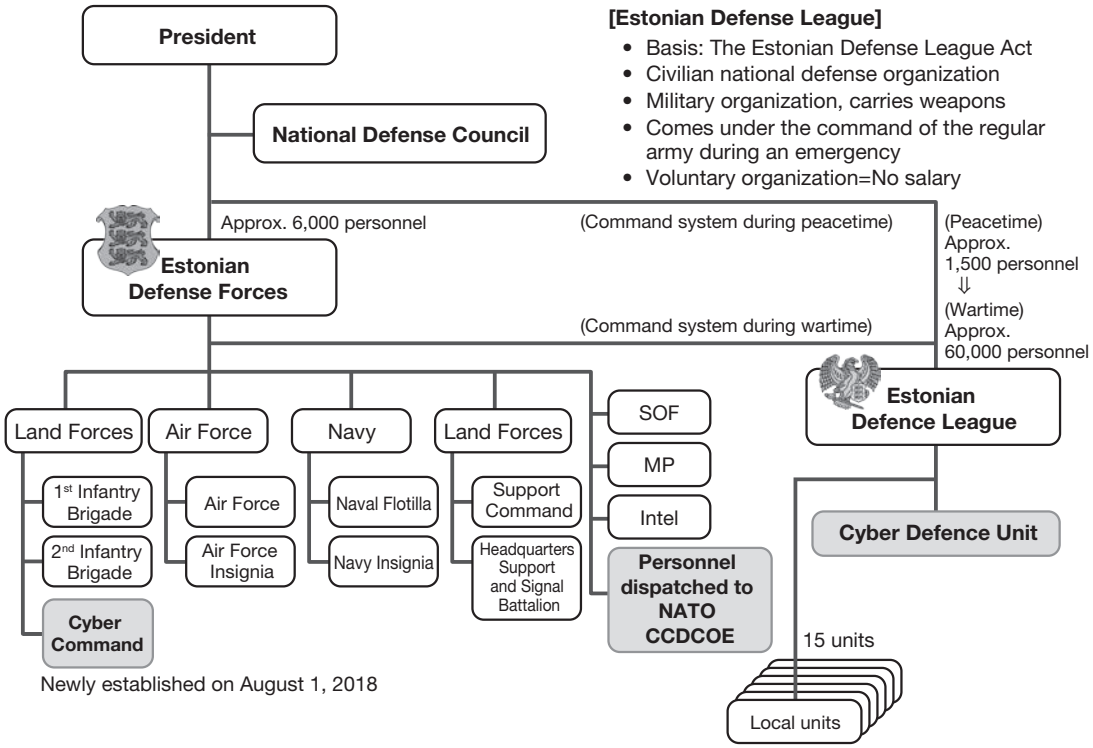


Figure 6 Overview of the organization of the Estonian Defense Forces

Note: The Cyber Command was newly established as a subordinate unit of the Land Forces on August 1, 2018.
Source: Drawn up based on the website of Estonian Ministry of Defense

- Gain, maintain and share cyberspace situation awareness.
- Plan and execute information operations.
- Provide Headquarters support for Joint Headquarters.
- Plan and execute strategic communications.
- Train, prepare and mobilize wartime and reserve units.
- Conduct functional area Training, Research and Development.

The Cyber Command of the Estonian Land Forces is organized as follows: Headquarters, HQ Support and Signal Battalion, Information Communication Technology Center, Cyber and Information Operations Center, Strategic Communications Center, and HQ and Support Company.[66] It has a strength of about 300 personnel (about 240 personnel from the existing communications unit, and about 60 newly recruited personnel), and its combat capability is expected to be completed by 2023.[67]

66 Cyber Command, http://www.mil.ee/en/landforces/Cyber-Command.

67 Kaitsevae kubervaejuhatus alustas tegevust (The Cyber Command of the Defense Forces began its attivities), http://www.mil.ee/et/uudised/10340/kaitsevae-kubervaejuhatus-alustas-tegevust.

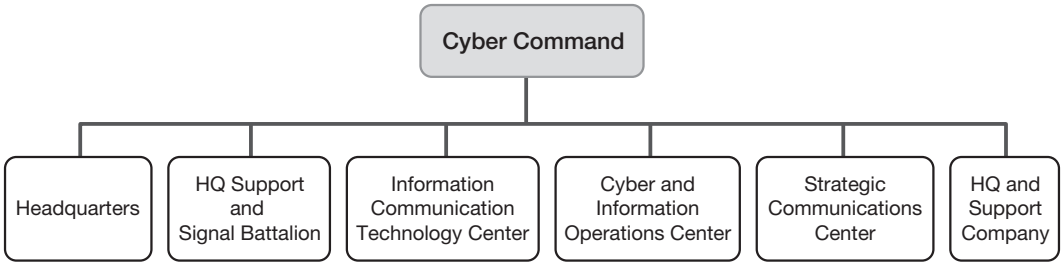


Figure 7 Organization of the Cyber Command of the Estonian Land Forces

Source: Extracted from the website of the Estonian Defense Forces

(iii) Cyber Defense Unit of the Estonian Defense League

To understand the cyber defense system of the Estonian Defense Forces, it is first necessary to gain an overview of the Estonian Defense League, which is a paramilitary organization.

The Estonian Defense League is defined as a civilian national defense organization under the Estonian Defense League Act (hereafter, "Defense League Act"), which provides for its organization as a military organization, its possession of arms, implementation of training, and incorporation under the command of the regular army in the event of an emergency. Civilians participate in the Defense League through their own free will, and they are not paid any salary as the Defense League is a voluntary organization.[68]

The Commander of the Defense League is appointed by the Estonian government based on recommendations put forth by the Minister of Defense and the Commander of the Defense Forces. Within the command system, the Commander of the Defense League is subordinate to the Commander of the Defense Forces. However, during peace time, the authority of the Commander of the Defense Forces to direct the Defense League is limited only to matters related to military training, while authority over the management and operation of the Defense League is exclusive to the Commander of the Defense League. During an emergency, the Commander of the Defense Forces has full command over the Defense League.

The Cyber Defense Unit is a unit that is in parallel with the 15 regional units under the Defense League, and comprises the Unit Commander, Unit Command, and multiple cells. The Unit Command is a staff organization that supports the decision-making of the Unit Commander, and the respective departments including logistics and supplies, analysis, and training, are made up of both volunteers and full-time personnel. There are multiple cells within the Unit that are engaged in various missions related to cyber defense, as well as maintenance and management, research, and tool development, among others.[69]

(iv) Mission of the Cyber Defense Unit

The core tasks of the Cyber Defense Unit are to provide education and training, and strengthen cybersecurity in the private sector.

Education and training, which is the first core task of the Cyber Defense Unit during

[68] Kadri Lasla, Anna-Maria Osula, LTC Jan Stinissen, *The Cyber Defence Unit of the Estonian Defence League*, p. 10.

[69] Ibid., pp. 13-14.

peacetime, aims to enhance the knowledge, skills, experience, and attitude in executing missions of key personnel. Seminars, information sharing study sessions, training, and field studies are planned for personnel. They also participate in the Locked Shield exercise and the Spring Storm exercise organized by the Estonian Defense Forces, improve their cyber defense skills, and master incident coping skills and information sharing procedures during emergencies.

The second core task of the Cyber Defense Unit is to strengthen cybersecurity in the private sector. In this respect, a wide range of technical support is provided to various public and private organizations to contribute to the strengthening of cybersecurity. Some examples of the initiatives implemented in this regard include consulting on security measures, implementation of tests on the security functions of information systems, malware screening on the computers of municipal schools, installation of security functions for the national electronic voting system, and security examinations.

Other tasks include providing support for cybersecurity for information and communication systems, and ensuring cybersecurity in times of emergency.

In particular, the Emergency Act sets out provisions for the Defense League to respond in the event of an emergency in order to limit the extent of damage, while the Cyber Defense Unit responds during a cybersecurity-related emergency, such as a large-scale cyberattack on critical services. Although the specific duties are not clearly stipulated, the government assigns the responsibilities on a case-by-case basis during such situations.[70]

(v) Recruitment of personnel, and their obligations and responsibilities

To be accepted as a member of the Cyber Defense Unit, personnel is required to be 18 years or older, have an impeccable personal and career history, be loyal to Estonia, and be strongly committed to protecting Estonia's independence and complying with the constitution. Not all personnel recruited are cybersecurity experts or individuals with advanced IT skills; lawyers, policymakers, and educators in the field of cybersecurity, among others, are also hired.[71] Candidates need to receive recommendation letters from two personnel who have already been hired by the Cyber Defense Unit, and these two recommending personnel are responsible for the candidate's suitability for the job. Those who are known to have health issues, criminal records, or observed to demonstrate inappropriate behavior, are not accepted. Candidates submit application forms to the Commander of the Cyber Defense Unit, undergo a background check, and a decision is made on whether the candidate is accepted or rejected within approximately three months. If accepted, the candidate is sworn in and officially joins the Unit.[72]

Personnel are required to protect Estonia's independence as well as constitutional order, and to comply with laws and regulations in carrying out the activities of the Defense League. Being a member of the Cyber Defense Unit in itself does not make it compulsory for personnel to participate in the activities of the Defense League. To begin with, the Defense League is an organization established through participation base on the free will of members. As such, whether or not to partake in a specific mission rests on the free will of the respective personnel. In particular,

---

70 Ibid., pp. 22-24.

71 Estonian Defence League's Cyber Unit, http://www.kaitseliit.ee/en/cyber-unit.

72 Kadri, *The Cyber Defence Unit of the Estonian Defence League*, pp. 15-17.

personnel of the Cyber Defense Unit participate in activities as volunteers without receiving any remuneration from the government, while receiving a salary through their day jobs in regular companies. As such, they participate in the activities of the Cyber Defense Unit in spare moments between their main jobs. When carrying out a mission, they are required to wear either the uniform of the Defense League, or to wear the badge of the Defense League on their own attire.[73]

(vi) Logistical support and access to confidential information

The Cyber Defense Unit is allocated with the necessary equipment for performing its duties in coordination with the Estonian Defense Forces and the Ministry of Defense. The Defense League has the right to use the facilities and equipment of the Estonian Defense Forces for free, through prior arrangements and coordination. The information and communications infrastructure managed by the Cyber Defense Unit is supplied through contracts with external parties. The expenses related to the operation of the Cyber Defense Unit are covered by the government's budget, as well as subscriptions, donations, and revenue from contracts.[74]

In performing its duties, the Cyber Defense Unit needs to access the information of public and private vital service providers, and for both the public and private sectors, the detailed information concerning critical infrastructure often constitutes confidential information that cannot be disclosed. Access to information on critical infrastructure in the private sector is managed through the conclusion of non-disclosure agreements concerning the handling of information for support missions during peacetime. However, in an emergency, there is no choice but to respond on a case-by-case basis. This is viewed as an issue that should be resolved going forward.

As for the critical infrastructure operated and managed by the national government, the smallest number of volunteers needed for the Cyber Defense Unit is subjected to security screening, and a system has been established that enables them to access confidential information on an official basis. The types of confidential information that can be accessed by these personnel are determined in accordance with the principle of "need to know," based on the judgement of the manager of the critical infrastructure. Hence, assigning security clearance to the personnel of the Cyber Defense Unit ensures that they do not pose a risk to information security.[75]

(vii) Status under international law in the event of an international armed conflict

The respective units of the Defense League, including the Cyber Defense Unit, carry out their respective missions under the leadership of the Commander of the Estonian Defense Forces in the event of an international armed conflict. As the personnel of the Defense League are organized through the participation of private-sector volunteers, measures are taken to ensure that they fulfill the qualifications of combatants in accordance with international law.

Under international law, members of an army fall into two categories. The first category comprises members of the regular army of the countries involved in the conflict, and includes militia or volunteers who make up a part of the regular army. The second category comprises members of the militia or volunteers other than the aforementioned, and includes organized

---

73 Ibid., pp. 18-19.
74 Ibid., p. 27.
75 Ibid., pp. 31-32.

resistance activities that belong to the countries involved in the conflict. Such organizations are deemed as members of the army by fulfilling the following four criteria set out in the international customary law and Article 4A(2) of Geneva Convention (III).

(1) Under the command of a single person who is responsible for his/her subordinates.
(2) Wearing a fixed unique badge that can be identified from a certain distance away.
(3) Carries weapons openly in the public.
(4) Carries out operations in accordance with the law of armed conflict and customary law.

An irregular unit that belongs to countries involved in the conflict, and which fulfill the four criteria set out above, is qualified to be a combatant unit, and is exempted from combatant liability while having prisoner-of-war status.[76]

Let us attempt to apply the provisions of these international laws to the Defense League.

Firstly, as the Defense League comes under the command of the Estonian Defense Forces during wartime, members of the Cyber Defense Unit correspond to the first category of militia or volunteers who form a part of the regular army. On the other hand, the Defense League during peacetime does not fall under the command of the Estonian Defense Forces. For this reason, it does not correspond to the first category of militia or volunteers who form a part of the regular army, but corresponds to the second category of other militia or volunteers and therefore is required to fulfill the four criteria. With regard to the four criteria to be deemed as a member of the army, the first criteria require it to be under the command of a single person who is responsible for his/her subordinates. The Defense League clearly fulfills this, with a Commander of the Defense League and a Unit Commander of the Cyber Defense Unit, which is a subordinate unit under the Defense League. As for the second criteria of wearing a fixed unique badge that can be identified from a certain distance away, members are required to wear the uniform or wear the badge of the Defense League over their own attire, so this condition is also fulfilled. The third criteria of carrying weapons openly in publics is not particularly meaningful in the context of cyberwarfare. With regard to the fourth criteria of carrying out operations in accordance with the law of armed conflict and customary law, education and training on the law of armed conflict are implemented regularly, while operations are carried out in accordance with international law under the command of the Unit Commander in times of emergency. Hence, this criteria is also fulfilled.

Based on the above, regardless of any declaration of war or whether or not there is a clear armed attack, civilian volunteers who are the members of the Cyber Defense Unit are qualified as combatants under international law, and can perform various duties as members of the Estonian Defense Forces.[77]

(viii) Comparison with Japan

In the case of Japan, the Cyber Defense group is made up of the SDF Command Control Communication Computers Systems Command and the respective communications and system defense groups of the land, maritime, and air defense forces. Personnel of the respective cyber defense units comprise only members who have been nurtured through education and training

[76] Michael N. Schmitt, *TALLIN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS Second Edition*, Cambridge University Press, p. 403.

[77] Kadri Lasla, Anna-Maria Osula, LTC Jan Stinissen, *The Cyber Defence Unit of the Estonian Defence League*, pp. 34-36.

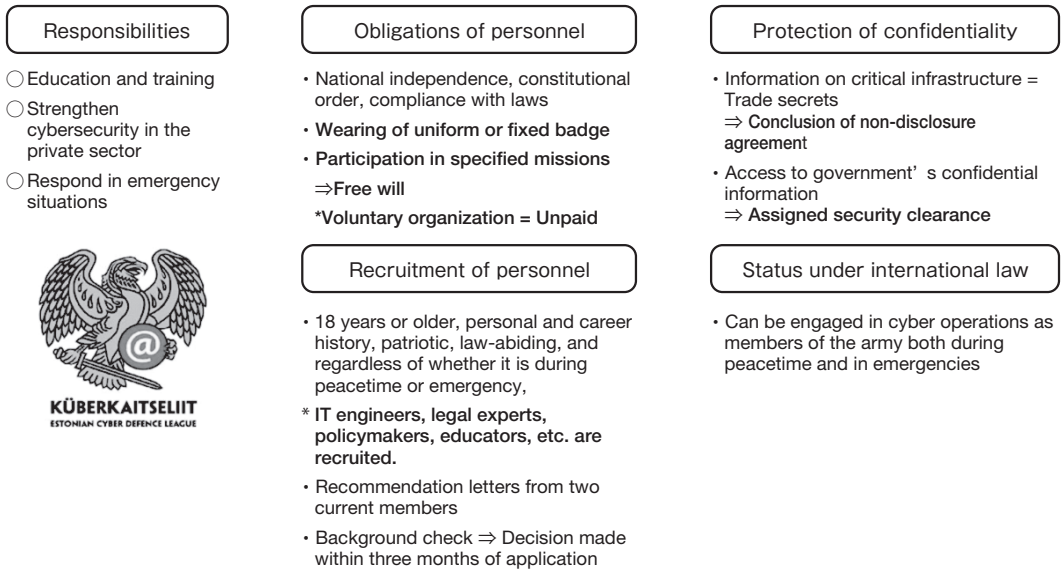


Figure 8 Overview of Cyber Defense Unit

Source: Drawn up based on the reference literature (*The Cyber Defence Unit of the Estonian Defence League*)

within the Self-Defense Force. In Estonia, the cyber defense system is constituted primarily of the Cyber Defense Unit of the Estonian Defense League, which is a paramilitary organization made up of civilian volunteers. However, in August 2018, a new Cyber Command was established under the Estonian Land Forces, which is the regular army of Estonia.

Comparing Japan and Estonia from the perspective of national defense organizations related to cyber defense, a significant difference is observed. In Japan, although SDF reserve personnel system that utilizes civilians has been put in place, it does not specialize in cyber defense. On the other hand, in Estonia, the cyber defense force is composed primarily of the Cyber Defense Unit, a paramilitary organization made up of civilians. (Alongside with the establishment of the new Cyber Command, which is a regular military unit, there is a need to pay attention to the command systems and relationship between the regular military unit of the Cyber Command and the paramilitary organization of the Cyber Defense Unit in future.)

Members of the Cyber Defense Unit are engaged in their day jobs (such as in IT corporations in the private sector or as university professors), while at the same time build up their own capacity through various training programs designed by the Cyber Defense Unit. In times of emergency, they participate in the defense of the country's critical infrastructure. Through the activities of the Cyber Defense Unit, cybersecurity personnel from government organizations and a wide range of industrial sectors interact and engage in exchanges from peacetime, making it easier to cooperate when an incident occurs. Smooth response can therefore be expected.

There is a shortage of experts in the field of cybersecurity not only in Japan but in countries around the world. Although government organizations and corporations are frantically engaged in the competition for human resources with advanced capabilities, Estonia's initiatives are characterized not by the capturing of human resources with advanced capabilities, but in the use of the method of providing a space for national defense activities in cyberspace.

Table 7 Comparison of the national defense strategies and organizations of Estonia and Japan

	Estonia	Japan
National defense strategy	• Positioning of the maintenance of vital services as a main course of action in the national defense strategy	• No particular points raised about the defense of critical infrastructure (Contributing to government-wide initiatives including the private sector)
National defense organization (cyber)	• Main entity: Cyber Defense Unit of the Defense League * After August 2018, the newly established Cyber Command is expected to become the main entity • Main responsibilities: Education and training, strengthening of cybersecurity in the private sector, response during an emergency	• Main entity: Cyber Defense Group, etc. * Means of utilizing civilians not yet developed • Main responsibilities: Defense of SDF's system and network

Source: Drawn up based on Estonia's National Defense Strategy and other documents, and the Defense of Japan

(ix) Feasibility of implementation in Japan

While a Cyber Defense Unit that utilizes civilian volunteers is an extremely beneficial and appealing system, if a similar system were to be introduced in Japan, it is still unknown if the system will be accepted, and whether it can become an established institution. For example, Marine Rescue Japan is an example of a voluntary organization in the area of maritime security. Marine Rescue Japan is a public rescue system supported by national and local government agencies such as the Japan Coast Guard, police, and fire department. As such, it assists in the activities of civilian voluntary rescuers participating in the rescue of people or boats in distress in coastal waters. In addition, the fire corps system under the fire department, while not a voluntary organization, can also serve as a reference. Unlike full-time firefighters, members of the fire corps have other jobs but are mobilized during disasters and for training. They are engaged in keeping guard against fires, putting down riots, disaster prevention, mitigation of damage, as well as support and awareness-raising activities for local residents.

Hence, volunteer activities that support public organizations and systems such as a fire corps can possibly be applied to the field of cybersecurity. However, in the case where such volunteer organizations are associated with the activities of the Ministry of Defense and Self-Defense Forces, which are responsible for national defense, it is necessary to resolve the problems related to the status of personnel under international law. In an international armed conflict, when general civilians are involved in various actions carried out by the Ministry of Defense and Self-Defense forces in relation to cyber defense, there is a possibility that this may correspond with direct participation in hostility by civilians through connection with the three cumulative standards: the threshold of harm, direct causality, and combatants. This may in turn be deemed as committing a (war) crime. To resolve this issue, Estonia's Cyber Defense Unit has designed its system cautiously to ensure that the civilian volunteers are recognize as combatants under international law, in preparation for the event that a large-scale cyberattack is carried out as a part of an international armed conflict.

If Japan were to introduce the effective aspects of Estonia's Cyber Defense Unit system, it would be appropriate to first promote the establishment of a voluntary organization under the

leadership of the government, utilize the existing SDF reserve personnel system, and build a system that allows cybersecurity experts from the private sector to be involved in national defense.

4. Policy recommendations for promoting public-private partnership

Up till this point, this paper has conducted an overview of public-private partnership initiatives related to Japan's cyber defense. It then looked at the various policies of Estonia, undertook a comparison with Japan, and considered the feasibility of implementing these cybersecurity policies in Japan. Based on these reviews, this section offers several policy recommendations for promoting public-private partnership for Japan's cyber defense.

(1) Review of the cybersecurity strategy

Japan's cybersecurity strategy should position cybersecurity for critical infrastructure as the issue of top priority. With regard to the respective policy approaches set out in the cybersecurity strategy, it should clearly set out the order of priority based on an analysis of the respective degree of importance and level of urgency.

Japan's current cybersecurity strategy sets out the following four policy approaches: Enabling socio-economic vitality and sustainable development; Building a safe and secure society for the people; Contribution to the peace and stability of the international community and Japan's national security; Cross-cutting approaches to cybersecurity. The first policy approach, "Enabling socio-economic vitality and sustainable development," can only be realized by ensuring the security of Japan and the stable functioning of critical infrastructure that is the basis of our socio-economic system. The suspension of the functions of critical infrastructure through a large-scale cyberattack can cause damage that has a severe impact on citizens' lives and socio-economic activities, and is also a highly probable event. It is clear that ensuring cybersecurity for critical infrastructure is a matter of the highest priority in comparison with other measures.

From this perspective, Japan's cybersecurity strategy should clarify the order of priority of measures as well as the priority matters, rather than simply listing the policy approaches. At the same time, it should position measures for the protection of critical infrastructure as an issue of the highest priority. Furthermore, alongside with strengthening information-sharing systems between the public and private sectors in order to enhance attribution ability for identifying the masterminds behind attacks, the explicit declaration of putting in place various measures for enhancing the overall resilience of critical infrastructure can also be expected to have considerable effect of deterring the attackers.

(2) Strengthening the supervision and guidance of critical information infrastructure (CII) operators

If we were to consider the probability of a large-scale cyberattack on critical infrastructure and the degree of severity of damage, carrying out a risk analysis and the formulation of a business continuity plan are the responsibilities of CII operators, and the implementation of these activities should be supervised and guided by the government.

However, the current Basic Act on Cybersecurity only calls for CII operators to engage in cooperative efforts for the cybersecurity measures implemented by the government and local public organizations; there is no legal obligation for them to engage in such cooperation. For this reason, in addition to the fact that CII operators are lagging behind in conducting such risk

analyses and formulating business continuity plans, the government has no means of capturing the contents of these plans.

To resolve this issue, under the Basic Act on Cybersecurity, set out provisions on the responsibilities of CII operators, which is to conduct risk analyses on cyberattacks on critical infrastructure, draw up and review business continuity plans based on the results of these risk analyses, and report to the Prime Minister via NISC. The Basic Act on Cybersecurity should also set out provisions for the responsibilities of the national government, which is to exert all efforts to secure trade secrets in the results of the risk analyses and business continuity plans submitted by CII operators, draw up emergency response plans for large-scale cyberattacks, and validate and review these plans through exercises and other means. When revising the law, the Basic Act on Disaster Management (Act No. 223 of 1961) can be used as a reference. Article 39 of the Basic Act on Disaster Management states that a designated public corporation must formulate a disaster management operation plan based on the government's basic disaster management plan, review it every year, and report it to the Prime Minister through the competent Minister. By taking this example as a reference and incorporating new provisions in the Basic Act on Cybersecurity, it is possible to mandate CII operators to report to the government on the formulation of business continuity plans.

The revision of this law can eliminate delays by CII operators to conduct risk analyses and formulate business continuity plans. At the same time, based on the risk analyses and business continuity plans reported by the CII operators, the government can draw up a cross-agency emergency response plan for a large-scale cyberattack at the national level.

(3) Enhancing the functions of the National center of Incident readiness and Strategy for Cybersecurity (NISC)

Ensuring cybersecurity for critical infrastructure in Japan is based on the voluntary efforts of CII operators. The competent ministries and agencies of the respective fields of critical infrastructure have the authority to supervise CII operators, which is based on laws governing the respective industries. Under the current system, the Cybersecurity Strategy Headquarters and NISC do not have direct supervision authority over CII operators. For this reason, measures are promoted through advice and recommendations, as well as general coordination with the competent ministries and agencies of critical infrastructure. As the implementation of cybersecurity policies for critical infrastructure is under the jurisdiction of the respective competent ministries and agencies, there is a possibility that differences may arise in the security measures for each field of critical infrastructure. Moreover, it is not efficient as there is a need to assign a supervising manager and establish a supervising department for cybersecurity in each competent ministry and agency.

For this reason, as demonstrated by the example of RIA in Estonia, a system that enables the unified implementation of security measures for all critical infrastructure should be established by concentrating the supervisory authority for the execution of cybersecurity policies by CII operators on NISC. In doing so, the cybersecurity-related departments of IPA and NICT, as the executive organs for the supervisory work, should be utilized in projects commissioned by the government to establish a system for enabling the implementation of supervisory work on CII operators.

(4) Preparing for a large-scale cyberattack at the national level as a form of armed attack

In promoting public-private partnership in cyber defense, exercises implemented jointly by the public and private sectors is an extremely effective means. In the event of damage to critical infrastructure due to a large-scale cyberattack, response should not be made only by the CII operator that has incurred damage; rather, there is a need for the competent ministries and agencies of the critical infrastructure in question, emergency response organizations such as CERT, and other CII operators to work as one to respond. To enable joint response by the respective public and private-sector actors, it is important to prepare the procedures for dealing and responding to incidents, and to validate their effectiveness.

In particular, with regard to large-scale cyberattacks on critical infrastructure, there is a strong likelihood of a situation that requires a judgement call on whether or not an attack has been carried out on Japan as a form of armed attack. In the Locked Shields exercise organized by NATO, in parallel with a technical offense and defense exercise based on the scenario of a cyberattack on critical infrastructure and air base, a strategic decision-making exercise by policymakers was also held. To ensure that Japan is able to respond appropriate in such situations, cyber exercises based on the scenario of a large-scale cyberattack on critical infrastructure, launched as a part of an armed attack, should be implemented, and the recognition of the situation, responses by the Ministry of Defense and Self-Defense Forces, as well as response by CII operators should be validated.

(5) Establishing pro-bono cyber defense organizations, and enhancing and utilizing the SDF reserve personnel system

To utilize the limited number of cybersecurity experts effectively, it is effective to build a mechanism similar to the Cyber Defense Unit of Estonia, through which civilians can participate in the cyber defense of the country as a social contribution activity. To track the approximately 58 billion yen worth of virtual currency that had leaked out from a virtual currency exchange company in January 2018, dozens of engineers acting in good faith ("white hackers") participated in the effort.[78] In cases such as this, we can see how civilians with advanced cybersecurity skills can help in dealing with cyber incidents as a goodwill activity. In the large-scale cyberattack that occurred in Estonia in April 2007, cybersecurity engineers from within and outside Estonia supported CERT-EE through an ad-hoc and informal human network. The success of Estonia's Cyber Defense Unit system can probably be attributed to the provision of a space where such good-intentioned engineers can participate in the noble activity of supporting the "cyber defense of the motherland." In addition to employees of government agencies, information and communications corporations, and the information security departments of general corporations, white hackers are present in various sectors. It would be effective for the government to provide a space for highly-skilled white hackers to play an active role in.

The first policy for realizing these goals is support for the establishment of pro-bono cyber defense organizations. In recent years, in addition to general volunteer activities, "pro-bono activities" (derived from the Latin expression "pro bono publico" meaning "for the public interest") as a form of social contribution have been developing gradually. Working adults

78 Nihon Keizai Shimbun, "NEM Ou Zenryo Hakka, Ryushutsu Jyokyo no Kaisetsu Saito mo" [Goodwill Hackers in Pursuit of NEM Also Set Up Websites Covering the Leakage Situation], https://www.nikkei.com/article/DGXMZO27182300210220 18CC0000/.

participate in these activities by making use of their specialized knowledge and skills. Already, the National Police Agency has drawn up a manual (model)[79] for volunteer activities in the field of cybercrimes, aimed at countering and clarifying the illegal and harmful information circulating on websites and bulletin boards on the Internet, and is promoting activities such as cyber patrols by civilian volunteers. To provide an activity space that calls for more advanced capabilities, aimed at cybersecurity engineers who possess a higher level of technical skills, the defense of cyberspace has been positioned as a social contribution activity for protecting the security of the country, and the government is leading efforts to establish pro-bono organizations with a focus on cybersecurity experts and IT engineers. Through such efforts, it is possible to build a system in which pro-bono cyber defense organizations cooperate with NISC to provide technical support to CII operators that have suffered damage, as a part of the response to large-scale cyberattacks on critical infrastructure.

The second policy is to enhance and utilize the SDF reserve personnel system in relation to cyber defense in the Ministry of Defense and Self-Defense Forces. Three systems are currently in place: the ready reserve personnel system, the reserve personnel system, and the reserve candidate personnel system. Reserve personnel and ready reserve personnel are engaged in various occupations in their private lives as working adults or students, and participate in training to maintain the necessary skills required by SDF personnel. They are mobilized through defense call-ups and disaster call-ups, and partake in activities as SDF personnel on these occasions. Under the current system, civilians who wish to become a reserve personnel, who can be expected to play an active role in the field of cybersecurity, and who hold official qualifications such as data processing specialist, are recruited in the "information processing" category under the reserve candidate personnel system (Technical). They undergo the necessary education and training for 10 days within a two-year period, and are appointed as reserve personnel after completing the training. Reserve personnel are called up through a defense call-up order, civilian protection call-up order, and disaster call-up order, and become SDF personnel when they are mobilized.[80] By engaging in activities as an SDF personnel under the orders of the commander of a cyber defense-related unit, they can acquire qualification as a combatant under international law rather than remain as civilians. However, the current education and training for reserve candidate personnel and reserve personnel focuses on common areas such as mental training, weapons training, basic training, and physical training. The education and training system for reserve personnel who are responsible for cyber defense should cover not only the common subjects that are the minimum requirements in basic training for SDF personnel, but should also be revised to focus on subjects with a strong connection to cyberwar, such as international law and the protection of confidentiality. At the same time, education and training should be implemented in the Cyber Defense Group and the systems defense units of each Self-Defense Force, and a system should be established to enable units specializing in cyberwar to respond swiftly in the event of an emergency.

By combining these two policies, Japan should be able to create a system close to the Cyber Defense Unit of Estonia. In short, civilians who wish to contribute to national defense in the

---

[79] National Police Agency, "Saiba Bohan Borantia Katsudo no Tame no Manyuaru (Moderu)" [Manual for Cyber Crime Voluntary Activities (Model)], http://www.npa.go.jp/cyber/policy/volunteer/manual.pdf.

[80] Ministry of Defense, "Heisei 30 Nendo Yobi Jieikanho Boshu Yoko (Gino Kobo)" [FY2018 Recruitment Guidelines for Reserve Candidate Personnel (Open Skills Recruitment)], http://www.mod.go.jp/gsdf/jieikanbosyu/pdf/ y/30yobihoginouy.pdf

area of cybersecurity can be encouraged to play an active role in voluntary activities related to cybersecurity as a member of the pro-bono cyber defense organization during peacetime, as well as serve as a member of the specialized cyberwar unit as an SDF personnel through defense call-ups during an emergency.

Conclusion

This paper examined, through a comparison with Estonia's cybersecurity policies, the cybersecurity policies that Japan has implemented to date, how public-private partnership initiatives on the protection of critical infrastructure have advanced, which policies are superior in comparison with other countries, which areas are lagging behind with regard to the implementation of measures, and which measures need to be implemented going forward.

Estonia drew lessons from the large-scale cyberattack that struck in April 2007, and has positioned the protection of vital services as the issue of highest priority in its cybersecurity strategy. The RIA consolidates the authority for the supervision of planning, formulating, and execution of cybersecurity policies, and strengthens regulations over vital service providers through the development of legal systems. Vital service operators are actively involved in national policies, and in addition to promoting security measures for information systems, also participate in various cyber exercises to contribute to the strengthening of the cybersecurity of Estonia as a whole. Furthermore, volunteer cybersecurity engineers who played an active role in the large-scale cyberattack incident in Estonia have become members of the Cyber Defense Unit under the Estonian Defense League, a paramilitary organization. While engaging in their day jobs, they wear the uniform of the Estonian Defense League and engage in national defense missions in cyberspace when a cyber incident occurs at the national level. In August 2018, the Cyber Command was newly established in the Estonian Defense Forces, and attention should be paid to the cooperative system that will be established by the Cyber Command, which is an arm of the regular army, and the Cyber Defense Unit, which is a paramilitary organization. Such public-private partnership initiatives in Estonia can be applied to Japan's cybersecurity policies.

Japan has, till now, steadily promoted cybersecurity policies. However, the means of cyberattacks are becoming increasingly ingenious and complex. To respond flexibly and swiftly to changes in the threats, it is important not only to utilize the latest cybersecurity technologies, but also to take reference from best practices promoted by Estonia to develop a public-private partnership system that corresponds with Japan's characteristics. In particular, during Prime Minister Abe's visit to Estonia in January 2018, Japan's participation in NATO CCDCOE was approved. On top of that, during the visit to Estonia by Defense Minister Onodera in May the same year, the dispatch of the defense ministry's staff to NATO CCDCOE was approved.[81] Going forward, in addition to promoting cooperation in the cyber field between Japan and Estonia through the dispatch of defense ministry staff, the acquisition of information locally about public-private partnership initiatives in the field of cyber defense in Estonia is also expected to be reflected in Japan's cybersecurity policies.

Cyberspace is a new theater of war. Unlike other domains, it is highly dependent on private-

[81] Ministry of Defense, "Esutonia Boeiso Kaidan (Gaiyo)" [Japan-Estonia Defense Ministers' Meeting (Summary)], http://www.mod.go.jp/j/approach/exchange/nikoku/docs/2018/05/06_j-estonia_gaiyo.pdf

sector actors. To achieve cyber defense for the country, there are limitations to the response that can be delivered by the government and military organizations alone. Hence, it is necessary to put tireless effort into cooperating with private-sector actors to realize “deterrence through resilience.”

Tracing Criticisms of the "Basic Defense Force Concept" During the Second Cold War —Controversies over Japan's Defense Policy in the 1980s—*

CHIJIWA Yasuaki**

Abstract

This research discusses why Japan's "Basic Defense Force Concept" adopted earlier was maintained amidst the widely-discussed demise of détente and the arrival of the "Second Cold War" between the United States and the Soviet Union entering the 1980s. From the perspective that perceives the Basic Defense Force Concept as a "beyond-the-threat theory," the defense controversies that unfolded during the Second Cold War were waged between the Basic Defense Force Concept and criticisms of the Basic Defense Force Concept resembling the "counter-threat theory" based on the increasing threat recognition. As a result, the Basic Defense Force Concept was not abandoned, which probably might finish with the victory of the Basic Defense Force Concept against the "counter-threat theory." However, that was actually not the case. The Basic Defense Force Concept began to coexist with the "Idea of Defense Force Reinforcement," a competing theory to the Basic Defense Force Concept that took prominence during the Second Cold War, due to the "Idea of Attached Table Early Achievement" and the "Idea of Attached Table Revision and Concept Change," considered to be a competing theory to the Basic Defense Force Concept as well, due to the "Idea of Attached Table Revision and Concept Continuation."

Introduction

This research discusses why the "Basic Defense Force Concept (*Kibanteki Boeiryoku Koso*)," adopted in the "National Defense Program Outline (*Boei Keikaku no Taiko* or *Boei Taiko*) for FY 1977 and Beyond" (1976 NDPO) formulated on October 29, 1976, was maintained amidst the widely-discussed demise of détente (easing of tensions) and the arrival of the "Second Cold War (*Shin Reisen*)" between the United States and the Soviet Union entering the 1980s, based on official documents, the oral histories and interviews of related people, and more while taking up criticisms from inside and outside Japan regarding the concept as well as various discussions concerning the concept in the political process. Until now, although there has been discussion

* Originally published in Japanese in *Boei Kenkyusho Kiyo* [NIDS Security Studies], vol.21, no.2, March 2019. Some parts have been updated.

** Senior Fellow, National Security Policy Division, Center for Military History

regarding the rising criticisms of the Basic Defense Force Concept in the 1980s,[1] there has not been a sufficient explanation for why the concept was maintained despite this. Answering this question will lead to understanding of the sustainability of Japan's defense concept, the theoretical structure in the background, and the development of Japan's defense policy during the Second Cold War, and provide hints for future security policy.

On January 1, 1979, the U.S. and China normalized their diplomatic relations that had been antagonistic during the Cold War. Prior to this, Japan and China had normalized their relations on September 29, 1972. The Soviet Union, which had a disadvantage in the strategic environment due to Japan and the U.S.' reconciliation with China in the 1970s, turned to coercive activity abroad. Entering 1979, there were frequent activities around Japan by Soviet missile destroyers, cruisers, electronic reconnaissance aircraft, anti-submarine aircraft, and more. The regional threat posed by the Soviet Union increased with the confirmation by the Japan Defense Agency of Soviet ocean minesweeping augmentation (January 1979), weapons transport to Kunashiri Island and Etorofu Island (May), the Far East deployment of the *Minsk* aircraft carrier (July), as well as the construction of military base on Shikotan Island and the Far East deployment of supersonic, long-range Backfire bombers and mid-range SS-20 missiles (October)[2]. In addition, following the Iran hostage crisis at the American embassy in Iran on November 4, 1979, the Soviet Union suddenly invaded Afghanistan on December 24. Western countries were shocked that the Soviet Union had carried out military intervention outside its sphere of influence. President James E. Carter, Jr. announced the "Carter Doctrine" that called for protecting interests in the Persian Gulf on January 28, 1980, which caused the widely-discussed demise of the détente and the arrival of the Second Cold War between the U.S. and the Soviet Union. The tensions between the East and West soon extended to Northeast Asia.

The Basic Defense Force Concept defined Japan's ideal defense force as follows: "[T]he possession of the assorted functions required for national defense, while retaining balanced organization and deployment, including logistical support," "Japan will repel limited and small-scale aggression, in principle, without external assistance," "At this time, the present scale of defense capability seems to closely approach target goals of the above-mentioned concept," and Japan's defense concept "will be standardized so that, when serious changes in situation demand, the defense structure can be smoothly adapted to meet such changes." The premise of the Basic Defense Force Concept was a recognition that "the international political structure in this region - along with continuing efforts for global stabilization - will not undergo any major changes for some time to come, and that Japan's domestic conditions will also remain fundamentally stable."[3] In other words, there is no question that it was a defense concept premised on détente in the 1970s. Therefore, based on the rapid developments in the international situation following the formulation of the 1976 NDPO, the Basic Defense Force Concept began to be treated as a "enfant

---

1 Hideo Otake, *Nihon no Boei to Kokunai Seiji: Detanto kara Gunkaku he* [Japan's Defense and Domestic Politics: From Détente to Military Buildup] Sanichi Shobo, 1983; Akihiro Sado, *Sengo Nihon no Boei to Seiji* [Defense and Politics of Japan after the War] Yoshikawa Kobunkan, 2003; Takao Sebata, *Boei Keikaku no Taiko to Nichi-Bei Gaidorain* [The NDPO and the Guidelines for Japan-United States Defense Cooperation] Bokutakusha, 1998.

2 Otake, *Nihon no Boei to Kokunai Seiji*, pp.270-276.

3 "The National Defense Program Outline For FY 1977 and Beyond" (Approved by the National Defense Council and the Cabinet on October 29, 1976).

terrible" (Haruo Natsume, who contributed as the Agency's Director of the Defense Division to the Post-4th Defense Build-up Plan (*Boeiryoku Seibi Keikaku*) issues connected with formulation of the 1976 NDPO)[4].

From the perspective that perceives the Basic Defense Force Concept as a "beyond-the-threat theory (*datsu-kyoi ron)*," the defense controversies that unfolded during the Second Cold War were waged between the Basic Defense Force Concept and criticisms of the Basic Defense Force Concept resembling the "counter-threat theory (*kyoi taiko ron*)" based on the increasing threat recognition. As a result, the Basic Defense Force Concept was not abandoned, which probably means a finish with the victory of the Basic Defense Force Concept against the counter-threat theory. However, that was actually not the case as shown in this research. The Basic Defense Force Concept began to coexist with the "Idea of Defense Force Reinforcement (*Boeiryoku Zokyo Ron*)," a competing theory to the Basic Defense Force Concept that took prominence during the Second Cold War, due to the "Idea of Attached Table Early Achievement (*Beppyo Soki Tassei Ron*)" and the "Idea of Attached Table Revision and Concept Change (*Beppyo Shusei/Koso Henko Ron*)," considered to be a competing theory to the Basic Defense Force Concept as well, due to the "Idea of Attached Table Revision and Concept Continuation (*Beppyo Shusei/Koso Keizoku Ron*)." The Attached Table (*Beppyo*) showed a concrete plan for unit organization and equipment procurement of the NDPO.

Furthermore, the Idea of Defense Force Reinforcement mentioned here has the same meaning as the traditional counter-threat theory and the Required Defense Force Concept (*Shoyo Boeiryoku Koso*).

While the Idea of Attached Table Early Achievement also essentially means Basic Defense Force early achievement, the Idea of Defense Force Reinforcement and the Basic Defense Force Concept were perceived coexisting under the Idea of Attached Table Early Achievement because it was possible to avoid conceptual disputes (at the stage of the non-achievement of the attached table, the counter-threat theory and the beyond-the-threat theory were considered to be the same for carrying out defense force buildup) by focusing on the attached table. Moreover, against the Idea of Attached Table Revision and Concept Change, the concept of changing the defense concept accompanied by attached table revision to the counter-threat theory, the Idea of Attached Table Revision and Concept Continuation had the concept of it not being necessary to change the Basic Defense Force Concept even if there was revision of the attached table.

1. The "OK Personal Paper" and Rise to Prominence of the "Idea of Defense Force Reinforcement"

When Michita Sakata, who promoted the formulation of the 1976 NDPO, resigned from his post as Director General of the Defense Agency on December 24, 1976, those who succeeded him as Director General did not necessarily have positive sentiment toward the 1976 NDPO as he did. Ganri Yamashita, who served as Director General during the Masayoshi Ohira administration from December 1978, stated at the Diet on March 6, 1979 that "the current situation has certainly become more severe" in comparison to the international situation at the time of the

[4] National Graduate Institute for Policy Studies [hereafter GRIPS] (eds.), *Natsume Haruo Ororu Hisutori* [Oral History of Haruo Natsume] GRIPS, 2004, p.245.

formulation of the 1976 NDPO[5]. Although Joji Omura, who became Director General during the Zenko Suzuki administration in July 1980, stated, "There is no need to change the NDPO if the '1981 Mid-term Planning Estimates' (*Chuki Gyomu Mitsumori* or *Chugyo* estimates on the main work of the Self-Defense Forces (SDF) for the next 5 years) planned to be formulated in 1982 are in line with it." He also stated, "If a case occurs in which that does not happen…there would have to be discussion on such points in the National Defense Council or in a Cabinet meeting[6]." In a speech at a business leader meeting on March 28, 1979, Ground SDF Chief of Staff Shigeto Nagano, as a leader of the people in uniform, mentioned the deployment of 32 divisions of the Far Eastern Soviet Army, improvement of the performance of tanks and range of artillery, the presence of Soviet military bases on Kunashiri Island and Etorofu Island, the Far East deployment of the Kiev-class aircraft carrier *Minsk* and the increasing breadth of landing operations by helicopters, restrictions on the actions of the U.S. Seventh Fleet by the Far East deployment of the supersonic, long-range Backfire bombers, and more. He also stated, "The situation has changed, and we have to turn to revising the NDPO bit by bit in the near future."[7] This was the first time for a leader of the people in uniform to mention in an official capacity the necessity to revise the 1976 NDPO[8]. In addition, the changes in the situation surrounding the 1976 NDPO also affected the writing style of the *Defense White Paper*. The *FY1978 Defense White Paper* still stated that there had not been any major changes in the basic domestic and foreign situations from the time of the formulation of the NDPO, so defense force would be built up in accordance with the NDPO.[9] However, in the FY1979 edition, although it is stated that "…showing that the international situation around Japan includes factors of instability…severe factors are recognized in the situation," subtle phrasing is used that "it is believed there have been no drastic changes (*henkasitatoha ienaito mirareta*) in the conditions forming the premise of the outline."[10] At the Defense Councilor meeting on May 1, 1979 that deliberated the *FY1979 Defense White Paper*, a discussion took place on "…Explanation of NDPO: Simplification" according to the minutes.[11]

---

5 May 6, 1979, Minister Ganri Yamashita's response during the Budget Committee of the 87th House of Representatives, No. 20, the House of Representatives and the House of Councilors, Kokkai Kaigiroku [Minutes of the Diet] [Online] Available at: http://kokkai.ndl.go.jp/cgi-bin/KENSAKU/swk_dispdoc.cgi?SESSION=10576&SAVED_RID=1&PAGE=0&POS=0&TOTAL=0&SRV_ID=5&DOC_ID=8564&DPAGE=1&DTOTAL=22&DPOS=14&SORT_DIR=1&SORT_TYPE=0&MODE=1&DMY=11902.

6 November 25, 1980, Minister Joji Omura's response during the Cabinet Committee of the 93rd House of Councillors, No. 10, Kokkai Kaigiroku [Minutes of the Diet] [Online] Available at: http://kokkai.ndl.go.jp/cgi-bin/KENSAKU/swk_dispdoc.cgi?SESSION=10576&SAVED_RID=4&PAGE=0&POS=0&TOTAL=0&SRV_ID=5&DOC_ID=9633&DPAGE=1&DTOTAL=18&DPOS=2&SORT_DIR=1&SORT_TYPE=0&MODE=1&DMY=26321.

7 *Asahi Shimbun* (Asahi Newspaper), March 29, 1979.

8 Ibid.

9 *FY1978 Boei Hakusho* [Defense White Paper], p.81; See also Atsuyuki Sassa and Hajime Doba, "Kohan na Mondaiteiki de Kokumin no Rikai Kitai: 53 nenban Boei Hakusho no Shiten to Tokucho" [Expectations for Citizens' Understanding by Widespread Raising of Issues: Views and Characteristics of the FY1978 Defense White Paper] *Kokubo* [National Defense] 27:9, September 1978, p.8.

10 *FY1979 Defense of Japan* (English version), p.81.

11 "Dai 4 Kai Sanjikan Kaigi Giji Yoroku" [Abstract of Minutes from 4th Councilors Meeting] (May 1, 1979), Historical Division of the Defense Agency, *Sanjikan Kaigi Giji Yoroku, Showa 54 Nen* [Abstract of Minutes from Councilors Meeting (1976)] ½, p.1137 (Main building 4A-034-00/2005 Defense 01221100) [Archived in National Archives of Japan].

At this time, Japan's ally the U.S. began to intervene in earnest in Japan's defense force buildup. Secretary of Defence Harold Brown, who met with Foreign Minister Saburo Okita on March 20, 1980 during Okita's visit to the U.S., stated, "The Government of the U.S. hopes for (Japan) to have a steady, remarkable increase in its defense spending.[12] At the Japan-U.S. Summit Meeting between Prime Minister Ohira and President Carter in Washington, D.C. on May 1, 1980, President Carter himself stated, "I would like Japan's efforts to be made to quickly achieve a pre-existing governmental plan in order to respond to the new situation," implicitly requesting advancing implementation of the Mid-term Planning Estimates.[13] On December 12, 1980 as well, during his visit to Japan, Brown requested Prime Minister Suzuki to raise defense spending 9.7% above the previous fiscal year within the FY1981 budget compilation.[14]

Amidst this, the main leadership of the so-called "Idea of Defense Force Reinforcement" that criticized the Basic Defense Force Concept was Hisahiko Okazaki, who served as the Japan Defense Agency Councilor (in charge of international relations) from July 1978 as a transferred official from the Ministry of Foreign Affairs. In May 1979, Okazaki wrote a paper entitled "Judgment of the Situation of the NDPO (Draft)," which he called the "OK personal paper" as an homage to the thesis entitled "Concept for Japan's Defense Buildup" (also known as the "KB personal paper") by Takuya Kubo, the former Director-General of the Defense Bureau.[15] The KB personal paper was a source of the Basic Defense Force Concept. Within it, Okazaki wrote, "In the 1976 NDPO, judging from the big-picture perspective, synergy is being built up from specific military force to amount of equipment to formation, and organization is being built up with the understanding that the specific program will not change if there are no changes to the 'basic' situation." However, he also wrote, "The 'five conditions' (the Japan-U.S. Security Arrangement, peaceful coexistence between the U.S. and the Soviet Union, confrontation between China and the Soviet Union, closer relations between the U.S. and China, and maintenance of the status quo on the Korean Peninsula) were not the NDPO itself, but part of the explanation." It is certainly true that the recognition of the international environment was not from the 1976 NDPO but rather as indicated in the FY1976 and FY1977 editions of the *Defense White Paper*.[16] Thus, because the judgment of the situation and program content of the 1976 NDPO "originally had no direct connection," he pointed out that it was possible to separate them and only discuss the program, and advocated the following.

---

12 *Asahi Shimbun* (Asahi Newspaper), March 22, 1980.

13 Ibid, May 2, 1980 (evening paper).

14 Ibid, December 13, 1980.

15 In addition to Okazaki, people within the Inner Bureau at this time such as Defense Division Director Hisakatsu Ikeda (November 1978-December 1980) also criticized the Basic Defense Force Concept. GRIPS (eds.), *Hoshuyama Noboru Oraru Hisutori* [Oral History of Noboru Hoshuyama] (below) GRIPS, 2005, p.59.

16 The *FY1977 Defense White Paper* states that "major changes in the international environment" would correspond to major changes occurring to the following various points. A) Effective future maintenance of the Japan-U.S. security system. B) Efforts to avoid nuclear war and large-scale conflict apt to lead to nuclear war by the United States and the Soviet Union. C) No fundamental resolution of Sino-Soviet confrontation, allowing for minor improvement. D) Continued adjustment in Sino-American relations. E) Generally unchanged Korean Peninsula situation along present lines and continued unlikelihood of at least major conflict there. *FY1977 Defense of Japan* (English version), pp.55-56.

> "As the future department working system, without losing sight of the big-picture international situation, based on detailed analysis of the Soviet Union's military capabilities and the results of research under the Guidelines (the Guidelines for Japan-U.S. Defense Cooperation formulated on November 27, 1978), objective, scientific operations will be carried out that calculate the defense force that Japan should build up, and those results must be Japan's new defense concept substituting for the "NDPO" that is already finishing its historic mission."[17]

Okazaki later stated that the Basic Defense Force Concept was "a strategy that completely does not envision potential enemies, and would be fine with a full selection of defense equipment such as swords and battle flags," and also stated, "I thought it was quite stupid, and never once used Sakata's concept when answering questions in the Diet when I was Defense Councilor."[18]

Against counter-threats, the Idea of Defense Force Reinforcement that represented the OK personal paper, Noboru Hoshuyama, who was deeply involved in the formulation of the 1976 NDPO as a senior staff member of the Defense Division (and held positions following the formulation of the 1976 NDPO including Head of the System Analysis Office to Head of Defense Planning, 4th Contract Section Head of the Central Procurement Office, and 2nd Surveying Section Head of the Defense Bureau), critically reacted, stating, "(The Idea of Defense Force Reinforcement insisted) 'what we have now is based on the NDPO, so nothing can be done to break away from the NDPO.' It was a leap in logic."[19] Hoshuyama also stated in regard to the U.S. pressuring Japan on defense that the "anti-NDPO faction in Japan…caused such statements in a foreign country."[20] Hoshuyama reflected that discussions took place between "people who could understand that great efforts were required to achieve this (the 1976 NDPO), people who also understood what was explained by Kubo (such as beyond-the-threat theory), and people who were critical of such concepts and thought they wanted to achieve something in their own age."[21]

2. The Idea of Attached Table Early Achievement

However, the conflict between the Basic Defense Force Concept and the Idea of Defense Force Reinforcement has become unexpectedly tranquil.[22] This was because of the appearance of the argument of the concept of the early achievement of specific Basic Defense Force military size indicated in the attached table of the 1976 NDPO, also known as the "Idea of Attached Table Early Achievement."

On April 2, 1979, Prime Minister Ohira himself established his Comprehensive Security Research Group as his personal advisory committee, entrusting it to consider security policy from

---

17 "'Boei Keikaku no Taiko' no Josei Handan ni Tsuite (Soan)" [Judgment of the Situation of the NDPO (Draft)] (May 6, 1979), p.1 (quote from Sado, *Sengo Nihon no Boei to Seiji*, pp.316-318).

18 Hisahiko Okazaki, *Kokusai Josei Handan Hanseiki* [International Situation Judgments: 50 Years] Ikuhosha, 2005, pp.84-85.

19 GRIPS (eds.), *Hoshuyama Oraru Hisutori* (Oral History of Hoshuyama) (below), pp.58-59.

20 *Ibid.*

21 *Ibid.*

22 See also Keiji Omori, *Waga Kuni no Kokubo Senryaku* [Japan's National Defense Strategy] Naigai Shuppan, 2009, pp.266-267.

the so-called "comprehensive security (*Sogo Anzen Hosho*)" perspective.[23] Comprehensive security had the recognition that security policy until then was biased toward military matters, and based on the first oil crisis that accompanied the outbreak of the Fourth Arab-Israeli War since October 6, 1973 and other events, is a concept that perceives security issues from wide perspectives including economic issues and energy issues. In the following year on June 12, 1980, Prime Minister Ohira suddenly passed away, but the Group submitted the "Comprehensive Security Research Group Report" to Acting Prime Minister Masayoshi Ito on July 2. Within the report, the Group requested not only a review of the 1976 NDPO but also its "early implementation."

> "Maintaining the Japan-U.S. Security Arrangement, maintaining denial power, and building up the Basic Force that are all established within the NDPO are not being realized. That is a problem."
> "Filling the gap (meaning maintaining the Japan-U.S. Security Arrangement, building up denial power, and building up the Basic Force) are matters that should be given high priority. That is just for implementing the NDPO. In reality, the fact that what the government decided has not been implemented must be said to be governmental negligence. The government has an obligation to clarify to the citizens that even the minimum necessity of the denial power is not being built up in the current situation, and swiftly implement the NDPO."
> "Of course, the NDPO itself has the characteristic that it should be revised according to the changes in the international situation. However, if Japan's military force is premised strictly as being for self-defense, as long as there are close relations between Japan and the U.S., there is an upper limit on the military force that is necessary, and that upper limit should not be shifted carelessly."[24]

---

[23] The members were as follows. Chairman: Masamichi Inoki, Chairman, Research Institute for Peace and Security. Policy Researchers and Executive Secretaries: Tsuneo Iida, Professor, Nagoya University; Masataka Kosaka, Professor, Kyoto University; Policy Researchers: Hiroshi Akuto, Assistant Professor, University of Tokyo; Jun Eto, Professor, Tokyo Institute of Technology; Toshio Oosu, International Organization Section Chief, International Finance Division, Ministry of Finance; Tokio Kano, Vice President, Energy Conservation Center, Tokyo Electric Power Company; Hiroo Kinoshita, Director, Secretarial Division, Minister's Secretariat, Ministry of International Trade and Industry; Hiroshi Kimura, Professor, Hokkaido University; Kimitaka Kuze, Deputy Director-General, Minister's Secretariat, Ministry of Home Affairs; Kisho Kurokawa (Architect); Kenji Konosu, Head of Planning Office, Minister's Secretariat, Ministry of Agriculture, Forestry and Fisheries; Masamori Sase, Professor, National Defense Academy of Japan; Atsuyuki Sassa, Director General, Personnel and Education Bureau, Defense Agency; Seizaburo Sato, Professor, University of Tokyo; Ayako Sono (Writer); Yasushi Tanahashi, Deputy Vice-Minister, Minister's Secretariat, Ministry of Transport; Tooru Toyoshima, Head, Paris-Japan Trade Center, Japan External Trade Organization; Mineo Nakajima, Assistant Professor, Tokyo University of Foreign Studies; Koji Watanabe, Councillor, Minister's Secretariat, Ministry of Foreign Affairs; Shoichi Watanabe, Professor, Sophia University; Policy Researchers and Secretaries: Yasuhiko Okada, Assistant to the Director, Research Planning Division, Minister's Secretariat, Ministry of Finance; Yasuo Saito, Assistant to the Director, Northeast Asia Division, Asian Bureau, Ministry of Foreign Affairs; Advisors: Kenichiro Hirano, Assistant Professor, University of Tokyo; Mitsuru Yamamoto, Professor, Hosei University.

[24] Comprehensive Security Research Group, *Sogo Anzen Hosho Kenkyu Guruupu Hokokusho* [Comprehensive Security Research Group Report] (July 2, 1980), Research Office of Akihiko Tanaka, Institute for Advanced Studies on Asia, The University of Tokyo, *Detabesu Sekai to Nihon* [Database World and Japan] [Online] Available at: http://www.ioc.u-tokyo.ac.jp/~worldjpn/documents/texts/ JPSC/19800702.O1J.html.

The Japan Defense Agency also publicized that it took the same position as the Comprehensive Security Research Group in answers in the Diet and the *Defense White Paper*. In this process, the Japan Defense Agency referenced the interpretation resembling counter-threat theory of the Basic Defense Force Concept. At the House of Representatives Committee on Cabinet on November 4, 1980, Director Omura stated in the Diet, "I believe that it is not true to say that there was absolutely no consideration for potential threats in the foundation (of the Basic Defense Force Concept)," "In the *Defense White Paper* the following year as well, there will also be an explanation at an appropriate page length concerning the issue of such threats."[25] (In the *FY1977 Defense White Paper* mentioned by Omura, there was certainly the statement, "The essential, universal nature of defense is preparation to meet external threats. Obviously, any defensive system which disregards external threats is inherently untenable." Although it was stated, "The qualitative requirements of the Standard (Basic) Defense Force are defined as those elements of defense capability needed to confront threats," at the same time, beyond-the-threat theory-like phrases were used such as "This approach, which centers on quantitatively assessing defense capability based on peacetime defense preparedness…"[26] and "conclusiveness in a certain sense,"[27]and among the uniform group there were people who were dissatisfied because they interpreted the Basic Defense Force Concept as the counter "low-threat" theory). The opposition parties did not accept these answers. While the government stated that the NDPO was not created with specific countries as threats, on the other hand, in response to beyond-the-threat theory criticism, it was answered that it was not the case that there was absolutely no envisioning of threats because limited and small-scale aggression was envisioned, but that was strange.[28] In response, Defense Bureau Director General Akira Shiota (June 1980-July 1982) answered in line with the Comprehensive Security Research Group report, stating, "Current buildup is being carried within the bounds of the NDPO. Moreover, in the current situation, when I thought about the current situation in which the attached table created based on that concept has not yet been attained, I view matters such as the Soviet army's recent reinforcement in the Far East to be increasing potential threats. Based on this international situation, we are saying that at the very least, the NDPO's attached table created through the Basic Defense Force Concept should be swiftly achieved."[29] On the 25th of the same month at the House

---

25 November 4, 1980, Minister Joji Omura's response during the Committee on Cabinet of the 93rd House of Representatives, No. 7, Kokkai Kaigiroku [Minutes of the Diet] [Online] Available at: http://kokkai.ndl.go.jp/cgi-bin/KENSAKU/swk_dispdoc.cgi?SESSION=25805&SAVED_ RID=1&PAGE=0&POS=0&TOTAL=0&SRV_ID=5&DOC_ID=3874&DPAGE=5&DTOTAL=368&DPOS= 88&SORT_DIR=0&SORT_TYPE=0&MODE=1&DMY=25863.

26 *FY1977 Defense of Japan* (English version), pp.52-53, 74.

27 *FY1977 Defense White Paper*, p.52. The nuance of this part in *FY1977 Defense of Japan* (English version) is slightly differ from the original Japanese text.

28 November 4, 1980, House of Representatives member Yuichi Ichikawa's question during the Committee on Cabinet of the 93rd House of Representatives, No. 3, Kokkai Kaigiroku [Minutes of the Diet] [Online] Available at: http://kokkai.ndl.go.jp/cgi-bin/KENSAKU/swk_dispdoc.cgi?SESSION=25805&SAVED_RID=1&PAGE=0&POS=0&TOTAL=0&SRV_ID=5&DOC_ID=3874&DPAGE=5&DTOTAL=368&DPOS=88&SORT_DIR=0&SORT_TYPE=0&MODE=1&DMY=25863.

29 November 4, 1980, Government Delegate Akira Shiota's answer during the Committee on Cabinet of the 93rd House of Representatives, No. 7, Kokkai Kaigiroku [Minutes of the Diet] [Online] Available at: http://kokkai.ndl.go.jp/cgi-bin/KENSAKU/swk_dispdoc.cgi?SESSION=25805&SAVED_RID=1&PAGE=0&POS=0&TOTAL=0&SRV_ID=5&DOC_ID=3874&DPAGE=5&DTOTAL=368&DPOS=88&SORT_DIR=0&SORT_TYPE=0&MODE=1&DMY=25863.

of Councillors Committee on Cabinet, Shiota spoke further, "Although I believe the Basic Defense Force Concept is typically spoken of as a concept of beyond-the-threat theory, so to speak, I believe that is not necessarily the case."[30]

The thinking seen in the responses by the Japan Defense Agency in the Diet are organized in the *FY1981 Defense White Paper*. While indicating that "the Defense Agency acknowledges that the circumstances have changed in various ways since 1976 when the outline was determined," the white paper states the following:

> "It takes the stand that when the outline is reexamined, consideration should be given not only to a change in the international situation but also to various trends in Japan and the progress of the outline's implementation. For the immediate future, the agency considers it imperative to attain the level of defense capability as envisioned by the outline – which can become a nucleus for a shift to a stronger posture at any time – as soon as possible. Therefore, it has no thought of revising the outline immediately."[31]

In other words, based on the increasing threat posed by the Soviet Union, because the current defense force still had not reached the Basic Defense Force level indicated in the 1976 NDPO attached table, the attached table would be swiftly achieved. In addition, as the white paper stated that the "(the level of defense capability as envisioned by the NDPO) can become a nucleus for a shift to a stronger posture at any time – as soon as possible," it does not forget to reference the so-called "expansion clause" in the 1976 NDPO of "it (This defense capability) will be standardized so that, when serious changes in situations so demand, the defense structure can be smoothly adapted to meet such changes." GSDF member Takeshi Oba indicates regarding the Idea of Attached Table Early Achievement, "At a glance, unrelated to increasing threats, it takes the form of continuing defense buildup based on the Basic Defense Force Concept, but in reality it reinforces defense force linked with increasing threats, and can be interpreted as adjusting the trajectory by skillfully taking the Required Defense Force Concept."[32]

Through the Idea of Attached Table Early Achievement in this way, it became possible for the Basic Defense Force Concept and the Idea of Defense Force Reinforcement to unexpectedly coexist at the stage of the attached table being unachieved. Additionally, from the standpoint of the people in uniform, it was not a review of the Basic Defense Force Concept, but rather firstly a shift to advocating that a review was necessary for the cap of using 1% of GNP for defense in

---

30 November 25, 1980, Government Delegate Akira Shiota's answer during the Committee on Cabinet of the 93rd House of Representatives, No, 10, Kokkai Kaigiroku [Minutes of the Diet] [Online] Available at: http://kokkai.ndl.go.jp/cgi-bin/KENSAKU/swk_dispdoc.cgi?SESSION=28976&SAVED_RID=1&PAGE=0&POS=0&TOTAL=0&SRV_ID=5&DOC_ID=7568&DPAGE=5&DTOTAL=368&DPOS=94&SORT_DIR=0&SORT_TYPE=0&MODE=1&DMY=29100.

31 *FY1981 Defense of Japan* (English version), p.173.

32 Takeshi Oba, "Kibanteki Boeiryoku ni Motozuku Shorai no Rikujo Boeiryoku no Arikata" [Ideal Future Ground Defense Force Based on Basic Defense Force] *Rikusen Kenkyu* [Studies of the Land Warfare] 48:3, March 2000, p.31.

order to build the Basic Defense Force.[33] Originally at the time of the establishment of the 1% of GNP cap, the anticipated figure for 1% of GNP was a little over 12 trillion yen, and although the expenses cap in the Japan Defense Agency's preliminary calculations was 8-9 trillion yen, so it showed a considerable surplus. Following this the defense budget surplus under the 1% of GNP cap was lost because the economic growth rate was more sluggish than predicted and expensive main equipment was stockpiled in large amounts. For example, Hideo Miyoshi, who contributed as GSDF Chief of Staff in the formulation of the 1976 NDPO, stated at the Liberal Democratic Party (LDP) Defense Force Buildup Subcommittee on October 2, 1984 following his retirement, "The 1% figure was not used during the deliberations for drawing up the NDPO. …It would be desirable to withdraw this (the 1% of GNP cap) and carry out the NDPO according to its intent."[34] (Later, the 1% of GNP cap was abolished by a Cabinet decision on January 24, 1987.)[35]

When he wrote the paper "Grand Strategy for Japanese Defense Second Draft," Okazaki, the author of the OK personal paper, made efforts to "organize the issues through flexible interpretations in accordance with the NDPO ideas as much as possible in order to simplify the future transfer and developments from the NDPO.[36] In his new paper, although he stated, "The 'minimum' necessary amount is originally relative to the surrounding military capabilities, and it should not be denied that the surrounding military force has greatly changed compared to 1976," he also states, "At the present time, there are existing only defense buildup goals decided by the government, as well as unachieved goals, and it is firstly an urgent matter to achieve these goals."[37] In addition, on June 14 he addressed Omura, stating in his personal opinion entitled "Judgments and Countermeasures regarding Japan's Defense Force Reinforcement Requests by the U.S." that "it is fully expected that (the future results of Japan-U.S. consultations) will be to find common ground between the NDPO's goals and the proposals by the U.S. However, in any event, the early achievement of the NDPO is increasingly important as a midway goal, and it is not considered necessary to issue the conclusions of the talks within this fiscal year."[38] He thus actually amended the position he worked out in the OK personal paper and returned to the Ministry of Foreign Affairs in the same year.

On July 23, 1982 at a National Defense Council meeting discussing the 1981 Mid-term Planning Estimate that was decided the same day, the Japan Defense Agency reported,

---

33 National Institute for Defense Studies [hereafter NIDS] (eds.) "Muramatsu Eiichi Oraru Hisutori" [Oral History of Eiichi Muramatsu] in NIDS (eds.), *Oraru Hisutori, Reisenki no Boeiryoku Seibi to Domei Seisaku* [Oral History, Defense Buildup and Alliance Policy During the Cold War] (3) NIDS, 2014, pp.300-302. Orient Shobo Editorial Department, *Jieitai Tatakawaba: Boei Shutsudo* [If SDF Battle: Defensive Mobilization] Orient Shobo, 1976, pp.300-302.

34 "Boeiryoku Seibi Sho Iinkai" [Defense Force Buildup Subcommittee], Omura Joji Kankei Bunsho [Joji Omura-Related Documents] III-1-9-7 [Archived in Center for Modern Japanese Legal and Political Documents, University of Tokyo].

35 "Kongo no Boeiryoku Seibi ni tsuite" [Future Defense Force Buildup] (Approved by the National Defense Council and the Cabinet meeting on January 24, 1979).

36 "Koto Setsumeian, 5 gatsu 13 nichi, Okazaki Ki" [Oral Explanation Draft, May 13, Okazaki's Writing] pp.2-3, *Hoshuyama Noboru Kankei Bunsho* [Noboru Hoshuyama-Related Documents] (63-1), pp.3-4 [Archived in the Modern Japanese Political History Materials Room of the National Diet Library in Japan].

37 Hisahiko Okazaki, "Nihon no Boei Senryaku Dai 2 Ko" [Grand Strategy for Japanese Defense Second Draft] (March 25, 1981), pp.23-24. *Hoshuyama Kankei Bunsho* [Hoshuyama-Related Documents] (63-2).

38 Councillor Okazaki, "Beikoku ni Yoru Waga Boeiryoku Zokyo Yosei ni tsuite Handan to Taisaku" [Judgments and Countermeasures regarding Japan's Defense Force Reinforcement Requests by the U.S.] (56.6.14), p.5, *Omura Kankei Bunsho* [Omura-Related Documents] (III-1-7-3).

"Compared to 1976 when the NDPO was formulated, the recent international military situation surrounding Japan is increasingly severe due to the considerable reinforcement of the Soviet Union's Far Eastern Army and other vigorous activities. On the other hand, the current situation of Japan's defense force has not reached the scale determined in the NDPO and has various issues. There is still a gap with the level of the NDPO. By correcting such substantive and qualitative deficiencies, major enhancement of Japan's defense capabilities can be expected compared with the current situation."[39]

3. Defense Pressure on Japan by the U.S. and the Idea of Attached Table Revision and Concept Change

On the other hand, even after the change from the Carter administration to the Ronald W. Reagan administration on January 20, 1981, the U.S. still did not change its stance of requesting Japan to reinforce its defense force. On March 9, 1981 at a press conference, U.S. Ambassador to Japan Michael J. Mansfield, who retained his post after the administration change, from the position that stressed defense force content and "role-sharing" between Japan and the U.S. more than defense spending numbers as favored by the previous Carter administration, stated that it was hoped that Japan would take a responsibility for Japanese mainland and the surrounding waters, where there was a shortage of military power accompanying the deployment change of the U.S. Seventh Fleet to the West Indian Sea, and mentioned strengthening Japan's anti-submarine capabilities and air defense.[40] At the time, the U.S. had adopted the "Swing Strategy" that would divert the U.S. fleet and others in the Asia-Pacific to Europe if Europe was attacked by the Soviet Union, and if that happened, it would need an expanded role by Japan in defense fields in order to fill the gap. It was hoped that the SDF would guard U.S. aircraft carrier mobile troops, detect Soviet submarines through escort vessels and antisubmarine aircraft, place blockades on the Soya, Tsugaru, and the Tsushima Straits, and other actions. The Soviet navy had 100 submarines in the Pacific Ocean alone at the time, while the U.S. Seventh Fleet only had 25 antisubmarine aircraft.[41]

In regard to Japan's concept of the Idea of Attached Table Early Achievement, in a discussion between Foreign Minister Masayoshi Ito, who was visiting the U.S., and Secretary of State Alexander M. Haig, Jr., Ito stated, "The government intends to make efforts to quickly achieve the defense force level decided in the NDPO," and it is recorded that this was conveyed in the meeting to the U.S. side.[42] However, after this on the same day during a meeting with Secretary of Defense Caspar W. Weinberger, Weinberger pointed out to Ito that "compared to the time the NDPO was

---

[39] "Kokubo Kaigi ni okeru Boeicho no Hokoku Yoshi" [Defense Agency's Report Summary in the National Defense Council] (July 23, 1982). However, as Chairman of the Joint Staff Council Tsugio Yada stated in a speech during the business leader meeting on May 7, 1981, "The NDPO has become unsuitable for the situation due to the changes in the international situation," among the people in uniform there was still a tendency to call for revision of the 1976 NDPO. *Asahi Shimbun* (Asahi Newspaper), May 7, 1981.

[40] *Asahi Shimbun* (Asahi Newspaper), March 10, 1981. See also Yasuaki Chijiwa, *Taishitachi no Sengo Nichi-Bei Kankei – Sono Yakuwari wo Meguru Hikaku Gaikoron 1952-2008* [The Ambassadors and Post-war Japan-U.S. Relations: Diplomatic Consideration on Their Roles 1952-2008] Mineruva Shobo, 2012, pp.133-134.

[41] James E. Auer, "Engaging Japan: An American Naval Officer's Relationship with Japan during the Cold War," *Journal of American-East Asian Relations* 15 (2008), p.97.

[42] "Ito Gaimu Daijin Heigu Kokumu Chokan Kaidan" [Discussions Between Foreign Minister Ito and Secretary of State Haig], p.4, *Omura Kankei Bunsho* [Omura-Related Documents] (III-1-3-9).

formulated, the international situation was changing."[43] At a press conference following his return to Japan, Ito stated that he did not interpret Weinberger's statement as a request to review the NDPO.[44] However, according to U.S. Department of Defense documents, there was spreading recognition within the Department until June that "We believe the outline has become obsolete and needs to be revised."[45] James E. Auer, who served as Special Assistant for Japan in the Office of the Secretary of Defense for close to 10 years from April 1979 during the Carter administration to August 1988 during the Reagan administration, reflects, "To Americans, at least, *Taiko* strategically was almost meaningless. Japan will deal with small-scale attack, but Japan's only potential enemy was the Soviet Union. And there is no way the Soviet Union will make a small-scale attack. So that part, we thought, was meaningless. Attached to the *Taiko* was the Standard (Basic) Defense Force, *beppyo*, annexed. And *beppyo* was reasonable. However, Japan didn't have forces around in the *beppyo*. So *Taiko* itself look us to be strategically not logical. And the *beppyo* was a goal. But Japan didn't have a capability, that kind of force didn't exist, and we didn't see any schedule or plan to achieve that level."[46]

From June 10-12, 1981, the 13th Japan-U.S. Security Subcommittee (SSC) was held in Hawaii. During the discussions, the Japanese side approached the Idea of Attached Table Early Achievement with a policy of conveying, "We consider it a major step forward that the goal is beginning to be seen for achieving the defense force level determined in the NDPO, which had not been foreseen to be achieved until now, in the (to be formulated in the following year) 1981 Mid-term Planning Estimates."[47] In response, according to the memo of Defense Bureau Director-General Shiota, one participant from the U.S., Assistant Secretary of Defense for International Security Affairs Francis J. West, concluded that the NDPO was "out of date," and pressed the Japanese side for more defense efforts.[48] Furthermore, the U.S. side presented the following concrete proposal for requests such as defense of surrounding sea and airspace, defense of 1,000 nautical miles of sea lanes, and response capability buildup against the Soviet Union's Backfire aircraft.

- 12 air force units of fixed-wing antisubmarine aircraft, 125 P-3C aircraft (the attached table level was 10 air force units of aircraft excluding 6 air force units with HSS2 patrol helicopters from 16 air force units of land-based anti-submarine aircraft. An additional 80 P-3C aircraft were needed)
- 5 escort flotillas of antisubmarine ship units for maneuvering purposes, 70 antisubmarine ships, 20 submarines (the attached table had 4 escort units, about 60 ships and 16 ships for each)
- 14 air force units of interceptor aircraft (the attached table level was 10 air force units of aircraft. A further 80 F-15 aircraft were needed for the additional 4 air force units)

---

43 *Asahi Shimbun* (Asahi Newspaper), March 27, 1981 (evening paper).

44 Ibid.

45 Memorandum for Secretary of Defense, June 30, 1981, No. 00906, Japan and the United States: Diplomatic, Security, and Economic Relations, Part II: 1972-1992, National Security Archive (Washington, D.C.).

46 Author's interview with James E. Auer, November 7, 2012, Tokyo.

47 "Jieitai no Heiryoku Tassei Gaikan ni tsuite no Setsumei (An)" [Explanation Regarding the SDF Force Achievement Outline (Draft)] (56.5), Omura Kankei Bunsho [Omura-Related Documents] (III-1-4-14).

48 "Boeikyokucho Memo" [Defense Bureau Director-General Memo] (6.15), Omura Kankei Bunsho [Omura-Related Documents] (III-1-4-4).

- 2 air force units of early warning aircraft, 16 E-2C airborne early-warning system (the attached table level was 1 air force unit)
- 3 months' worth of ammunition storage quantity (not written about in the attached table)[49]

The U.S. requests at the 13th SSC shocked Japan (Foreign Minister Sunao Sonoda used the expression "asking Japan to build a 10 story building out of a 1-story house[50]). At a press conference after the SSC, Administrative Vice-Minister of Defense Toru Hara, who had attended, said that against the Japanese attendees discussed based on the Idea of Attached Table Early Achievement, in regard to the SDF's battle continuation capabilities, combat readiness, and modernization, in particular air defense and antisubmarine capabilities, "In the U.S. side opinion, there are some points beyond the framework of the NDPO," "in the regard to the NDPO itself, the U.S. side might think that the time of its enactment and the current circumstances were different."[51] In addition, Hara stated in response to a reporter's question that it seemed the U.S. side was saying that Japan could not handle even small-scale aggression, "There were people who made statements like that."[52] In respond to these requests by the U.S., Japan responded, "It would be troubling to force out the NDPO. It is not possible to review the NDPO from the current domestic situation. The priority is to achieve the NDPO level."[53] In the end, Hara had to generalize by stating, "There was a clash of opinions with nothing but requests to 'make more efforts' by the U.S. side. Although the Japanese side was thinking within the boundaries of the NDPO, the U.S. side was thinking of throwing out the NDPO. They were completely different views."[54] Shiota says, "We thoroughly said we wanted to quickly achieve the lines decided by the NDPO's attached table. We said we would not listen at all to being told to do this or that for such and such purposes while not being able to reach that. That was our basic stance."[55] Further, Shiota says he did not show the U.S. side counter-threat theory-like interpretation of the Basic Defense Force Concept.[56]

However, the U.S. side did not accept this. On the 29th of the same month, Defense Agency Director General Joji Omura visited the U.S. to meet with Secretary of Defense Weinberger. It is recorded in Omura's memo that Weinberger stated, "Your efforts leave something to be desired in terms of timing aspects and in nature. Change the 1976 program."[57] On April 26, 1982 the following year at a press conference with Japanese press organizations in Hawaii, Pacific Commander in Chief Robert L. J. Long stated, "The 1976 NDPO is out of date now when the Soviet Union

---

49 *Asahi Shimbun* (Asahi Newspaper), June 16, 1981. See also Fumiaki Nishiwaki, "Shiireen Boei he "Kyodo Sakusen" – Fukamaru Nichi-Bei Domei Kankei" [Toward Defense of Sea Lanes "Joint Operations" – Deepening Japan-U.S. Alliance Relations], *Sekai Shuho* [World Weekly Report] 63:37 (September 21, 1982), p.15.

50 *Asahi Shimbun* (Asahi Newspaper), June 18, 1981.

51 Ibid, June 15, 1981 (evening paper).

52 "Jimu Jikan Kaiken (SSC Shuryogo)" [Press Conference by the Administrative Vice-Minister of Defense (Following the SSC)] (June 14), p.6, Omura Kankei Bunsho [Omura-Related Documents] (III-1-4-1).

53 *Asahi Shimbun* (Asahi Newspaper), June 15, 1981 (evening paper).

54 Ibid.

55 Japanese Modern Historical Manuscripts Association (eds.), *Shiota Akira Oraru Hisutori* [Oral History of Akira Shiota], Japanese Modern Historical Manuscripts Association, 2006, p.117.

56 Author's Interview with Akira Shiota, April 2, 2013, Tokyo.

57 "Wainbaga Kaidan Memo" [Weinberger Meeting Memo], Omura Kankei Bunsho [Omura-Related Documents] (III-1-6-1).

threat is increasing."[58] The gist of Long's comment was incorporated in the FY1983 edition of the *Report on Allied Contributions to the Common Defense*, which states, "The 1976 NDPO did not address the serious issues of sustainability of Japan's defense forces, the requirement for sea-lane defense protection, and has otherwise also grown seriously out of date."[59] According to Japan Defense Agency analysis at the time, "A trend is seen in the U.S. Congress of linking trade deficits with Japan with Japan's defense efforts."[60] Haruo Natsume, who became Deputy Vice-Minister at the time (June 1980-July 1982), recalls, "The reality was that the Japanese side was extremely surprised and did not know what to do."[61]

The Basic Defense Force Concept and the Idea of Defense Force Reinforcement, which was originally a competing theory, could temporarily coexist at the stage in which the attached table was not achieved, but this kind of discussion would change when the U.S. side issued a request to not finish the attached table, and a review of the attached table itself is needed. Additionally, as Natsume states, "In the end, it (the pressure about defense from the U.S. on Japan) later changed to voices in Japan calling for a review of the NDPO," [62] pushed by the U.S. request for reinforcing defense force, the discussion strengthened on a review of the 1976 NDPO centered on influential LDP members on defense issue such as LDP Security Affairs Research Council Chairman Asao Mihara.[63]

On July 18, 1981 immediately following the 13th SSC, at the taping of a TV program, Mihara disclosed that the LDP Security Affairs Research Council was promoting consideration of a review of the NDPO.[64] After this the formulation of the 1981 Mid-term Planning Estimates passed, and on December 21, 1984, the LDP Policy Affairs Research Council, Security Affairs Research Council, National Defense Division, and the Special Committee on the Military Base Affairs acknowledged the "Proposal Regarding Defense Force Buildup" that clarified that "reconsideration would be started regarding the NDPO."[65] On September 18, 1985, there was formulation of the 1986 Medium Term Defense Program (*Chuki Boeiryoku Seibi Keikaku* or *Chukibo*), which was a 5-year program that was raised in status from Mid-term Planning Estimates to a government program and determined necessary expenses. On October 6, the LDP decided to begin considerations regarding a review of the NDPO including not only the attached table but also the basic concept.[66] In other words, the idea was to change the defense concept to accompany the case of having to amend the attached table differ from the early achievement of the attached table in order to strengthen defense force. In the Diet in April 1986, LDP House of Councillors Member Masao Horie, who was also the former Commanding

---

58 *Asahi Shimbun* (Asahi Newspaper), April 28, 1982.

59 U.S. Department of Defense, *Report on Allied Contributions to the Common Defense: A Report to United States Congress, 1983* (Washington, D.C.: Department of Defense, 1983), p.55.

60 Japan Defense Agency, "Showa 57 Nendo Boei Yosan ni taisuru Beigawa no Hankyo ni tsuite" [The U.S. Reaction to the FY1982 Defense Budget] (57.1.8), p.1, Doba Bunsho [Doba Documents] (E-49), (Archived in the Research Institute for Peace and Security).

61 GRIPS (eds.), *Natsume Oraru Hisutori* [Oral History of Natsume], p.319.

62 Ibid.

63 Sebata, *Boei Keikaku no Taiko to Nichi-Bei Gaidorain*, p.154, 204; *Asahi Shimbun* (Asahi Newspaper), April 16, 1981.

64 *Asahi Shimbun* (Asahi Newspaper), July 18, 1981 (evening edition).

65 LDP Policy Affairs Research Council, Security Affairs Research Council, National Defense Division, and the Special Committee on the Military Base Affairs, "Proposal Regarding Defense Force Buildup," *Jiyu Minshu* [Liberal Democracy] 385, April 1985, p.48.

66 *Tokyo Shimbun* (Tokyo Newspaper), October 7, 1985.

General of the GSDF Western Army, asserted, "It would be too contradictory and illogical to only take command of land, sea, and air forces within the general boundaries of the attached table while simply leaving in place the basic NDPO concept. It would probably not be possible to respond to the changes after that."[67] It is possible to perceive the above discussion as the "Idea of Attached Table Revision and Concept Change," which is a form of the Idea of Defense Force Reinforcement.

In addition, the Research Council on Peace Issues, established by Prime Minister Yasuhiro Nakasone (inaugurated on November 27, 1982) on August 5, 1983 as his personal advisory council, pointed out the following in its report (*Comprehensive Security Policy for the International State, Japan*) compiled on December 18, 1984 the following year.[68]

> "While promoting reform efforts, the NDPO should be reconsidered. Eight years have already passed since its formulation and the international situation, including the military situation, has changed. Although Japan's economic strength is growing, its financial affairs are worsening, and it has become necessary to introduce new viewpoints for circumstances such as configuration of military force content changes accompanying technological development.
>
> Because the achievement period for the NDPO was thought to be comparatively short, there were self-imposed restraints on defense efforts, the expression form for the limited principles was slightly narrow, and it did not have a sense of completion as a valid combat readiness force against aggression that could occur at some point. The idea of the 'Basic Defense Force' central concept was primarily for defense buildup in peacetimes and does not clarify the response process and principles for a situation with increasing tension or a situation with a predicted emergency. Therefore, at the same time as being inadequate for responses, it is also inadequate in that it does not clarify necessary self-restraint principles demanded for responding to such a severe situation. The defense structure that should be created going forward should allow more flexible responses, and at the same time must also clarify more efficient, comprehensive defense systems and self-restrain principles. That is different from the essence of the Basic Defense Force Concept."[69]

---

67 April 23, 1986, Question by House of Councillors Member Masao Horie, 104th House of Councillors Special Investigative Committee on Foreign Affairs and National Security No. 2, [Online] Available at: http://kokkai.ndl.go.jp/cgi-bin/KENSAKU/swk_dispdoc.cgi?SESSION=18041&SAVED_RID=2&PAGE=0&POS=0&TOTAL=0&SRV_ID=6&DOC_ID=2401&DPAGE=2&DTOTAL=53&DPOS=31&SORT_DIR=1&SORT_TYPE=0&MODE=1&DMY=24538. See also NIDS (eds.), "Horie Masao Oraru Histori" [Oral History of Masao Horie], NIDS (eds.), *Oraru Hisutori, Reisenki no Boeiryoku Seibi to Domei Seisaku (1) – Yojibo Made no Boeiryoku Seibi to Nichi-Bei Anpo Taisei no Keisei* [Oral History, Defense Buildup and Alliance Policy During the Cold War (1) – Defense Buildup Until the 4th DBP and Formation of the Japan-U.S. Security Arrangement], NIDS, 2012, pp.332-333.

68 The members were as follows. Chairman: Masataka Kosaka, Professor, Kyoto University; Members: Yoshihisa Ojimi, Director and Counsellor, Arabian Oil Co.; lawyer Kinko Sato, Director, Fusosha Publishing; Tatsuro Sato, Advisor, Jiji Press; Ryuzo Sejima, Member, Provisional Council for Administrative Reform; Michio Takeuchi, Chairman of the Board, Tokyo Stock Exchange; Sohei Nakayama, Chairman of the Board, International University of Japan; Yoshihiro Nakayama, Professor, Aoyama Gakuin University; Masayoshi Namiki, Head of the Food Policy Research Institute, Food and Agriculture Policy Research Center; Yoshiji Miyata, Senior Advisor, Japan Federation of Basic Industry Worker's Union; Takashi Mukaibo, Acting Chairman, Atomic Energy Commission.

69 Research Council on Peace Issues, *Heiwa Mondai Kenkyukai Hokokusho, Kokusai Kokka Nihon no Sogo Anzen Hosho* [Research Council on Peace Issues Report: Comprehensive Security Policy for the International State, Japan] Ministry of Finance Printing Bureau, 1985, p.82.

The chairman of the Research Council on Peace Issues who stated that "'the Basic Defense Force' central concept was primarily for defense buildup in peacetimes and does not clarify the response process and principles for a situation with increasing tension or a situation with a predicted emergency" and requested the reconsideration of the NDPO had also taken an important role in the advocacy for the concept of "resistance force (*teiko ryoku*)" as a former member of Defense Agency Director General Sakata's personal advisory committee the "Committee to Study Defense" (*Boei wo Kangaeru Kai*) and supported the Kubo Concept since the KB personal paper from an international politics viewpoint. He was Masataka Kosaka, a professor at Kyoto University.

4. The Idea of Attached Table Revision and Concept Continuation

In January 1985, Noboru Hoshuyama, who had been appointed Director of the Defense Division, says, "In January 1985 when I became a Director of the Defense Division, it was a major issue whether to reform the NDPO, which had been formulated 10 years earlier.[70] However, the Idea of Attached Table Revision and Concept Change was replaced by that can be called the "Idea of Attached Table Revision and Concept Continuation" which regarded revision of the attached table under the Basic Defense Force Concept was possible.[71]

This concept was clarified by Prime Minister Nakasone through his answers in the Plenary Session of the House of Representatives on April 8, 1986.

> "As stated in the main text of the NDPO, in the case of a need arising for changing equipment systems and other matters in order to respond to technical level trends of various countries, through deliberations and decisions in Cabinet meetings and the National Defense Council, it is considered to be possible to change the attached table. As part of making this change, I believe it will not be immediately reviewing the fundamental concepts of the NDPO including the Basic Defense Force Concept, which is the fundamental spirit of the NDPO, and repelling limited and small-scale aggression without external assistance, and other matters. In any event, the government is not considering amending not only the NDPO but also the attached table and other matters for the present."[72]

In response to this, like Hoshuyama, there was a concept that "it has come to be thought generally and ordinarily until now that the NDPO attached table was substantively halted. Even if the halt was slightly increased, it is doubtful that there is persuasive power to explain that 'it is

---

70 Noboru Hoshuyama, "Hyoshi/Memo"[Cover/Memo] Hoshuyama Noboru Kankei Bunsho (Dai 2 ji Ukeirebun) [Noboru Hoshuyama-Related Documents (Second)] (1075) (Archived in the Modern Japanese Political History Materials Room of the National Diet Library in Japan).

71 See also Asao Mihara (with Kazuo Yasuhara), "'1 % Waku' Minaoshi ha Shincho ni: Yakudatsu Jieitai niha mada Sobi Busoku" [Carefully Reviewing the '1% Cap': There is Still Insufficient Equipment in the SDF Useful] *Economist* 62:32, August 7, 1984, pp.61-62; Eiji Fukazawa, "'Boei Keikaku no Taiko' Minaoshi Rongi no Kiseki" [Trajectory of the Discussion on the Review of the NDPO] *Rippo to Chosa* [Legislation and Research] 144, March 1988, pp.29-30.

72 April 8, 1986, Responses of Prime Minister Yasuhiro Nakasone to Questions in the Diet, the Plenary Session of the House of Representatives of the 104th Diet, No. 8, Kokkai Kaigiroku [Minutes of the Diet] [Online] Available at: http://kokkai.ndl.go.jp/cgi-bin/KENSAKU/swk_dispdoc.cgi?SESSION=39030&SAVED_RID=2&PAGE=0&POS= 0&TOTAL=0&SRV_ID=6&DOC_ID=2393&DPAGE=2&DTOTAL=71&DPOS=28&SORT_DIR=0&SORT_TYPE=0&MODE=1&DMY=44262.

not being reviewed.'"[73] However, the *Defense White Paper* of the same fiscal year also stated that the government does not intend to amend the attached table. It also showed the same view as the answers in the Diet of Nakasone, stating, "Moreover, when the need arises for a reformation of equipment structure and other systems of the Self Defense Forces in order to cope with further changes in, for example, the technological standards, the attached table of the Outline can be amended after deliberation and approval by the Security Council of Japan (reorganized from the National Defense Council in July 1, 1986) and the Cabinet. Even if alterations to the attached table were to be made, this should not be interpreted as an immediate 'revision' of the Outline which would mean a change of the fundamental concept of the Outline such as the 'possession of defense forces capable effectively coping with situations up to the point of limited and small scale aggression' outlined in the text."[74] Furthermore, in the *FY1987 Defense White Paper* within the "Mechanism of the Outline" item, in response to criticism that there was a change in scale and content of limited and small-scale aggression and the NDPO could not effectively repel it, it is stated that the NDPO "has its own built-in mechanism which enables it to cope with changes in the circumstances," and it is mentioned that the 1976 NDPO provides that the nation's defense buildup be carried out "with due consideration given to qualitative refinement and improvement of the defense capability so that it can cope with changes in technological standards in other countries." The response was that "[t]hrough qualitative improvement of main defense equipment within the outline, it will be possible to deal with such changes over a considerably long period of time." Continuing on, the white paper focuses on a note that in the attached table, "this list is based upon the equipment structure that SDF possesses or is scheduled to possess" at the time of drafting of the NDPO. "This is in consideration for the possibility that quantitative figures of the units and main equipment as specified in the attached table may be altered depending on changes in equipment systems that can result from scientific and technological progress in the future." "The fundamental concept underlying the Outline is to seek to build up a more efficient defense capability. This means that quantitative figures for main equipment can be altered even without changes in equipment systems. For example, when new equipment is introduced to replace separate functions held by more than one Self-Defense Force and when it is considered appropriate, from the standpoint of greater efficiency, to place the new equipment under control of one of the forces, the boundaries separating the Ground, Maritime and Air Self-Defense Forces as defined in the attached table may be altered or slightly changed in the quantitative figures for main equipment set aside for each of the three forces." This means it is possible to change the attached table accompanying equipment system changes and other matters or defense force optimization.[75]

On November 20, 1986 before this, Prime Minister Nakasone stated during answers in the Diet, "Now is the time to exert all efforts to achieve the NDPO level." He indicated the Basic Defense Force Concept would be continued for the time being, stating, "In regard to problems afterwards, they should be thought about taking into consideration all of the circumstances at that point in time. Therefore, whether the Basic Defense Force will be further extended or whether

---

73 Noboru Hoshuyama, "'Boei Keikaku no Taiko' no Minaoshi" [Review of the NDPO] Hoshuyama Noboru Kankei Bunsho (Dai 2 ji Ukeirebun) [Hoshuyama-Related Documents (Second)] (1536).

74 *FY1986 Defense of Japan* (English version), p.81.

75 *FY1987 Defense of Japan* (English version), pp.77-78. See also GRIPS (eds.), *Hoshuyama Oraru Histori* [Oral History of Hoshuyama] (below), pp.67-68.

a new concept will emerge should be appropriately thought about taking into consideration the various conditions…at that time."[76] In the "Instructions Regarding Creation of Defense Programs and Other Matters" established in April 1977, although it was assumed that there would be a review of the NDPO based on the "Joint Mid-term Defense Estimates" based on the "Joint Long-term Defense Estimates" drawn up by the Chairman of the Joint Staff Council,[77] Seiji Ema, who served as Head Planner of the Defense Bureau from July 1984-July 1986, states, "From my perspective working on the mid-term programming later until 1986 Medium Term Defense Program, there was no suggestion of having to change the NDPO by reflecting this (the Joint Mid-term Defense Estimates) to that (the NDPO).[78] In the end, the attached table was not revised during the 1976 NDPO period.

In reality, both the Idea of Attached Table Revision and Concept Change and the Idea of Attached Table Revision and Concept Continuation had strong sides that argued for advocating the vague Basic Defense Force Concept or criticisms against it, and it cannot be said that it became a sophisticated concept. Therefore, both ideas might seem contradictory at a glance, but there remain vague parts regarding whether there were essential differences in the concepts. For example, if the threat recognition of the Idea of Attached Table Revision and Concept Change is limited to small scale aggression, the problem is the relative scale of limited and small-scale aggression, and although there is no need to change the Basic Defense Force Concept itself, it seems such logic was not fully sophisticated.[79] Consider this background for the Idea of Attached Table Revision and Concept Continuation simply supplanting the Idea of Attached Table Revision and Concept Change.

Conclusion

The defense controversies that unfolded during the Second Cold War were not waged between the Basic Defense Force Concept and counter-threat theory-like Basic Defense Force Concept criticisms that responded to rising recognition of threats. It is also not the case that the Basic

---

[76] November 20, 1986, Responses of Prime Minister Yasuhiro Nakasone to Questions in the Diet, House of Representatives Committee on Cabinet of the 107th Diet, No. 6, Kokkai Kaigiroku [Minutes of the Diet] [Online] Available at: http://kokkai.ndl.go.jp/cgi-bin/KENSAKU/swk_dispdoc.cgi?SESSION=4461&SAVED_RID=1&PAGE=0&POS=0&TOTAL=0&SRV_ID=6&DOC_ID=8290&DPAGE=1&DTOTAL=1&DPOS=1&SORT_DIR=1&SORT_TYPE=0&MODE=1&DMY=5518. However, Nakasone later gave his opinion, "I did not necessarily approve of the 'Basic Defense Force Concept'. Rather than that, what was important was to think about how to create a realistic system that could respond to aggression by a foreign enemy. For example, specific issues such as how to deploy Tomahawks. Although building up Basic Defense Force was important, it was necessary to have something above it. Incidentally, if I advocate that, the Socialist Party will get riled up. Basic Defense Force means political safety, but I also felt it was useless to just go down such a safety road. It was a position that required defense force for emergencies were needed." Yasuhiro Nakasone (Interviewed by Takuma Nakashima, Ryuji Hattori, Amiko Nobori, Hidekazu Wakatsuki, Narushige Michishita, Ayako Kusunoki and Takao Segawa), *Nakasone Yasuhiro ga Kataru Sengo Nihon Gaiko* [Japanese Foreign Policy since 1945: Yasuhiro Nakasone Oral History] Shinchosha, 2012, pp.258-259.

[77] Defense Division, Defense Breau, "Boei Shokeikaku Kunrei no Gaiyo To ni tsuite" [Regarding Defense Programs Instructions], *Boei Antena* [Defense Antenna] 202, May 1977.

[78] NIDS (eds.), "Ema Seiji Oraru Hisutori" [Oral History of Seiji Ema] in NIDS (eds.), *Oraru Hisutori, Reisenki no Boeiryoku Seibi to Domei Seisaku* [Oral History, Defense Buildup and Alliance Policy During the Cold War] (7), NIDS, 2017, p.140.

[79] Such points were made sophisticated in Defense Bureau Director-General Seiki Nishihiro's "'Power Vacuum' Theory" (*'Chikara no Kuhaku' Ron*) clarified in the House of Representatives Special Security Committee on August 24, 1987, but I would like to discuss this again in a different manuscript.

Defense Force Concept emerged victorious as a result. From when the Basic Defense Force Concept was originally established, there were ambiguous interpretations like beyond-the-threat theory-like interpretation, counter low-threat theory-like interpretation, the "Validation Theory" (*Kensho Ron*, theory that it is possible to oppose in the end when verifying whether it is possible to oppose low threats with defense force derived from the beyond-the-threat theory) interpretation.[80] As Shigeki Nishimura, a staff of the Ground Staff Office at the time, pointed out regarding the reality of the Basic Defense Force Concept, "This term has vague logic and has been degraded with dirty fingers marks due to opportunistic usage."[81]

Based on the increasing threat posed by the Soviet Union in Northeast Asia with the demise of détente and the arrival of the Second Cold War, as well as the pressure regarding defense from the U.S. on Japan, criticisms within Japan grew against the Basic Defense Force Concept, and the Idea of Defense Force Reinforcement emerged as represented in Councillor Hisahiko Okazaki's OK personal paper. However, according to the Idea of Attached Table Early Achievement that appeared in the Comprehensive Security Research Group Report, Defense Bureau Director-General Akira Shiota's answers in the Diet, the *FY1981 Defense White Paper*, and more, the Idea of Defense Force Reinforcement unexpectedly began to coexist with the Basic Defense Force Concept. There was greater interest among people in uniform about the 1% of GNP cap on defense spending that was capable of hindering building Basic Defense Force, and Okazaki changed his position. Following this, the U.S. issued requests not settled in the attached table at fora such as the 13th SSC. In Japan as well, people centered on influential LDP members on the defense issue called for the Idea of Attached Table Revision and Concept Change, a form of the Idea of Defense Force Reinforcement, and the Research Council on Peace Issues Report also requested reconsideration of the Basic Defense Force Concept. However, the Idea of Attached Table Revision and Concept Change was supplanted by the Idea of Attached Table Revision and Concept Continuation that enabled revising the attached table under the Basic Defense Force Concept shown in the FY1986 and FY1987 editions of the *Defense White Paper*. Competing counterarguments to the Basic Defense Force Concept were, we can say, successively incorporated into the Basic Defense Force Concept itself. This is understood through tracing criticisms of the Basic Defense Force Concept during the Second Cold War.

---

80 Yasuaki Chijiwa, "Unfinished 'Beyond-the-Threat Theory': Japan's 'Basic Defense Force Concept' Revisited," *National Institute for Defense Studies Journal of Defense and Security* 18:1, November 2015, pp.97-98.

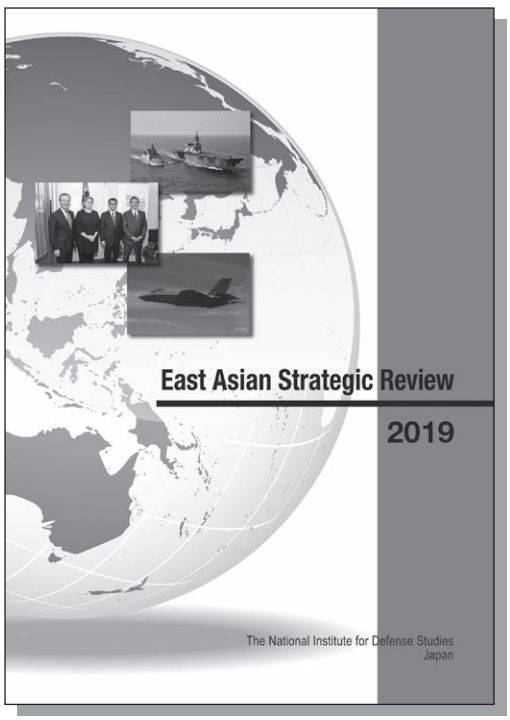
81 Shigeki Nishimura, *Boei Senryaku to ha Nanika* [What is Defense Strategy?] PHP Institute, 2012, p.203.

East Asian Strategic Review 2019

National Institute for Defense Studies (NIDS)

The maintenance of peace and stability in East Asia requires an objective understanding of the regional security environment.

With the aim of facilitating that understanding, NIDS researchers examine trends and developments in East Asian security circumstances from their unique perspectives, and compile their analyses in the East Asian Strategic Review (EASR), which is published annually.



【Contents】

ISBN 978-4-86482-074-5

http://www.nids.mod.go.jp/english/publication/east-asian/e2019.html

No. 20 December 2019

National Institute for Defense Studies, Tokyo

NIDS