Cybersecurity Governance in Japan

Hidetoshi OGAWA, Motohiro TSUCHIYA
Keio University, Tokyo, Japan
hidetoshi.ogawa@keio.jp

Abstract: The massive cyberattacks against Estonia in 2007 marked the beginning of new era where cyberspace can be misused by daunting malicious actors as part of new operational domain like land, sea and air, which differs from ordinary cybercrime in nature. Japan has not been exempted from such cyberattacks and experienced a number of severe information breaches, to begin with the Japan Pension Service case in 2015 with the leakage of more than 1.25 million citizen's personal information. The aggravating security situations both in real and cyberspace urged Japan to review and improve its governance several times in terms of laws, strategies, and policies as well as organisational structures, coupled with increased budget and human resources. As a result, Japan denounced two cyberattacks by means of public attribution to date, WannaCry to North Korea in 2017 then so-called APT10 to China in 2018. This paper analyses Japan's efforts since past ten years to strengthen her cybersecurity governance from the viewpoint of anticipation and attribution, which require better coordination and cooperation public-public (interagency), public-private and private-private.
Keywords: Cybersecurity, Governance, Japan, Attribution, Anticipation

INTRODUCTION

On 18th of December 2018, the Abe Administration in Japan approved the new National Defense Program Guidelines (NDPG) and Mid-Term Defense Program (MTDP). The NDPG are tailored in line with the National Security Strategy and sets forth Japan's basic defence policy and long-term (approximately 10 years) strategic objectives of defence capabilities, which are materialised in detail by MTDP's five-year-programme.

The last NDPG were adopted in 2013. Why were the 2013 NDPG, which were supposed to be effective for around ten years, rewritten after just five? There were three main factors behind the decision.

First was the changing situation in East Asia. North Korea has repeatedly conducted nuclear and missile tests. There were some hopes that the North Korea–United States summit, held in Singapore in June 2018, would result in positive changes in North Korean autocratic leader's posture as per a big deal, but in reality, there has been no progress at all with regard to their nuclear weapons, ballistic missiles and other international concerns.

Second was the changes taking place with Japan's ally, the United States. Former President Donald Trump was promoting policies that differ from those of past administrations. While working on dialogue with North Korea, the Trump administration was promoting a world-wide review of the United States' relationship with its traditional allies to seek from them more financial contributions, self-help by spending bigger defence budget. Against this backdrop, severe tensions arose with regard to the introduction of THAAD (Terminal High Altitude Area Defense Missile) deployment in South Korea, among China, Russia, Korea and United States in 2017. Especially China went beyond diplomatic accusations and took

multiple economic sanctions against South Korea, like mass-tourism ban from China to South Korea. As we observe today much visibly Chinese assertive and aggressive activities with regard to Taiwan, Japan, South China Sea with ASEAN countries, India or even toward European countries, China seems to have changed its international strategy drastically, abandoning Deng Xiaoping's "Hide your talents and wait for future opportunities" policy. Xi Jinping became Chinese president in 2013 (CCP Chairman 2012), claiming "Chinese Dream" for the great rejuvenation of the Chinese nation. This Supreme Leader's fanfare of "the time has come" is executed bureaucratically by communist's administrative machinery, military, and diplomats, as in military provocation, wolf worrier diplomacy, crackdown of Muslim minorities in Xinjiang and democratic group in Hong Kong, together with diplomatic tensions with U.S., Australia, etc. Sino-Japanese relations have been relatively well controlled on political and diplomatic level, while on the ground, the intensity and frequency of Chinese vessels' intrusion onto Japanese territorial sea and contiguous water have been aggravated, turning these incidents like continuous phenomenon (Ministry of Foreign Affairs, 2021).

Third was the rapid development of new, game-changing technologies or so-called emerging and disruptive technologies (EDT) such as cyber & space technology, artificial intelligence (AI), quantum computing, big data analytics, drones, hypersonic weapon system, novel materials, biotechnologies and so on. In addition to the conventional operational domains of land, sea, and air, experts have begun discussing concepts like cross-domain attacks that cross over into new domains such as space, cyberspace, and the electromagnetic spectrum, hybrid warfare, and multi-domain battles.

These rapidly changing situations have urged Japan to review her national security posture, including revision of the NPDG at earlier stage than expected.

In this paper, we will discuss developments in Japanese policies and the underlying Japanese governance with a specific focus on cybersecurity. As one of the countries where information communications technologies (ICT) have penetrated everyday life the most, Japan is faced with numerous cybersecurity threats, and it has steadily reviewed its policy and governance to adequately respond to those threats. Although the Japanese Constitution sets some legal constraints on Japan's possible response to cyberattacks and measures against cybersecurity threats, such as exclusive defence-oriented policy derived from pacifism as well as strict respect of privacy, that does not mean that Japan's hands are completely tied. We analyse how Japanese policies have developed as the international situation has become more serious.

A FRAMEWORK FOR ANALYSIS

ANTICIPATION OF CYBERATTACKS

As things stand, the biggest problem in cyberspace is cyberattacks. While these are called attacks, in most cases, there are no casualties, and there are few examples of physical damage. Most things reported as cyberattacks actually fall into the category of cybercrimes or cyber espionage (spying), and these are more accurately referred to as cyber operations. In the

context of international law, this refers to "the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace" (Schmitt, 2013a). In contrast, a cyberattack refers to "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (Schmitt, 2013b).

Although there is a difference in the degree of damage, if cyberattacks are anticipated and prevented, a government can aim for better governance. However, this comes at a trade-off with cost, just as the cases for preparedness against large-scale natural disasters. Bearing in mind that the complete elimination of risk - zero risk - is impossible in almost all areas but especially so in cyber domain, the government, private organisations, individuals should determine a proper level of investment and the best doable set of policies or solutions to reduce the risk to an acceptable one, from the viewpoint of probability of occurrence, scale and nature of possible damage.

Even though the risk is a matter of probability, the best thing is to be able to predict the disaster, attack, or conflict. Such predictions would improve fundamentally risk assessments, on which policies and measures should be based. Studies are coming out that focus on anticipatory governance from that standpoint.

Anticipatory governance is a prescriptive system for expressly working on the mutual interaction of the three elements of complexity, acceleration, and policy. In particular, "anticipatory governance is a system of institutions, rules, and norms that provides a way to use foresight, networks, and feedback for the purpose of reducing risk and increasing capacity to respond to events at earlier rather than later stages of development" (Fuerth, 2011). In other words, anticipatory governance is applying system theory for prediction to policy. The method includes both traditional predictive techniques (time series analysis, statistics, simulation, etc.) and more innovative predictive techniques (Delphi method, scenario analysis, environmental scanning, etc) (Poli, 2012).

However, it is easy to imagine that the degree to which anticipatory governance is applied will vary greatly depending on the type of risk. In Figure 1 (Tsuchiya, T., 2020), the horizontal axis is whether the problem is more global or local, and the vertical axis is whether it is easier or harder to anticipate, based on the fastness or slowness of progression.

When for example, five problems - environment, infectious diseases, social security, natural disaster, and cybersecurity are plotted on the figure, we see that environmental problems are global ones that cross national boundaries, but their progression is relatively slow. It can take several years or even decades for the problem to manifest. Of course, there are cases where the problem cannot be perceived in the early stages. If it is perceptible, however, then one can anticipate what kind of consequences it will bring about.

Social security is normally a domestic problem that remains within the borders of each country. In most cases, the population trends in each country can be predicted. There are cases where many people die due to large-scale disasters, pandemic or war, but, aside from such cases, it is clear what the working population will be several decades down the road. As such, it is easy to understand the kinds of social security problems that will (or will not) manifest.

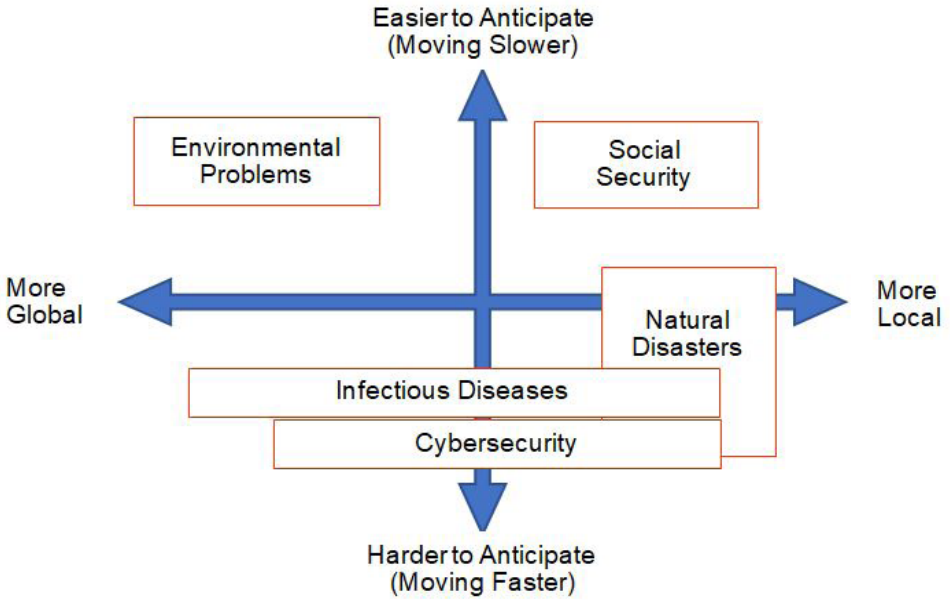

Figure 1. *Two Dimensions of Anticipation*

In contrast, although the disaster areas tend to be localized, it is still difficult to anticipate or predict earthquakes, tsunamis, volcanic eruptions, and other natural disasters. Earthquake prediction tests are ongoing, but, at best, they give warnings several seconds or minutes in advance. It is difficult to know whether there will be a big earthquake the following day. However, there are some natural disasters that have become easier to anticipate based on experience, such as, abnormal climate caused by changes in ocean currents.

Comparatively speaking, cyberattacks are generally difficult to anticipate. Some of the infectious diseases, like the ongoing Covid-19 pandemic have similar character. They are not completely unseeable but difficult to predict its spread and degree of impact at early stage. With regard to the cybersecurity, there are always malicious human actors unlike diseases or disasters which do not deliberately choose the victims. But when cybercrimes are committed for monetary gain, the targets are often chosen at random, making it difficult to predict the identity of the victim beforehand. However, targeted attacks such as spear phishing toward specific individuals or organizations, or state-sponsored cyberattacks, DDoS attacks have always specific motivations and intentions of the author, which leave some room for anticipation notwithstanding its practical difficulty. An example of such anticipatable cyberattacks are “commemorative date attacks”. Together with rather general specific days like New Year Day, April Fool’s Day or Christmas, the 18th September (Mukden/Manchurian incident perceived as the beginning of Japanese Imperial Army’s invasion to China in 1931), 15th August (end of World War II with Japanese surrender to allied forces) and some other historic dates are known where many cyberattacks attempts from China to Japan were conducted until several years ago. Since then, it has become much fewer these past few years. It may be partially owing to the higher tension in Sino-U.S. relations, which would have distracted their attention from Japan-China issue. Other element would be that as the sophistication of anti-DDoS and other technical solutions have prevented successfully from service disruptions and major defacement incidents, such attacks seem to have been perceived less effective for ordinary attackers.

Nations that can mobilize the funds and personnel are interested in engaging in "active defence," whereby they infiltrate the networks and systems of attackers in advance and conduct defensive attacks as soon as a cyberattack is anticipated. (Kaplan, 2016). The strategy announced by the United States Department of Defense, in September 2018, contained the phrase "defend forward." It refers to stopping cyberattacks in countries where attackers are located, before they can attack within the United States (Department of Defense, 2018).

The more focused the cyberattack, the more local the damages, but with the ransomware called "WannaCry" that spread in 2017, there was a global impact, with 200,000 infections and damages in 150 countries.

In cybersecurity, attempts have been made to apply deterrence by punishment and deterrence by denial from nuclear security theory, and the concept of cyber hygiene, which applies public health theory, has been introduced to reduce the risk of damages. However, anticipatory governance in cybersecurity is at the stage where various theories and methods are brought together and tried to apply whether they are effective or not. If anticipation becomes possible, the position of cybersecurity on Figure 1 can be moved upward, which implies that its policy and measures would be dealt with like in more conventional and physical domains with better assurance.

ATTRIBUTION OF CYBERATTACKS

Attribution refers to identifying attackers and their affiliates. In case of conventional military attacks in physical domain, attribution is not normally a difficult job. For example, if North Korea fired a ballistic missile, satellite images and other means can be used to attribute the attack with crystal clear evidence. However, when it comes to cyberattacks, attribution is often extremely difficult due to several reasons.

First of all, as the name cyber-espionage suggests, cyber-information theft and various covert cyber-operations are different in nature from conventional wars with proclamation of war or other armed conflicts. They are rather closer to traditional intelligence activities. As of today, there is no international law that generally prohibits non-destructive intelligence activities, either in physical space or in cyberspace. If information theft activities conducted by a state or individuals commissioned by a state are attributed, it can be subject to various countermeasures or sanctions against such a state, not limited to the prosecution of suspected perpetrators for their crime based on domestic law. At least it would degrade the country's reputation and affect diplomatic relations. Therefore, unlike the example of natural disasters in a broad sense in the previous section, cyber-attackers, who are definitely human-being lurking behind machines and networks, usually have an incentive to cover up their identity and operations as much as possible. It goes without saying that the cybercrimes by non-state sponsored simple criminals are alike at least as to their identity.

Secondly, there are technical factors specific to cyberspace based on the current Internet technology. It is possible to take over systems remotely and secretly then to form attack assets (bot nets) for future massive operations, which easily cross over national boundaries. Unlike secret cyber-espionage operations, even in the case of DDoS attacks which are generally

much perceptible cyberattacks, their source - physical location of each terminal sending attack packets is not at all necessarily the attacker's one, rather innocent victims in most cases. Real-time analysis of NICTER Project (NICTER, 2021). by the National Institute of Information and Communications Technology on possible attacks and their preparation against Japan shows that the source-countries have changed quickly but recent major ones are China, Russia, Netherland, Switzerland, etc., which reaffirms private cybersecurity companies reports, like FireEye. This illustrates the reason why automated cyber counterattacks and hacking-backs are difficult and not enthusiastically supported for fear of uncontrolled escalation, if not prohibited as a means of possible retaliation only by the government. The Paris Call for Trust and Security in Cyberspace made in November 2018 affirmed the need to "take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors" (Paris Call, 2018).

Due to such nature of cyberattacks, it is indispensable for making attribution possible to conduct multifaceted activities and put them together for all-source analysis, not only collecting and analysing purely IT technical information but also contributions from intelligence communities, investigative agencies, diplomatic and military agencies, as well as international cooperation especially amongst like-minded countries.

Attribution capabilities are an essential tool for countering cyberattacks (Rid & Buchanan, 2014). Without attribution capabilities, there can be little room to apply "deterrence by punishment" as the author stays unknown. On the other hand, if a country or countries in cooperation can attribute cyberattacks, then various options become possible to give consequences to the author, which are expected to have deterrence effect to some extent, if not comparable to such examples as the mutual assured destruction doctrine in nuclear power of balance.

One of the recent developments in this area is the EU Cyber Diplomacy Toolbox adopted by the Council of the European Union in June 2017 (EU, 2017). It reminds that "attribution to a State or a non-State actor remains a sovereign political decision based on all-source intelligence and should be established in accordance with international law of State responsibility. In this regard, EU stresses that not all measures of a joint EU diplomatic response to malicious cyber activities require attribution to a State or a non-State actor." This provision would contribute to better flexibility and manoeuvrability for collective and individual responses at various intensity. The document also affirms that "measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures, ... facilitate mitigation of immediate and long-term threats, and influence the behaviour of potential aggressors in a long term."

Japan has made two "public attributions" denouncing malicious cyber-activities to date, first case of which was abovementioned "WannaCry" attributed to North Korea in December 2017 (Ministry of Foreign Affairs, 2017), then so-called "APT10" to China in December 2018 (Ministry of Foreign Affairs, 2018). These acts are also expected to influence the behaviour of current and potential aggressors.

The United States have engaged much actively in attribution, which led to more various countermeasures, from public attribution to summit level demarches (White House Office of the Press Secretary, 2013; White House Office of the Press Secretary, 2015) and indictment of the suspected individuals (Office of Public Affairs, 2014).

MAIN ACTORS IN JAPANESE CYBERSECURITY GOVERNANCE

CYBERSECURITY STRATEGIC HEADQUARTERS

The Cybersecurity Strategic Headquarters (hereinafter CSHQ) is a political organisation that formulates Japanese cybersecurity basic policy, and convened periodically at ministerial level. Until the Basic Act on Cybersecurity (Basic Act on Cybersecurity, 2014) was enacted in 2014, it was called the Information Security Policy Council (ISPC), but this act renamed it and strengthened its role with a clear legal basis. The two cybersecurity strategies developed by the ISPC (2010 Information Security Strategy for Protecting the Nation and 2013 Cybersecurity Strategy) were not an object of the cabinet's action, while the cybersecurity strategies afterwards formulated by the CSHQ should be brought forward for cabinet approval, based on article 12 of the Basic Act on Cybersecurity.

This procedural change reflects the increased awareness of the importance of cybersecurity, following major international and domestic incidents. It is also to be noted that the ISPC was established based on cabinet ordinance, while the CSHQ has explicit legislative foundation in the Basic Act on Cybersecurity.

The head of the CSHQ is the Chief Cabinet Secretary, post of which has been generally perceived as the right hand of successive Prime Ministers and as the Minister primus inter pares. Under his chairmanship, seven cabinet ministers as well as seven experts from private sector and academia participate. With regard to the members from the cabinet, there are five ministers-with-portfolio (Chairman of the National Public Security Commission governing National Police Agency, Minister of Internal Affairs and Communication, Minister for Foreign Affairs, Minister of Economy, Trade and Industry, Minister of Defence). Their ministries are mandated to support the administrative operations of the CSHQ with the Cabinet Secretariat and considered to be the leading contributors to the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), placed in the Cabinet Secretariat and specifically in charge of the matter. We will see the NISC and these five ministries and agency later.

From the viewpoint of our framework for analysis, the creation of the CSHQ with clear legal basis is expected to strengthen cybersecurity governance, by means of inter-ministerial structured cooperation to improve anticipatory governance and the capacity of attribution. As demonstrated in the EU Cyber Diplomacy Toolbox document, public attribution and related measures are not purely technical but political and diplomatic, which require holistic approach. Close collaboration of CSHQ's five ministries at least and political decision at the end are indispensable to make it happen.

NATIONAL CENTER OF INCIDENT READINESS AND STRATEGY FOR CYBERSECURITY (NISC)

The National Center of Incident Readiness and Strategy for Cybersecurity (NISC) is a relatively small organisation with around 200 staff today but plays increasingly important role in cybersecurity policy making in Japan, together with its operational functions for the protection of government networks as "GovCERT" (Government Computer Emergency Response Team). It also acts as National CSIRT in tandem with JPCERT/CC (Japan Computer

Emergency Response Team Coordination Center) in the private sector. Before the enactment of the Basic Act on Cybersecurity in January 2015, the NISC stood for "National Information Security Center" since its creation in 2005. As this abbreviation had been already known to at least Japanese cybersecurity community, they tried to keep "NISC" for the sake of visibility as a brand, while its full denomination was changed to accommodate the terminology "cybersecurity" used in the Basic Act. In Japan, the connotation of cybersecurity is something relating the overall security of cyberspace which interpenetrates and fuses with the physical world, beyond a mere mishmash of wires and computers and the accent was not on the exclusion of non-cyber element of information security, as it had not fallen under NISC's mandate from the outset.

The NISC is one of the few central administrative organisations which has been allocated increasing manpower and budget, against the general tendency to cap them in the context of public finances reconstruction. At the time of its creation in April 2005, it started with only 22 staff strong (NISC, 2007). Fifteen years later, it has grown nearly ten times bigger.

In terms of the annual national budget for cybersecurity, it was JPY 36.95 billion in total (initial budget + supplementary budget) in fiscal year 2012. It has almost steadily increased and more than doubled in FY 2020 with JPY 101.98 billion (Figure 2). It is clear from this budgetary tendency together with the strengthening of the NISC's effectives as above that the Japanese government has reasonably prioritised cybersecurity over recent years. The significant surge of supplementary budget in FY 2015 was primarily linked to the huge data breach of Japan Pension Service.

However, those budget numbers are for all ministries combined. Out of the JPY 101.98 billion in FY2020, the NISC's portion is only 3.8% at 3.88 billion yen. This represents current NISC's status and role in the government which is at the middle ground between a full-fledged central agency and a coordinating Task Force-like organisation.

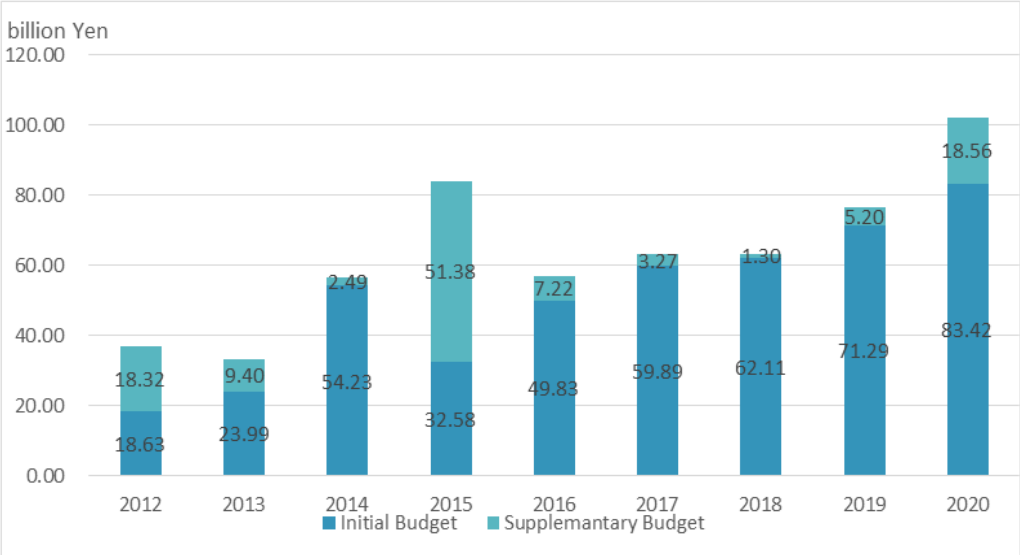

Figure 2. *Japanese Government Budget Related to Cyber (Information) Security*
Source: NISC

Below is the NISC's organisational structure, representing its main missions (Figure 3).

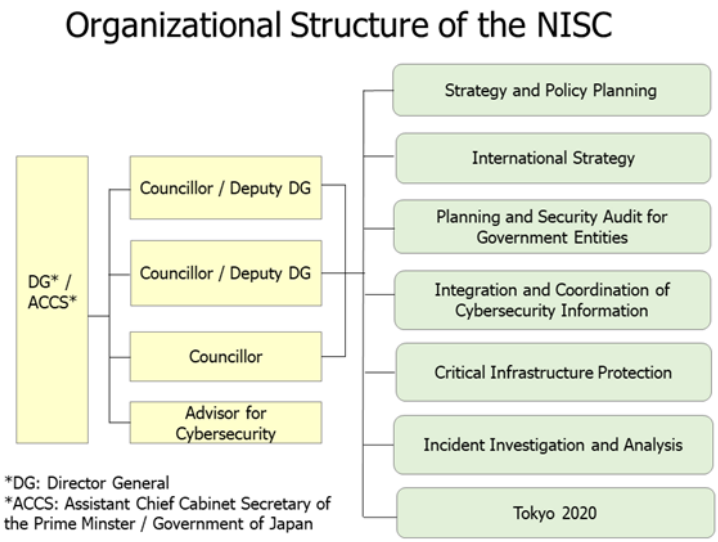

Figure 3. *Organisational Structure of the NISC*
Source: NISC

The head (Director-General) of the NISC is the Assistant Chief Cabinet Secretary (ACCS)

When the National Security Secretariat (NSS) was established within the Cabinet Secretariat in January 2014, the ACCS also began serving as the Deputy Secretary General of NSS. This made the ACCS responsible simultaneously for three roles: Head of the NISC (cybersecurity), Head of the physical security and crisis management, and newly added mission as Deputy Head of the NSS (national security).

There are three ACCSs under the Prime Minister, the Chief Cabinet Secretary, and the Deputy Chief Cabinet Secretary (DCCS) in charge of Administration. This DCCS is de facto the top official of all central administration. Three ACCSs under the DCCS are also very high rank – equivalent to Vice-Ministers or Secretary-Generals, i.e., No.1 officials of each ministries and agencies. But the real strength of ACCSs resides in the fact that they are in direct decision line up to the top, the Prime Minister. It matters a lot when the issues in question are of strategic importance, requiring political decision and attention, and especially when they are overarching across multiple ministries. The cybersecurity is a good example of such strategic issues. In this structure, the cybersecurity has been assigned to the ACCS in charge of "Situation Readiness and Crisis Management". Other two ACCSs' portfolio are for "domestic affairs" and "foreign affairs" respectively.

From the viewpoint of cybersecurity governance in the context of broader crisis management, important is the fact that the ACCS in charge of situation readiness and crisis management is, in one person, responsible both for physical crisis and cyber one. As mentioned above, its third new chapeau is the Deputy Head of the National Security Secretariat. It goes without saying that this is based on the understanding that the crises of high magnitude regardless physical, cyber, hybrid, are nothing but the central issue of the national security. It is also noteworthy that the successive ACCSs in charge of situation readiness and crisis management have been nominated from amongst top level civilian officials of the Ministry of Defence.

The NISC itself is dedicated for cybersecurity but working very closely with the organ in charge of physical security under the same boss – ACCS. Moreover, one of the two (or more) Deputy Director-Generals at NISC should be filled with by the Councillor of Crisis Management as stipulated in Article 1 of the Rules for Appointing Councillor of Crisis Management in Cabinet Secretariat [Prime Minister decision, April 9, 1998] (NISC, 2016). In practice, this post has been occupied by persons from the National Police Agency (NPA) with natural inclination onto cyber-physical crisis. In the event of a major cyberattack, he/she is expected to serve as an interface with police organisations.

Customarily, the position of the Deputy Director-General who is not the Councillor of Crisis Management has been alternatingly filled by someone from the Ministry of Internal Affairs and Communications (MIC) or someone from the Ministry of Economy, Trade and Industry (METI). This is also customarily linked to the nomination of the Counsellor in charge of strategy and policy planning (de facto No.3 of the NISC), which flip-flops between MIC and METI to let them always have either at No.2 or No.3. They are expected to play a leading role in formulating national cybersecurity strategies, laws and other instruments which we will take up later in Section 4 below, even though these matters normally involve all directions.

As briefly mentioned at the beginning of this section, NISC's main missions can be categorised in two: one is to formulate or coordinate national cybersecurity strategy and cross-sectional policies, and the other is operational tasks.

As for the policy side, together with the Basic Act of Cybersecurity and successive national cybersecurity strategies, the NISC also set forth a minimum standard (baseline standard) of cybersecurity for the central government ministries and agencies – "Common Standards Group for Information Security Measures for Government Agencies and Related Agencies" (NISC, 2018), accompanied by periodical onsite audit and penetration testing, guidelines for critical infrastructure operators (Cybersecurity Policy for Critical Infrastructure Protection, 2020), promote public awareness campaign, etc. On the operation side, the NISC monitors government network and systems 24/24h, 365/365d in parallel with each organisation's individual SOC (Security Operation Centre) or relevant measures as GSOC (Government Security Operation and Coordination Team) (GSOC, 2017). Also, it analyses cyberattacks and threats toward government in cooperation with relevant authorities and shares them with organisations concerned. On top of these functions as a GovCERT in narrow sense, it facilitates public-private, private-private information sharing especially for critical infrastructures, other voluntary private organisations, as well as operators and service providers of the Tokyo Olympic & Paralympic games.

NATIONAL SECURITY COUNCIL AND NATIONAL SECURITY SECRETARIAT

Before the enactment of the Basic Act on Cybersecurity, the Information Security Policy Council was not based in law. It was a subordinate council to the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters). However, in December 2013, the Act for Establishment of the National Security Council was enacted, and the National Security Council and its secretariat, the National Security Bureau, were established in January 2014. In November of the same

year, the Basic Act on Cybersecurity was enacted, establishing the Cybersecurity Strategic Headquarters and reorganizing the NISC. With this, the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters), the Cybersecurity Strategic Headquarters, and the National Security Council began working side by side on policy making and coordination (Figure 4).

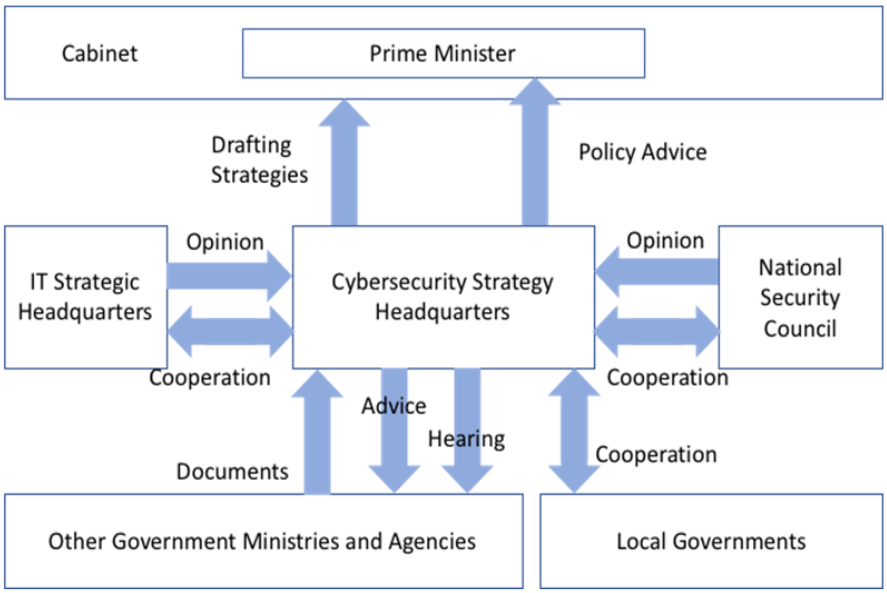

Figure 4. *Cybersecurity Governance of the Japanese Government*
Source: Source: Based on a figure on "Basic Cyber Security Law" enacted, "Control Tower" established across ministries and agencies, XTECH (Nov. 10, 2014), https://tech.nikkeibp.co.jp/it/atcl/column/14/346926/110700098/?ST=mkt-trend

As stated earlier, the Director-General of the NISC, who is responsible for the secretariat functions of the Cybersecurity Strategic Headquarters, serves concurrently as the Deputy Secretary General of the National Security Secretariat (NSS), which is responsible for the secretariat functions of the National Security Council. Consequently, from this standpoint, the Cybersecurity Strategic Headquarters and the National Security Bureau are closely linked as well.

The Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society engages in general IT and cyber policy proposals and coordination with emphasis on the promotion of use or adequate developments like e-government, while the Cybersecurity Strategic Headquarters engages in strategic cybersecurity issues with natural focus on security and safety. Meanwhile, the NSS oversees the matters when they relate national security. In the past, the majority of NSS's mission was around something political, military and diplomatic of strategic importance that affect national security. However, the recent development that is sometimes described as geo-economic or geo-technical reminded the need to adequately deal with such relatively new challenges from the angle of national security. To this end, the government decided to establish an "Economic Division" within the NSS in April 2020.

RELATED GOVERNMENT MINISTRIES AND AGENCIES

As seen above, five ministries and agency which are represented permanently at the Cybersecurity Strategic Headquarters by their Minister are expected to play leading role in Japan's overall cybersecurity policy, while all other ministries and agencies have also much to do with it in their respective competent sectors and of course on themselves.

It should be noted that the Cabinet Secretariat line (NISC, NSS or IT Strategic HQ) is politically influential as located under hospices of the Prime Minister and with its mandate of overall interagency coordination, they nevertheless do not normally have a statutory power to order or regulate something beyond the government. To apply national strategies or basic policies set forth by the Cabinet Secretariat organisations in a concrete manner on a specific area, they should usually be transposed or detailed by laws, regulations, ministerial ordinances or guidelines of the competent ministries and agencies. In this regards, competent authorities for critical infrastructure (CI) play vital role at the national level cybersecurity, such as Financial Services Agency, Ministry of Land, Infrastructure, Transport and Tourism, Ministry of Health, Labour and Welfare. But in this paper, we will just briefly overview so-called "Five Ministries and Agency of the CSHQ" to let the CI related governance of Japan be examined in future research.

National Police Agency

In Japan, the National Police Agency (NPA) is both a law enforcement and an intelligence agency. As an intelligence agency, preventing serious cyberattacks before they occur is an important role, together with its law enforcement-related policy, like investigations, arrests and handing over to public prosecutors of cybercrime perpetrators, after they were committed.

As part of general public security and anti-crime measures, the NPA takes measures against cybercrime, so do the Prefectural Police Headquarters. From historical reasons, actual law enforcement power is assigned to each Prefectural Police and NPA is not entitled to exercise it. However, in reality, almost all the heads and some influential high rank posts of the Prefectural Police are dispatched from the NPA, which makes de facto hierarchical order.

In November 2014, the Japan Cybercrime Control Center (JC3) was established under the NPA. It is used as a framework for sharing and utilising information, knowledge, experience, and expertise between industry, academia, and law enforcement.

The NPA is one of the few central administration organisations which has a Direction-General (Bureau) level organisation specialised for information and communications in which quite a number of technical officials (whose background are computer sciences, mathematics and other natural sciences) at various levels are recruited and working. This is another strong point of NPA, together with intelligence arms on the ground, to deal with not only cybercrimes in strict sense but also adversary's cyber operations in broader sense.

Ministry of Internal Affairs and Communications

The Ministry of Internal Affairs and Communications (MIC) was established in 2001 by combining two ministries and one agency. The part representing "Internal Affairs" stands for the local autonomy and is by no means linked to law enforcement or internal intelligence organs

as in many countries. In the context of cybersecurity, the part representing "Communications" derived from the Ministry of Post and Telecommunications is relevant. They have three ICT related Bureaus (Direction-General) for such areas as electronic and radio communication, broadcasting, frequency allocation and control, ICT research and development with its affiliated research institutes, telecommunications infrastructure like broadband and mobile networks, etc. As the total number of full-fledged Bureau ("局-Kyoku") is rigidly controlled not to allow easy self-growing of administration, the fact that the MIC has three ICT dedicated bureaus "Kyoku" illustrates the matter is really the centre stream for them. A Director-General of such ICT Bureaus has possibility to become the top official of the MIC as recorded in the past, unlike other organisations. In 2017, the MIC changed a Director-General's mandate from generic "information and communications" to specifically "information security", then in the following year, reorganised as Director-General for cybersecurity. This Director-General is called "統括官-Tokatsukan" and is officially treated as equivalent level to a DG of "局-Kyoku" as both are translated as DG, while the latter is generally perceived senior. This was the first case in Japanese central administration to establish a DG that is uniquely dedicated for cybersecurity.

In terms of general IT security, the MIC and the Ministry of Economy, Trade and Industry (METI) have the longest experience and the widest portfolio compared to other organisations which are recently established or focusing on specific areas. The MIC traditionally approached to ICT from telecommunications, while METI from computers and other hardware. When the internet and personal computers began to be commonly used in 1990s, the MIC (then Ministry of Post and Telecommunication) and the METI (then Ministry of International Trade and Industry) contended for jurisdiction over ICT, which was journalistically described "Hundred Years' War". In fact, it did not last so long with reasonable mutual compromise. However the alternating nomination of No.2 and No.3 of the NISC between MIC and METI may be somewhat linked to this, even official external explanations would be "both MIC and METI people's expertise is needed."

As the telecommunications carriers and internet service providers (ISP) also fall under MIC's jurisdiction, the MIC's role in cybersecurity become even bigger with the advent of 5G era. The establishment of a Director-General for Cybersecurity could be interpreted as a response to strengthen cybersecurity governance by the MIC.

Ministry of Economy, Trade and Industry

The Ministry of Economy, Trade and Industry (METI) has a Cybersecurity Division at its Commerce and Information Policy Bureau, which is involved in cybersecurity primarily from the standpoint of hardware. For example, devices like computers and mobile phones fall under the jurisdiction of the METI. They have many technical officials in various directions at the ministry and researchers at its affiliated research institutes, just in the case of MIC above, even though their focus was traditionally rather on safety standards, OT operational safety, etc. in the past. Consequently, the METI has ample experience, resources to deal with overall cybersecurity as a main pillar with the MIC and others. Besides this generic mission for cybersecurity, the METI also plays a pivotal role for specific critical infrastructure protection. Amongst fourteen CI sectors of Japan, the METI is responsible for five as sectoral competent authority/regulator: electric power supply, gas, chemical, credit card, petroleum (NISC, 2020). It is easy to imagine how it would be disastrous if nuclear power plants or power grids were targeted by cyberattacks.

Thus, the competent sections for such CI areas of METI's coverage should take appropriate measures to have them protect themselves adequately, as competent authority for CI, as described at the beginning of this section.

The METI recently places a particular focus on supply chain risk. Supply chain risk is becoming more and more of a reality. As the ministry in charge of hardware, the METI is watching the situation carefully and considering how to respond, in cooperation with NISC and NSS if necessary.

Ministry of Defense

The Ministry of Defense (MOD) is involved in cybersecurity from the standpoint of national defence. However, cyberattacks differ in nature from attacks by conventional weapons that fire explosive munitions. Besides, notwithstanding its capability, the MOD has traditionally taken an extremely prudent approach as to how it should be involved in general cybersecurity for fear of meddling in civilian domain.

In March 2014, a cyber defence unit was established under the direct leadership of the Minister of Defense. However, according to the initial explanation, the mission of the cyber defence unit was only to protect the systems and networks of the MOD and the Self-Defense Forces (SDF), and there were around 100 people in the unit at its launch. Based on the budget of fiscal year 2018, the number of personnel was increased to around 150, but this is quite small compared to the nearly 7,000 people in the United States Cyber Command. The Japan Ground Self-Defense Force (JGSDF), Maritime Self-Defense Force (MSDF), and Japan Air Self-Defense Force (JASDF) also have personnel in charge of cybersecurity, which brings the total up to around 430 people, but there is still no comparison with the U.S. Cyber Command, other major like-minded countries posture or even with possible adversaries' one.

Working with the NSS, the MOD played a leading role in drawing up the new National Defense Program Guidelines (NDPG). Within the MOD, the Bureau of Defense Policy oversaw the NDPG, and the Defense Policy Division prepared the draft.

Ministry of Foreign Affairs

The Ministry of Foreign Affairs (MOFA) has been working to secure their communication systems since historically long as the diplomacy relies much on secured communication which should not be deciphered by a third party. But it is quite recent that the MOFA became fully engaged in more general cybersecurity policy after such eye-opening events as cyberattacks against Estonia in 2007 and the substantiation of cyber-diplomacy like in the United Nations negotiations on cybersecurity as below. At the meeting of the Information Security Policy Council (ISPC) held on 26th April 2012, Minister of Foreign Affairs, Koichiro Gemba, made the position clear, saying, "Today there is a fundamental discussion going on in international society about whether or not conventional international law will apply to cyberspace. The MOFA has looked at the issue from all angles, and we believe that it is appropriate to take the position that conventional international law should rightfully apply to cyberspace as well" (Information Security Policy Council, 2012). One year later, in May 2013, it was decided to add the Minister and Ministry of Foreign Affairs to ISPC as new regular member.

The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE)

is a UN-mandated working group and has been held so far five times intermittently since 2004. The first three UNGGE, fifteen countries participated. Participation increased to twenty countries the fourth group and to twenty-five countries the fifth time. Japan has consecutively participated in the UNGGEs since the third group in 2012. Japan provided a written input, at the fifth UNGGE which failed to make a consensus report as discrepancies of views between the West, Russia and China have not been converged: "Japan believes that cyberspace should be a space where freedom is assured without unnecessary restrictions, and where all actors who wish to access it are neither denied nor excluded without legitimate reason. Our efforts comply with the following five principles; free flow of information, rule of law, openness, self-governance, and multi-stakeholder approach" (U.N. General Assembly, 2017). Japan joined the current - sixth UNGGE, which started in 2019.

The MOFA is engaged in active bilateral cyber dialogue with fourteen countries and area as well as participates in many multilateral and regional dialogues in consort with other relevant ministries. To lead such international formal talks with counterparts, an ambassador at large in charge of cyber-diplomacy was first nominated in 2012 and followed by a setting-up of an independent Cyber Security Policy Division in 2016, the mission of which had been previously assumed by National Security Policy Division under the Foreign Policy Bureau.

PRIVATE SECTOR AND PUBLIC PRIVATE PARTNERSHIP

Even this paper intends to shed lights on public governance, the importance of private sector's participation and public private partnership in overall cybersecurity governance cannot be overstressed.

Like in most of countries, as internet has developed mainly in academia and private sector at first, the birth of cooperation hub was born in private sector. Today, Japan's so-called national CSIRTs are two: one is the NISC for government and CI, another is the JPCERT/CC for private company and individuals. The JPCERT/CC was created in 1996 much earlier than NISC and still maintain its legal status as a private entity and operational independence despite the fact that the government (METI and NISC) financially backs it up and closely cooperates with it.

Private cybersecurity-related organisations are developing. The Japan Network Security Association (JNSA) has 254 member companies as of March 1, 2021 (Japan Network Security Association, 2021), most of them can be placed in one of three groups: (1) subsidiaries of major corporations, (2) foreign companies, or (3) small and medium-sized enterprises. Not many major corporations specialize in cybersecurity.

The Japan Business Federation (Keidanren) has also been actively working on cybersecurity measures in recent years. Working with the Japanese government, Keidanren is attempting to promote Society 5.0 and believes that cybersecurity is essential for achieving that policy. Keidanren engages in research on cybersecurity as part of a subcommittee, makes suggestions, and puts on campaigns to promote public awareness. The Keidanren Declaration of Cybersecurity Management was issued in March 2018 (Keidanren, 2018).

Sectoral private cooperation like ISACs (Information Sharing and Analysis Center) are important. In Japan, ICT ISAC was the first one created in 2002, followed by Financial

ISAC and others. The government (NISC) is trying to facilitate and encourage cross-sectoral, public/private information sharing with strict respect of their autonomy, in such initiatives as CEPTOAR/CEPTOAR Council from 2009 for CI and Cybersecurity Council since April 2019 which we will see bellow.

JAPANESE GOVERNMENT STRATEGIES AND LAW

INFORMATION SECURITY STRATEGY TO PROTECT THE NATION

The distributed denial of service (DDoS) attacks against the United States and South Korea in July 2009 were a wake-up call for Japan on cyberattacks. In a DDoS attack, the targeted computer is flooded with access requests from countless number of machines, making its services unavailable. Large-scale DDoS attacks were launched at U.S. government websites and media on July 4, 2009, as the nation was celebrating its Independence Day. Three days later, on July 7, similar attacks were launched against government, media, and portal websites in South Korea.

In both countries, internet speeds dropped, and the targeted servers stopped responding, but there was no physical damage. However, two years prior to that, a DDoS attack was organized against Estonia, and because of the country's advanced use of information and communication technology, social functions were brought to a standstill. South Korea had prided itself in being a broadband Internet leader, making the impact of the DDoS attack significant, and the incident came to be called the "7.7 DDoS Attack."

The Japanese government was rocked by DDoS attacks against its ally, the United States, and neighbouring South Korea. In a press conference on December 17, 2009, Hirofumi Hirano, the Chief Cabinet Secretary of Yukio Hatoyama's cabinet said, "The (Japanese) government recognizes that the possibility of being targeted by similar attacks cannot be denied. Addressing cyberattacks and other such threats is an important challenge for national security and crisis management."

In response to instructions from the national government, the Information Security Policy Council announced the Information Security Strategy for Protecting the Nation the following year on 11th May 2010. Even before this strategy, the NISC and the Information Security Policy Council had presented various policies and plans since their establishment in 2005. However, inside the Japanese government, it was generally seen as a mere technical issue. This strategy, on the other hand, sought to boldly promote swift efforts from a national security and crisis management standpoints, based on the assumed possibility of a large-scale cyberattack (Information Security Strategy for Protecting the Nation, 2010).

About four months after the announcement of the strategy, on the morning of 7th September 2010, a Chinese trawler, operating near the Senkaku Islands, collided with boats of the Japan Coast Guard, which considered its operation to be illegal. The captain was arrested, and video of the collision was released, resulting in rapid deterioration of relations between China and Japan. In conjunction with this incident, there were posts on Chinese bulletin boards about conducting cyberattacks against Japan. The posts recommended a denial of service (DoS) attack against

a list of targets, including websites of Japanese government agencies, companies, and manga artists. A tool was distributed for automatic, repeated accessing of the targeted websites.

The Japanese government was aware of the posts, and each agency took action based on the Information Security Strategy for Protecting the Nation. The DoS attacks did take place, but no significant damages were reported.

CYBERSECURITY STRATEGY 2013

On 11th March 2011, a large-scale earthquake and subsequent tsunami hit north-eastern Japan. It was a major disaster, resulting in many dead and missing and a loss of power supplied to the Tokyo Metropolitan area by the Fukushima Daiichi Nuclear Plant. Its reactors melted down one after another, scattering radioactive material and forcing residents in the surrounding areas to evacuate. Power supply was greatly diminished, which led to planned outages in the Metropolitan area. Aftershocks followed, and the state of emergency continued.

Twenty days after the initial earthquake, an email with the subject, "Yesterday's Radiation Levels," was sent to officials in the Japanese government. Amidst the confusion caused by the Fukushima Daiichi Nuclear Plant, many recipients opened the attached PDF. This file contained a customized computer virus. Customized means that it had been tested beforehand using commercial anti-virus software to ensure it was not detected before it was sent. This exposed Japanese government computers to remote access.

Six months after the earthquake, in September 2011, it became clear that the Japanese defence industry had also been targeted. The email server of the Society of Japanese Aerospace Companies (SJAC) was secretly attacked, and an outside party had read SJAC emails. The SJAC is an industry organisation, and their email server was vulnerable to the attack because they had not implemented a cybersecurity policy. Their reasoning was that they did not have any important confidential information. Consequently, fake emails, indistinguishable from real ones, were sent to member companies. One of the recipients was Mitsubishi Heavy Industries (MHI).

MHI employees opened the attachment, believing the email to be an authentic one from the SJAC, and this led about eighty MHI computers and servers to become infected with a virus. This, in turn, resulted in an information leak. A later investigation showed that no serious information had been leaked from MHI, but it was clear that not only the Japanese government, but private companies as well, had been targeted, and this sent shock waves through Japanese society.

In 2010, when the Information Security Strategy for Protecting the Nation was issued, the Democratic Party of Japan was in power. In December 2012, however, the governing party changed when Shinzo Abe of the Liberal Democratic Party became prime minister again. Prime Minister Abe ordered a review of the National Defense Program Guidelines established in December 2009 under the Democratic Party. In response to the dire situation of cybersecurity, he also ordered a review of the Information Security Strategy for Protecting the Nation. The National Defense Program Guidelines were revised in December 2013, but before that, on June 10, 2013, the Information Security Policy Council announced the Cybersecurity Strategy (Information Security Policy Council, 2013).

Around the time that the term Internet of Things (IoT) came into use, Japan was working on becoming the world leader in IT and recognized that a suitably safe cyberspace would have to be created for that to happen. It would be noteworthy that until then, the term "information security" had been generally. However, in order to demonstrate the necessity of promoting efforts not only for technical information security but more broadly for cyberspace, the term "cybersecurity strategy" was adopted. The aim was to develop "world-leading," "resilient," and "dynamic" cyberspace and make Japan a global leader in cybersecurity. "Resilience" became a keyword.

BASIC ACT ON CYBERSECURITY 2014, REVISED IN 2016 AND 2018

After the Cybersecurity Strategy was published in 2013, the Japanese government went to work on drafting and implementing policies to achieve the objectives. The first step was the establishment of a cyber defense unit under the Joint Staff Office of the Self Defense Forces in March 2014, as previously mentioned. In November 2014, the Diet enacted the Basic Act on Cybersecurity (Basic Act on Cyber Security, 2014).

The main purpose of the Basic Act is not to achieve specific individual policies but to provide organisational structure and basic guidelines for the medium to long term.

With this, the Information Security Policy Council was reorganized into the Cybersecurity Strategic Headquarters that is given legal foundation. The NISC is not explicitly stipulated by name at the level of the Basic Act, but its head, Assistant Chief Cabinet Secretary is designated as a person in charge of Secretariat for the HQ.

Since the entry into effect of the Basic Act on Cybersecurity at 1st January 2015, it was revised twice, in April 2016 and in December 2018. The first revision was to enlarge the Cybersecurity Strategic Headquarters and the NISC's mandate of network monitoring, cybersecurity audit, and investigation of serious incidents, which were previously limited to central government ministries and agencies, to add 87 Incorporated Administrative Agencies and 9 Special Corporations. They are not government agencies in narrow sense but exercises quasi-public functions. A major information breach at one of them - Japan Pension Service - occurred in 2015, pushed the government to this reform. Even though, the enlargement has not gone beyond as far as private critical infrastructure operators, in consideration of private sector's autonomy. The second revision in 2018 aimed at creating a Cybersecurity Council, a framework of cooperation between mutually entrusted voluntary members. Taking into account of major common concerns of the private sector, the Basic Act was amended to include legal obligation of cooperation among the Council members to waive the obligation under the privacy law in some conditions with regard to information pertaining to their client, as well as sanctions against deliberate information leakage shared at the Council to protect them.

CYBERSECURITY STRATEGY 2015

At the end of November 2014, the month that the Basic Act on Cybersecurity was enacted, it became clear that Sony Pictures Entertainment (SPE) had been the target of a cyberattack.

Sony had been severely criticized in April 2011 when the personal information of 77 million people was leaked from the PlayStation Network. SPE is an American subsidiary of Sony, so the attack cannot be said as targeting a Japanese company, but because the Sony brand is a Japanese one, the incident has shaken Japanese society.

Moreover, the U.S. government attributed the cyberattack on SPE to the North Korean government. Once it became clear that a national government targeted a company in a foreign country, the shock was even greater. The reason for the attack seemed to be the film The Interview that SPE was set to release. The film ridiculed North Korean leader, Kim Jong-un, and is thought to have infuriated North Korean leadership. Around two weeks after the attack was discovered, the U.S. Federal Bureau of Investigation (FBI) announced the results of their attribution investigation and pointed the finger at North Korea (FBI National Presse Office Press Release, 2014). The NSA also participated in the FBI's attribution investigation (Winter, 2015). Michael Rogers, Director of the NSA, said that they were able to trace the path taken by the malware (Japan Network Security Association, 2016) over the Internet from North Korea to SPE in California (De Souza, 2015).

At that time, only two years had passed since the Cybersecurity Strategy was announced in 2013, but the Japanese government began working on revising it to address the enactment of the Basic Act on Cybersecurity and further changes in the cybersecurity environment. The Cybersecurity Strategic Headquarters initially planned to decide on the new strategy by June 2016.

However, in May 2015, a cyberattack was launched against the Japan Pension Service, and reports said that a large amount of pension information (pension numbers, pensioner names, addresses, and telephone numbers) was leaked. It was later confirmed that 1.25 million individuals' information had been breached. The Japan Pension Service is not a core agency of the Japanese government but rather a special public corporation. As such, part of its susceptibility was that it had been left out of priority cybersecurity measures of the Japanese government.

The investigation showed that there were problems in how the Japan Pension Service handled data, and human error was a major factor behind the leak. In a report published on August 20, 2015, the Japan Pension Service promised fundamental reform of its governance practices and organizational climate (Japan Pension Service, 2015).

The government failed to prevent the cyberattack, and although the attack was detected after the data was stolen, once data leaked, there is no way to get it back. The approach of anticipation, as described in this paper, was missing. It is impossible to predict every cybercrime, act of cyber espionage, and cyberattack before they occur. However, it is possible, to a certain extent, to identify trends in what kind of data criminals, spies, and attackers are targeting and what kinds of methods they may use. If anticipatory steps had been taken, the incident may have been prevented or mitigated..

The report on the result of post-mortem investigation includes the following very interesting statement:

This report includes information that could be used to infer the NISC's incident handling capabilities, but in light of the severity of the incident, we are disclosing as much information as possible to clarify the facts and have put the report together from the standpoint of accountability.

Indeed, the report shows how the NISC detected and addressed the incident, but it does not include attacker's attribution. There were no later reports of the stolen pension information being traded on the black market. As such, it is unlikely that the attacker's motive was money. If the Japanese government had the capabilities, attribution would have been an option. However, even if the Japanese government were able to identify the attacker, whether or not to announce it would have been a political decision. Accordingly, it is not possible to determine the actual attribution capabilities of the government from the outside.

Because of this incident, the almost-complete Cybersecurity Strategy was reviewed. It was approved by the cabinet on 4th September 2015, and made public as the 2015 Cybersecurity Strategy (Cybersecurity Strategy, 2015). The Basic Act on Cybersecurity was also amended to enlarge the umbrella of protection as mentioned in previous section.

CYBERSECURITY STRATEGY 2018 (CURRENT) AND 2021 (UPCOMING)

In May 2017, the WannaCry ransomware spread like wildfire among infected computers that had not installed essential Windows Update patches. There were as many as 200,000 victims in 150 countries. When WannaCry began spreading explosively in Europe, it was already after business hours in Japan, and this provided some time to respond before business resumed the next day. Additionally, fewer Japanese computers lacked the update as compared to those in other countries, and, so, the damages were not as great in Japan. The number was not zero, however, and there were cases where infections spread to Japan via affiliated companies overseas.

Under these circumstances, the Abe Cabinet approved a new Cybersecurity Strategy (Cybersecurity Strategy, 2018) on 27th July 2018. The 2018 Cybersecurity Strategy refers to cyberspace as a "frontier generating infinite values," while simultaneously noting that "it also increases the opportunities for malicious actors to abuse cyberspace. The risk of economic and social loss or damage in real space is expected to expand and accelerate exponentially." It also states that a response will not only be required for IoT but also for new technologies expected to be adopted in the future, including AI, financial technologies (Fintech), robotics, 3D printing, augmented reality (AR), and virtual reality (VR) (Cybersecurity Strategy, 2018).

In December 2017, the United States government attributed WannaCry to the North Korean government. Later, at a press conference on 20th December, Chief Cabinet Secretary, Yoshihide Suga, of the Japanese government announced, "We have definitively concluded that there was North Korean involvement behind the incident." However, he did not provide the grounds for the determination, stating that, due to the nature of the matter, he would prefer to withhold the details (Prime Minister's Office, 2017). This was the first case for the Japanese government to make clear public attribution.

This 2018 version of Cybersecurity Strategy is currently in use. It is set to be revised this year (2021) as in precedent cases.

On 13th May, the Cybersecurity Strategic Headquarters adopted a framework proposal of the next Strategy (Prime Minister's Office / NISC, 2021). The proposed framework further stresses increasing cyber threats, including those posed by state actors like China, Russia and North Korea, and Japan's determination to deter adversarial activities by all possible

means in cooperation with like-minded countries, together with efforts to improve its national resilience. Another pillar is to promote "Cybersecurity for all", "Digital Transformation (DX) with Cybersecurity", in tandem with the Digital Agency which will be established on 1st September 2021, as the newly adopted relevant laws stipulate. The Digital Agency is set to join the Cybersecurity Strategic Headquarters as a new regular member on its creation. The goal "Free, fair and secure cyberspace" and five principles: 1) Free Flow of Information, 2) Rule of Law, 3) Openness, 4) Autonomy of the Internet, and 5) Collaboration of Various Stakeholders, will remain unchanged.

NATIONAL DEFENSE PROGRAM GUIDELINES 2018

As mentioned at the beginning of this paper, the Japanese government approved new National Defense Program Guidelines on 18th December 2018. In a policy speech given in January 2018, Prime Minister Abe announced that the guidelines would be reviewed (Prime Minister's Office, 2018). The Council on Security and Defense Capabilities was established at the end of August in response. The NSS and the Ministry of Defense prepared the draft jointly, and it was discussed and reviewed seven times at informal gatherings. In December, the ruling parties – Liberal Democratic Party and Komeito approved the draft, thereby paving the way for a cabinet decision.

The focus of the guidelines is on cross-domain attacks and multi-domain warfare, and it pushes for improved capabilities in space, cyberspace, and the electromagnetic spectrum. Concerning cybersecurity, it specifies "the capability in an emergency to prevent the use of the other party's cyberspace used to attack Japan." This is a statement on the capability to conduct a cyber-counterattack in a careful roundabout way, excluding the possibility of pre-emptive cyberattacks. However, it shows a noticeable change from the strict defence-focused approach of the past and is significant because it clearly states that Japan will have attack capabilities in the event of an emergency (Ministry of Defense, 2019). The National Defense Program Guidelines set forth the long-term policy objectives for the next ten years, and the Self-Defense Forces are continuously working to strengthen their capabilities.

CONCLUSIONS

In this paper, we have discussed the cybersecurity governance of the Japanese government focusing on the actors, strategies, and law. As discussed in Section 2, anticipation and attribution play important roles in addressing cyberattacks. However, it is not necessarily clear that the Japanese government has been successful in both of those areas. In global or even some regional powers, civilian government agencies for signals intelligence (SIGINT) play an important role in both anticipation and attribution capabilities, but Japan does not have such an organisation.

In the days of analogue radio communications, the Defense Intelligence Headquarters of the Ministry of Defense played an important role in SIGINT. However, communications have been shifting from radio to optical fibre cable and from analogue to digital. This makes it

more difficult for SIGINT agencies to intercept information and requires that they leverage legal means to enlist the cooperation of telecommunications providers in order to monitor communications of possible adversaries and criminals.

The reason Japan has been passive in such digital SIGINT activities is the provision of secrecy of communications in Article 21 of the Japanese Constitution. There is a similar provision in Article 4 of the Telecommunications Business Act. Consequently, the Ministry of Internal Affairs and Communications and telecom providers have taken an extremely careful approach to privacy and have worked to protect the privacy of users. As seen in this paper, there have been several serious cyber incidents in Japan that pushed the government to update its cybersecurity policies. However, as no incident has led to physical damage to important infrastructure or loss of life, revolutionary policy shifts are difficult under such circumstances.

Nevertheless, the new National Defense Program Guidelines, issued in December 2018, set forth development of counterattack capabilities in the event of an emergency where a cyberattack is conducted against Japan. Even if Japan does not engage in pre-emptive cyberattacks, possessing counterattack capabilities will provide a certain level of deterrence. It is also noteworthy that the government has recently made it clear that some kind of serious cyberattack may constitute an armed attack and trigger the inherent right of self-defence under the Article 51 of the UN Charter as well as the Article 5 of Japan-US Security Treaty. It will be a challenge to determine the level of capabilities in terms of computer network exploitation (CNE), which is somewhere between computer network defence (CND) and computer network attack (CNA). CNE capabilities are key to both anticipation and attribution.

For the Japanese government and companies, cyber defence at consecutive mega international events were a big challenge. Having successfully finished the G20 Summit in Osaka and the Rugby World Cup in 2019, the Tokyo 2020 Olympics / Paralympics in 2021 and Osaka Expo 2025 will follow. There were also some cyberattacks at the Pyeong-Chang 2018 Winter Olympic Games, if not catastrophic. This again shows how difficult it is to ensure 100% security despite all the efforts engaged. Japan must continue to work on improving its cybersecurity capabilities, and to this end, sound governance is indispensable.

ACKNOWLEDGMENTS

This work was supported by Japan Society for the Promotion of Science's KAKEN Grant Number JP16KT0095 and Keio University Global Research Institute's Core Project (Security Cluster). The authors also thank Prof. Christoph Rademacher to induce us to write this paper and to give us useful comments.

REFERENCE LIST

Basic Act on Cybersecurity (2014). *Act No. 144 of 2014*, available at: http://www.japaneselawtranslation.go.jp/law/detail/?id=3591&vm=04&re=01, last visited: 17 May 2021 (all links below checked on the same date).

Cybersecurity Strategy (2015) (Japanese). Available at: https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf

Cybersecurity Strategy (2018). Available at: https://www.nisc.go.jp/eng/pdf/cs-strategy2018-en-booklet.pdf, https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf

De Souza, M. (February 19, 2015). *NSA Chief Says Sony Attack Traced to North Korea After Software Analysis, REUTERS*, available at: https://www.reuters.com/article/us-nsa-northkorea-sony/nsa-chief-says-sony-attack-traced-to-north-korea-after-software-analysis-idUSKBN0LN27Y20150219

EU (2017). *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*, *9916/17*, available at: https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

FBI National Presse Office (2014). Press Release (December 19, 2014) "*Update on Sony Investigation"*, available at: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

Fuerth, L. (2011). *Operationalizing Anticipatory Governance*, 2 PRISM 31, 31.

Government Security Operation and Coordination Team (GSOC) (2017). Objective: *Cross-organizational monitoring and quick response for the information security of governmental bodies*, available at: https://www.nisc.go.jp/eng/pdf/GSOC_Overview.pdf

Harold, S. W., Libicki, M. C., Tsuchiya, M., Ito, Y., Cliff, R., Jimbo, K. & Tatsumi, Y. (2016). *U.S. – Japan Alliance Conference: Strengthening Strategic Cooperation. Santa Monica, CA: RAND Corporation*, available at: http://www.rand.org/pubs/conf_proceedings/CF351.html

Information Security Policy Council (2012) (Japanese). Available at: https://www.nisc.go.jp/conference/seisaku/dai29/pdf/29gijiyoushi.pdf

Information Security Policy Council (2013) (Japanese). *Cybersecurity Strategy*, available at:
https://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf

Information Security Strategy for Protecting the Nation (2010) (Japanese). Available at: https://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf

Japan Network Security Association (2016). *Malicious software (malware) refers collectively to malicious software and code created with the intent to perform unlawful and harmful operations. What is Malware? (Japanese),* available at: http://www.jnsa.org/ikusei/03/08-01.html

Japan Network Security Association (JNSA) (January 1, 2019). *List of Member Companies (Japanese)*, available at: https://www.jnsa.org/aboutus/03_01.html

Japan Pension Service (2015). *Report Based on the Result of Investigation into the Information Breach at the Japan Pension Service by Unauthorised Access (Japanese)*, Available at: https://www.nenkin.go.jp/info/index.files/kuUK4cuR6MEN2.pdf

Kaplan, F. (2016). *Dark Territory: The Secret History of Cyber War*. Kindle Edition.

KEIDANREN (POLICY & ACTION) (March 2018). *Keidanren Cyber Security Management Declaration (Japanese)*, available at: http://www.keidanren.or.jp/policy/2018/018.html

Ministry of Defense (2018). "NATIONAL DEFENSE PROGRAM GUIDELINES for FY 2019 and beyond", "Medium Term Defense Program (FY 2019 - FY 2023)", available at: https://warp.da.ndl.go.jp/info:ndljp/pid/11591426/www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218_e.pdf
https://warp.da.ndl.go.jp/info:ndljp/pid/11591426/www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/chuki_seibi31-35_e.pdf

Ministry of Foreign Affairs (2017). *Statement by Press Secretary of the Ministry of Foreign Affairs on The U.S. Statement on North Korea's Cyberattacks*, available at: https://www.mofa.go.jp/press/release/press4e_001850.html

Ministry of Foreign Affairs (2018). *Statement by Press Secretary of the Ministry of Foreign Affairs on Cyberattacks by a group based in China known as APT10*, available at: https://www.mofa.go.jp/press/release/press4e_002281.html

Ministry of Foreign Affairs (2021). *Japan Coast Guard Agency, Monthly Total Number of Chinese Coastguard Intruding Japanese Seas Around Senkaku Is. from 2008-2021*, available at: https://www.mofa.go.jp/files/000465486.pdf

National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (2007). *NISC's Activities So Far (Japanese)*, Available at: https://www.nisc.go.jp/conference/seisaku/dai13/pdf/13siryou01.pdf

National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (2016). *Rules on Appointment of Deputy Head at NISC (Japanese)*, Available at: https://www.nisc.go.jp/law/pdf/kisoku2.pdf

National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (2018). *Common Standards for Information Security Measures for Government Agencies and Related Agencies (FY2018)*, Available at: https://www.nisc.go.jp/eng/pdf/kijyun30-en.pdf

National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (2020). *The Cybersecurity Policy for CIP (4th edition)*, available at: https://www.nisc.go.jp/eng/pdf/CIP_PPP_r1.pdf, https://www.nisc.go.jp/eng/pdf/CIP_4th_Edition_r1.pdf

NICTER (Network Incident analysis Center for Tactical Emergency Response) (2021). Available at: https://www.nicter.jp/en

Office of Public Affairs (May 19, 2014). *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, available at: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Paris Call (2018). Available at: https://pariscall.international/en/call

Poli, R. (2012). Complexity, Acceleration, and Anticipation, *Emergence: Complexity & Organization*, 14(4), 124-138.

Prime Minister's Office (December 20, 2017), Press Conference of the Chief Cabinet Secretary (Japanese), available at: https://www.kantei.go.jp/jp/tyoukanpress/201712/20_a.html

Prime Minister's Office (January 22, 2018). *Policy Speech by Prime Minister Shinzo Abe to the 196th Session of the Diet*, available at: https://japan.kantei.go.jp/98_abe/statement/201801/_00002.html

Prime Minister's Office / NISC (May 13, 2021). Framework Proposal of the Next Cybersecurity Strategy (Japanese), available at: https://www.nisc.go.jp/conference/cs/dai28/pdf/28shiryou01.pdf

Rid, T & Buchanan, B. (2014). Attributing Cyber Attacks, *Journal of Strategic Studies*, 38(1-2), 4–37.

Sanger, D. E. (2018). *Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. Crown.

Schmitt, N. M. (ed.) (2013a). *NATO Coop. Cyber Defence Cent. of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare*, 15.

Schmitt, N. M. (ed.) (2013b). *NATO Coop. Cyber Defence Cent. of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare*, at 106 (Rule 30).

The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition) (January 2020). Available at: https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4_r2.pdf

Tsuchiya, M. (2012). In Andreasson, K (ed.), Cybersecurity: Public Sector Threats and Responses, *Cybersecurity in East Asia: Japan and the 2009 Attacks on South Korea and the United States, Chapter 3*, 55-76.

Tsuchiya, M. (2016). In Kushida, K. E, Kasuya, Y & Kawabata, E. (eds.), Information Governance in Japan: Towards a New Comparative Paradigm, *Cybersecurity Governance in Japan: Two Strategies and a Basic Law*, 224-248. Kindle Edition.

Tsuchiya, T. (2020). *Cyber great game – Geopolitics of politics, economy, technology and data* (Japanese), Chikura-Shobo, 6.

U.N. General Assembly (August 11, 2017). *Developments in the Field of Information and Telecommunications in the Context of International Security, at 15, U.N. Doc. A/72/315*, available at: https://undocs.org/A/72/315

U.S. Department of Defense (2018). *Summary: Cyber Strategy*, 1-2, available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

White House Office of the Press Secretary (June 8, 2013). *Remarks by President Obama and President Xi Jinping of the People's Republic of China after Bilateral Meeting*, available at: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint

White House Office of the Press Secretary (September 25, 2015). *FACT SHEET: President Xi Jinping's State Visit to the United States*, available at: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

Winter, J. (January 10, 2015). *NSA Played Key Role Linking North Korea to Sony Hack, INTERCEPT*, available at: https://theintercept.com/2015/01/09/nsa-played-key-role-linking-north-korea-sony-h/

Woodward, B. (2018). *Fear: Trump in the White House*. Simon & Schuster.

XTECH (November 10, 2014). *Basic Cyber Security Law enacted, Control Tower established across ministries and agencies (Japanese)*, available at: https://tech.nikkeibp.co.jp/it/atcl/column/14/346926/110700098/?ST=mkt-trend

Zetter, K. (2014). *Countdown to Zero Day: STUXNET and the Launch of the World's First Digital Weapon*. Crown.

Hidetoshi OGAWA

Is career diplomat of Japan since thirty years actually serving as Minister & Deputy Chief of the Mission of Japan to NATO at Brussels, experienced in cybersecurity policy at the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and as Assistant CIO / Director of Information and Communications at the Ministry of Foreign Affairs. He continues to engage in research on cyber affairs at doctor course of Keio University, Japan.This article is written in such capacity and does not represent goverment's official view or position.

He obtained a bachelor's degree of law from University of Tokyo and a postgraduate diploma on international relations from University of Aix-Marseille III, France.

He is a member of U.S.-based association of cybersecurity specialists "(ISC)2" as CISSP (Certified Information Systems Security Professional).

Motohiro TSUCHIYA

Is the Dean and Professor of Faculty of Policy Management at Keio University in Japan. He is a member of Space Security Division of the Committee on National Space Policy at the Cabinet Office. He was a visiting scholar at University of Maryland, George Washington University, Massachusetts Institute of Technology and East-West Center. He authored Intelligence and National Security (Tokyo: Keio University Press, 2007, in Japanese), Cyber Terror (Tokyo: Bungeishunju, 2012, in Japanese), Cyber Security and International Relations (Tokyo: Chikura Shobo, 2015, in Japanese) and co-authored Cybersecurity: Public Sector Threats and Responses (Boca Raton, FL: CRC Press, 2012) and 30 other books. He earned his BA in political science, MA in international relations, and Ph.D. in media and governance from Keio University. He received 15th Nakasone Yasuhiro Award in 2019.