https://doi.org/10.1051/shsconf/202213400159

Cybersecurity and cyber defence strategies of Japan

Erkeley Ukhanova[1*]

[1]School of International Relations, Saint Petersburg University, 199034 Saint Petersburg, Russia

Abstract. Modern national security strategies of many states attempt at covering risks and threats rising in non-traditional domains of outer space, electromagnetic and cyberspaces. Cyberattacks aim at inflicting financial, psychological, technological and physical damage at various goals from individuals and corporations to states and international organisations. One of the specific features of a cyberattack is uncertainty of its source: it is sometimes impossible to identify the attacker. All these provide incentives for states to qualify cyberthreats as threats to their national security, thus pushing them towards establishing mechanisms of dealing with these threats. As a result, more states attempt at formulating their strategies of cyber security and cyber defence. Japan, as one of the developed countries, relies heavily on its information infrastructure and telecommunication networks, and the military realm is not an exception. Since the early 2000s, the Japanese government has been elaborating its cybersecurity and cyber defence strategies, steadily unfolding its strategic vision of the new security environment. Japan has come up with a complex strategy of information security, cybersecurity and cyber defence. A key approach of the cybersecurity strategy for Japan is acting in a proactive manner while enhancing its reactive capabilities, meaning containment and sustainability capabilities accordingly.

1 Introduction

International security is a highly dynamic environment, and it gets even more complex with ever-emerging new technology. This, undoubtedly, brings new threats and challenges to nation-states. It is clear by now that cyberspace has become a realm for international conflict, just as the traditional realms of land, sea, air, and space [1]. Cyberattacks — broadly understood as any crimes and violations in cyberspace including espionage, terrorism, warfare, etc. — have become means of achieving domestic and foreign policy goals. This is evidenced by a short but yet eventful history of misconduct in international cyberspace: attacks on Estonia (2007), Iran (2010), Saudi Arabia (2012), Ukraine (2015), the USA (2016), etc.

Consequently, governments see cyberattacks as threats to national security and attempt to act accordingly. Many of them have developed national laws and regulations for cyberspace; along with international efforts to tackle the problem. Some states have even established special cyberspace forces in their military to protect their cyber sovereignty.

Most of the states that address the issues of cybersecurity consider developing their means of cyber offence and cyber defence as a vital element of their national security strategies [2]. Japan is no exception, since the early 2000s, Japan has been developing a national regulatory framework to repel and prevent cyberthreats against society and the state. This endeavour includes national security and defence; hence cooperation and coordination are within the US-Japan alliance.

2 Japan’s cybersecurity evolution

Japan’s cybersecurity strategy is presented in a set of documents, both as a part of national security strategy and as special acts. The problem of cyberthreats was first recognized by the government in January, 2000 in its «Action Plan for Building Foundations of Information Systems Protection from Hackers and Other Cyberthreats». The Plan addressed such issues as telecommunications networks protection, further improvement of the legal framework and cooperation with the private sector and international community. This document was not perfect but it was the first step, and its significance is defined by the fact that the Japanese government recognized the importance of cybersecurity planning. An according law concerning basic principles of a society built on free and secure information flow via Internet and other telecommunications networks was passed in the National Diet by December the same year. This, again, raised the issue of personal information and data protection. A competent body under the leadership of the Prime Minister was established to solve these problems — Strategic Headquarters within the Cabinet. This initial phase of Japan’s cybersecurity policy ended with the publication of «Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure», meaning attacks on telecommunications, finance, aviation, railways, electricity, gas, government and administrative services.

[*] Corresponding author: e.ukhanova@spbu.ru

Cybersecurity was further addressed in «The First National Strategy on Information Security. Toward the realization of a trustworthy society» of 2006. The Strategy clearly indicated that Japan chose a preventive approach to cybersecurity: building an infrastructure for cyberspace control to ensure crime prevention was declared one of the main goals of the government. This was amended with «The Second National Strategy on Information Security» that came out in 2009 and declared priority on cybercrime response and recovery measures.

Sudden deterioration of the cybersecurity environment in 2009 marked with large-scale attacks on several government and financial institutions of the USA and South Korea, as well as multiple occasions of personal information leakages, prompted Tokyo to address Japan's ICT infrastructure security problems once again. In May, 2010 «Information Security Strategy for Protecting the Nation» was presented, in which the new proactive approach was declared. The document described measures on uniting private and state sectors in the name of preparedness for a potential large-scale cyberattack. Among those measures were government infrastructure consolidation, strengthening of critical infrastructure, raising public awareness of malicious software, standardisation of security requirements for cloud storage technologies, improvement of personal data and e-commerce protection, implementation of strict law enforcement control and digital criminology, and expansion of international cooperation.

Thus, by the end of the 2000s, Japan had a comprehensive information security strategy. It is notable that cybersecurity at this stage was considered an integral part of information security and was addressed accordingly.

Cybersecurity as a separate and autonomous matter came into focus in «Cybersecurity Strategy. Toward a World-Leading, Resilient and Vigorous Cyberspace» (2013). According to the Strategy, cybersecurity was not only a technological problem but also a foreign and defence policies instrument. For the first time, the document directly pointed out the necessity of actualization of threats and risks originating from external actors: "Risks which are a threat to national security as well as the lives, bodies, properties and other interests of people have appeared. The actualization of threats of targeted attacks thought to be aimed at the theft of technological and confidential information from Japanese government institutions, the defence industry, critical infrastructure providers, research institutions and other entities have also been indicated" [3]. The Strategy came out as a newsworthy framework as Japan, at the moment, was in the middle of closed negotiations on TPP, and WikiLeaks kept revealing secret information on various aspects of the future agreement, e.g. copyright and pharmaceuticals. Such leakages were seen as no less than a threat because of the potential harm they could do to Japan's stance in the negotiations and to her future benefits. The Strategy also observed that cyberattacks can be used by foreign governments as part of large-scale armed attacks on Japan, and this would require proper response from the Ministry of Defence and the Self-Defence Forces of Japan (SDF). This meant that Japan took a similar approach on militarization of cyberspace as it did for space [4].

In 2014, for the first time, the legal definition of cybersecurity was presented in «The Basic Act on Cybersecurity». According to the Act, "the term "Cybersecurity" means the necessary measures that are needed to be taken to safely manage information, such as prevention against the leak, disappearance, or damage of information which is stored, sent, in transmission, or received by electronic, magnetic, or other means unrecognizable by natural perceptive functions; and to guarantee the safety and reliability of information systems and information and telecommunications networks (including necessary preventive measures against malicious activities toward electronic computers through information network or storage media for information created by electronic or magnetic means), and that those states are appropriately maintained" [5]. Furthermore, the Cybersecurity Strategic Headquarters was established as part of the Cabinet. In 2018 a new Cybersecurity Council was appointed to help prepare for the Olympic Games in Tokyo.

In terms of the principle of free, fair and secure cyberspace, Japan condemns the exclusive possession, control, censorship, theft or destruction of information by autocratic regimes, as well as the malicious use of cyberspace by non-state actors. Autocratic regimes here mean, first of all, China and the DPRK, which are accused of organizing and sponsoring many cases of cyberattacks. There is an example of a group of hackers operating under the name APT 10 Group, which is associated with the Ministry of State Security of the People's Republic of China. From 2006 to 2018, the group was involved in hacking computer systems in order to steal intellectual property and confidential business information; at least 45 companies from 12 countries involved in finance and defence were its victims. APT 10 Group has also been charged with stealing personal information from over 100,000 US Navy personnel. Cyberattacks emanating from the DPRK mostly target the financial sector, which is explained by the need to find funds for the development of its nuclear missile program when international sanctions are imposed. In 2017, hundreds of thousands of computers around the world were infected with malware called WannaCry 2.0, which is associated with the North Korean government. The virus encoded information stored on computers and in order to decrypt it the owner had to pay a ransom by transferring the cryptocurrency Bitcoin.

Evolved views of Japan on cybersecurity were exhibited in the second edition of the Cybersecurity Strategy in September, 2015. This Strategy showed a more specific and practical approach and declared the goal of ensuring "a free, fair, and secure cyberspace; and subsequently contribute to improving socio-economic vitality and sustainable development, building a society where people can live safe and secure lives, and ensuring peace and stability of the international community and national security" [6]. The second Strategy was also focused on cyber diplomacy and development of international legal framework, but said little about cyberspace implications on the national defence of Japan.

This disbalance was levelled by the third Cybersecurity Strategy of July, 2018. Cyberthreats, as it was stated in the document, can now undermine the very foundations of democracy; regimes that reject democratic values are now main actors in cyberspace. Henceforth, it is imperative to enhance Japan's cyberspace defence through improvement of deterrence capabilities and advancement of situational awareness. This leads us to the cyber defence of Japan.

3 Cyber defence of Japan

Basic principles of cybersecurity apply to cyber defence as well. It is noteworthy that, to this moment, there is no cyber defence strategy as a separate document in Japan. In fact, her strategic view here is scattered through a body of government papers, including the US-Japan alliance documents.

Cyberthreats, in the context of national defence, were first mentioned in the Defence White Paper in 2010. The significance of this problem for the armed forces was explained by the deepening dependence of defence systems stable functioning on all levels (from the central command to the troops on the ground) on the information, communication and related technologies. Cyberattacks can also be used for intelligence purposes. Therefore, it was stated in the document, cyberattacks require an asymmetric strategy that can (not only diminish the enemy's forces) but also utilise its weak spots. To enhance the endurance of the ICT systems used by the SDF, their permanent update is imperative. Other means to achieve this goal is proper response and recovery readiness for potential cyberattacks; this problem was earlier addressed by implementing the C4 (Command, Control, Communications & Computers) system in 2008. Moreover, a special unit for cybersecurity was created in the SDF structure in 2013, the unit is responsible for constant monitoring of cyberspace in order to provide security of critically important infrastructure of the MOD and coordination between the Land, Maritime and Air SDF in regard with cyber defence. The unit of about 300 personnel is also tasked with prevention and detection of cyberattacks coming from state-level external actors that aim at Japan's military information networks.

The up-to-date version of the National Defence Program Guidelines (NDPG, 2018), the document that sets forth the basic policy for Japan's defence, defines cyberspace as one of the three new factors — along with space and electromagnetic space — that can radically change the current paradigm of national security. Thus, according to the Japanese strategists, Japan should achieve supremacy in all of the three new realms. One of the means to achieve that supremacy is building up deterrence capabilities in the way that any gains from the attack would be devalued by high costs for the enemy — deterrence by denial, the concept made relevant once again by the cyber era [7]. Such deterrence capabilities are to be achieved by build-up of the forces that can act in all spheres, that is the "cross-domain operations" concept. This approach is thought to provide higher-level integration of all armed forces and to enhance their cumulative power. And, should some of them lack power, it would not affect the defence capabilities of Japan as a whole.

Implementation of this concept will most likely require even deeper integration and coordination between the SDF branches, which means more joint exercises and training. The basic reasoning behind this cross-domain operations concept is the fact that the SDF uses the same information and communications networks that make the foundation of cyberspace itself. Thus, an attack on these networks can interfere with or even disrupt the SDF resistance and confrontation capabilities. So, logically, in order to avert such attacks, the SDF has to continuously monitor the security and stability of their own information systems and networks, while also reducing the time required to fully restore their functionality should there be damage inflicted by the adversary's actions. Moreover, in the event of a physical attack on Japan, the SDF must also be able to deprive the adversary of the opportunity to use cyberspace for their own purposes.

Details of the practical fulfilment of the abovementioned ideas can be found in the Medium Term Defence Program (MTDP), a five-year plan formulated based on the NDPG that shows the total amount of expenses for the term and the quantity of major equipment to be procured. The latest version of the MTDP covers the 2019-2023 financial period. The program states that, in addition to the functional groups operating in each branch of the SDF that are tasked with ensuring the security of their networks and information systems, it is necessary to create a joint cyber defence unit to solve higher-level tasks which might include resource allocation optimization and enhanced coordination between the SDF branches.

Another task category includes improving mechanisms for information collection, processing and analyses, as well as creating a practical learning environment for testing cyber defence capabilities of the SDF. The MTDP notes the need to monitor current (technological) trends and risks associated with cyberspace, measures to prevent them; cooperation with the private sector, the expert community, as well as with the US ally and other partners.

However, in light of the said above, it remains unclear exactly how the Japanese government is going to arrange and administer coordination through all the domains, including cyberspace, in an emergency situation. The conceptual part of the Multi-Domain Defence Force strategy is not too complicated; it is the practical part that raises questions and can cause problems. For instance, to synchronize the SDF operations in the cross-domain, it will most likely be necessary to establish a joint operations command, either ad hoc or on a permanent basis. This, in turn, could bring up the necessity to amend the Self-Defence Forces Act of 1954. Another potential issue is absence of a definitive legal demarcation of means of cyber defence and cyber offence. This inevitably raises a question of the constitutionality of acquisition of the means of offence by Japan. The documents described above make it clear that Japan continues to adhere to the principles of exclusive self-defence: all initiatives to enhance the SDF capabilities are aimed at deterrence, threat prevention, systemic stability and quick recovery if such need should occur. And that includes cyberspace.

This is distinctive of the Japanese approach from that of the United States that interpret supremacy in cyberspace as a capability to engage and suppress, all as a result of their own decision — emphasis on the offensive. This distinction, obviously, cannot affect the existence of the US-Japan alliance itself, nonetheless it once again brings up the question of alliance burden-sharing — something that has negatively impacted the alliance dynamics in the past. Nevertheless, when it comes to cyberspace, the allies have more common grounds as they both see China as one of the main cyberthreats, and in their assessments of the role of the private sector in ensuring cybersecurity [8].

The US-Japan security arrangements, namely the Guidelines for Japan-U.S. Defence Cooperation, do cover cyberspace. The relevant version of the Guidelines of 2015 promotes cooperation in space and cyberspace between the allies on the same basic principles as the SDF of Japan and the United States Armed Forces are interacting according to in all other realms: operational level integration, information and experience exchange, concentration on maintaining a stable security environment. Shared values and ideals (first of all, democratic), which are mentioned in virtually all US-Japan documents, are also emphasized in regard to the bilateral interaction in cyberspace. Consultations between the Joint Chiefs of Staffs of the SDF and US Forces, Japan leadership have been held since 2006 on the basis of the Working Group on Information Support.

The US-Japan cybersecurity and cyber defence cooperation is operated through several working mechanisms. Japan-US Cyber Dialogue is one of the intergovernmental groups coordinated by the foreign ministries of the two countries on a regular basis. It is a platform for consultations, information exchange and discussion on security problems and threats that both states face in cyberspace. The Dialogue took place for the first time in Tokyo in May, 2013; according to the Ministry of Foreign Affairs of Japan, this format provides an opportunity to enhance the bilateral cooperation on a number of issues, thus further strengthening the alliance. The discussion is typically focused on information exchange, position alignment for multilateral fora, coordination of cooperation for building cyber capabilities of third countries, and private-state cooperation for cyber defence. The parties hold meetings on an annual basis.

In 2013 another bilateral platform was established, the Japan-US Cyber Defence Policy Working Group. Essentially this is another discussion floor for cyber defence policies, but for the militaries of the two countries. The declared goal of the working group is to improve coordination between the SDF of Japan and the United States Armed Forces. The group holds meetings twice a year, the parties are represented by deputy director of the Department of Defence Policy of the Ministry of Defence of Japan and deputy assistant Secretary of Defence for Cyber Policy.

In the context of cyber defence, the US-Japan IT-forum should also be mentioned. This mechanism focuses on information and communication technology exchange between the defence ministries of the two countries since 2002. For instance, liaison officers of the SDF are sent to the educational institutions of the United States Armed Forces.

The higher effectiveness of practical interaction between the two countries is achieved during joint exercises. In March, 2013, Japan participated in the international component of the US Department of Homeland Security's Cyber Storm IV exercise. The experts of this department in 2017, in turn, took part in the exercises organized by the Ministry of Economy, Trade and Industry of Japan on the cybersecurity of industrial infrastructure control systems.

Cyber defence issues are also discussed in the framework of Japan-NATO interaction. In the Joint Political Declaration of April, 2013, cyber defence was included in the list of challenges for future cooperation, along with such issues as the aftermath of natural disasters, counterterrorism, disarmament, non-proliferation of weapons of mass destruction, and maritime security. No special acts concerning cybersecurity and cyber defence have been co-signed by Japan and NATO, but their common interests and approaches are constantly emphasized in joint statements. In 2015, Japan participated for the first time in NATO's largest cybersecurity exercise, Cyber Coalition. In 2018, Prime Minister Abe Shinzo announced Japan's desire to become a member of the NATO Cyber Defence Cooperation Centre, which is responsible for developing the alliance's cyber warfare capabilities.

In 2019, Japan and NATO agreed to intensify dialogue on cyber defence issues, focusing on maintaining rule of law, and predictable, secure cyberspace. The NATO Cyber Defence Cooperation Centre annually holds The International Conference on Cyber Conflict (CyCon), dedicated to a wide range of issues, including technological. One of the key speakers in 2019 was Special Adviser to Prime Minister of Japan Sonoura Kentaro. In December of the same year, Japan took part in the regular exercise «Cyber Coalition». In the Individual Partnership and Cooperation Program between Japan and NATO, signed on June 26, 2020, cyber defence has already been declared as the first in a series of priority areas of practical cooperation, which includes joint activities, Japan's participation in NATO seminars and symposia, exchange of official representatives, and participation in exercises.

4 Conclusion

It is now clear that the Japanese government in the last decade has begun to pay increased attention to the problems of ensuring cyber security and acquiring the necessary cyber defence capabilities. Realizing that with the accelerating development of information technology, the security environment for societies with the especially high level of information and digitalization is inevitably complicated, Japan has formed, it seems, a sufficient cybersecurity strategy. A distinctive feature of Japan's cyber defence strategy is that it is a defensive strategy that focuses on improving its own capabilities and does not imply aggressive actions against other actors.

Japan's vulnerability to cyber threats has long been considered the Achilles' heel of the country's defence. However, the steps it recently has taken suggest that this problem may soon be resolved. The basic approach the Japanese government is taking for its cybersecurity policy has a lot in common with its space policy, which has been showing significant progress [9]. In the context of the US-Japan alliance, it may be promising to further discuss the extension of Japan's right to collective self-defence to cyberspace. Speaking of international level efforts, Japan does not seem to rely too much on the normative aspect as cyber legalism has been proving futile [10].

Given the obvious relevance of the processes taking place in national and international cyberspace, it is important to not only observe, but to also conceptualize them. The Japanese case presents a perfect practical and academic relevance, as reaping the rewards of science and technology progress is virtually impossible without stability and security, more so including cybersecurity.

References

1. R. Buchan, Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? Journal of Conflict and Security Law, **17(2)**, 211 (2012).
2. M. Roscini, Cyber Operations as a Use of Force, *Research Handbook on International Law and Cyberspace*, 3,9 (2015).
3. *Cybersecurity Strategy. Toward a World-Leading, Resilient and Vigorous Cyberspace*, 8 (2013).
4. E. Ukhanova, Military aspect of Japan's space program, Asia and Africa today, **5**, 22-26 (2015).
5. *The Basic Act on Cybersecurity* (2014).
6. *Cybersecurity Strategy*, 5 (2015).
7. J. S. Nye Jr., Deterrence and dissuasion in cyberspace, International Security, **41:3**, 56 (2017).
8. I. Stadnik, N. Tsvetkova, United States cybersecurity policy. The evolution of threat perceptions, International Trends, **16:3**, 164 (2018).
9. E. Ukhanova, Japan’s space policy: state support for commercial sector, Japanese studies in Russia, **2**, 63-81 (2020).
10. L. Kello, Cyber legalism: why it fails and what to do about it, Journal of Cybersecurity, **7** (2021), https://doi.org/10.1093/cybsec/tyab014.