Quad Tech Network QTN Series

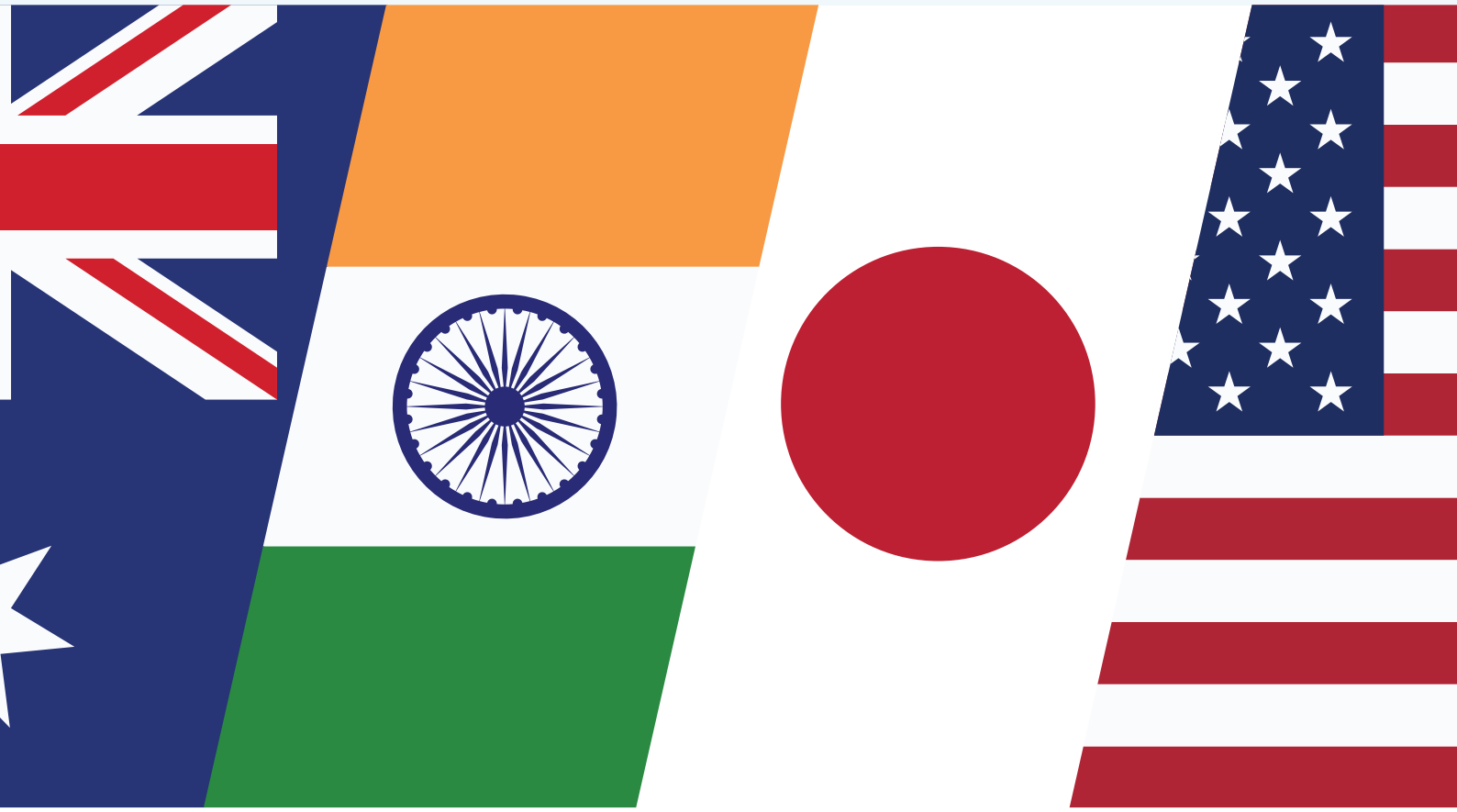
BUILDING COOPERATION: CYBER, CRITICAL TECHNOLOGY AND NATIONAL SECURITY

FEBRUARY 2021

Authors: Kohei Takahashi, Tatsuo Ide, Ikuo Takahashi, Kazuo Tokito, and Takahiro Sasaki

Paper edited by: Narushige Michishita and Kohei Takahashi

Series Editors: Katherine Mansted and Rory Medcalf



Australian National University

Center for a New American Security

政策研究大学院大学 GRIPS National Graduate Institute For Policy Studies

ORF

About the Quad Tech Network Series

The Quad Tech Network (QTN) is an Australian Government initiative to promote regional Track 2 research and public dialogue on cyber and critical technology issues.

This paper is part of a series of papers by universities and think tanks in Australia (the National Security College at The Australian National University), India (the Observer Research Foundation), Japan (the National Graduate Institute for Policy Studies) and the United States (Center for a New American Security).

The QTN series offers analysis and recommendations on shared challenges facing Australia and Indo-Pacific partners across four themes:

- international peace and security
- connectivity and regional resilience
- human rights and ethics, and
- national security.

The QTN is managed by the National Security College at The Australian National University, with the support of the Australian Department of Foreign Affairs and Trade.

About the Series Editors

Rory Medcalf is Head of the National Security College at The Australian National University. Professor Medcalf's professional background spans diplomacy, journalism, think thanks and intelligence analysis, including as founding Director of the International Security Program at the Lowy Institute from 2007 to 2015. Professor Medcalf has been recognised as a thought leader internationally for his work on the Indo-Pacific concept of the Asian strategic environment, as articulated in his 2020 book *Contest for the Indo-Pacific* (released internationally as *Indo-Pacific Empire*).

Katherine Mansted is the Senior Adviser for Public Policy at the National Security College at The Australian National University, and a non-resident fellow at the Alliance for Securing Democracy at the German Marshall Fund of the United States. She regularly writes and presents to government and public audiences on technology and security policy. Ms Mansted holds a Master in Public Policy from the Harvard Kennedy School of Government, and a first-class degree in law and international relations.

About The National Graduate Institute for Policy Studies

Located in the heart of the fascinating city of Tokyo, the National Graduate Institute for Policy Studies (GRIPS) is an international premier policy school with the aim of contributing to the betterment of democratic governance around the world. We excel at providing interdisciplinary education for future leaders in the public sector and conduct research on contemporary policy issues to generate innovative solutions. Founded in 1997 as a stand-alone graduate institute, GRIPS comprises world-class academics and distinguished practitioners with expertise in public sector policy formulation and management. Around 20 percent of the faculty and 70 percent of students are recruited from outside Japan. Our vibrant, diverse student body consists of almost 400 members hailing from 63 countries and regions – all with the ambition to advance good governance across the globe or contribute to policy related research. We offer a diverse array of masters and doctoral programs, from which students cultivate the ability to analyze issues and suggest solutions, develop interdisciplinary knowledge and skills that span related fields, and gain practical expertise. In addition to our degree programs, we also offer executive-level short-term training programs across a wide range of themes. Since our inception, our achievements in promoting good governance are considerable and far-reaching. Today, our impressive Alumni network of over 4,000 strong are actively shaping policy in more than 100 countries around the world.

For more information, please visit https://www.grips.ac.jp/en/

Australian Government

Department of Foreign Affairs and Trade

Published by the National Security College, The Australian National University, Acton ACT 2601, Australia

Available to download for free at nsc.crawford.anu.edu.au

Cover design and layout by Black Bear Creative.

About the Authors

Narushige Michishita is vice president and professor at the National Graduate Institute for Policy Studies (GRIPS) in Tokyo. He has served as member of the National Security Secretariat Advisory Board of the Government of Japan, global fellow at the Woodrow Wilson International Center for Scholars in Washington DC, senior research fellow at Japan's National Institute for Defense Studies, Ministry of Defense, and assistant counsellor at the Cabinet Secretariat for Security and Crisis Management of the Government of Japan. He acquired his Ph.D. with distinction from the School of Advanced International Studies (SAIS), Johns Hopkins University. A specialist in Japanese security and foreign policy as well as security issues on the Korean Peninsula, he is the author of "The US Maritime Strategy in the Pacific during the Cold War," in Sebastian Bruns and Sarandis Papadopoulos, eds., *Conceptualizing Maritime and Naval Strategy: Festschrift for Peter M. Swartz, Captain (USN) retired (Baden-Baden: Nomos, 2020); Lessons of the Cold War in the Pacific: U.S. Maritime Strategy, Crisis Prevention, and Japan's Role* (Woodrow Wilson Center, 2016) (co-authored with Peter M. Swartz and David F. Winkler); and *North Korea's Military-Diplomatic Campaigns, 1966–2008* (Routledge, 2009).

Kohei Takahashi is a researcher at the National Graduate Institute for Policy Studies at GRIPS. He holds a Ph.D. in sociology from the University of California, Riverside. He is a member of Center of Innovation, one of the main funding programs under the Center of Innovation Science and Technology–based Radical Innovation and Entrepreneurship Program launched by the Ministry of Education, Culture, Sports, Science and Technology in 2013.

Tatsuo Ide is Commander of the Japan Maritime Self-Defense Force and visiting researcher at GRIPS, Meiji University, and Waseda University. He holds a bachelor's degree in aerospace engineering from the National Defense Academy of Japan, a master's degree in nature and environment from the University of Air, and a doctorate from the Graduate School of Global Information and Telecommunication Studies, Waseda University. He has served as a line officer aboard JS *Yamagiri*, JS *Okishio*, and JS *Harushio*, a military system engineer in the Program Center, Command and Control System Center, and Ship System Center, and a staff in the Maritime Staff Office and the Joint Staff Office.

Takahiro Sasaki is Rear Admiral (retired) of the Japan Maritime Self-Defense Force (JMSDF), Research Principal at the National Security Institute of the Fujitsu Systems Integration Laboratories, visiting professor at the Hiroshima University and the Tokai University, and visiting researcher at the Meiji University. He holds a bachelor's degree in electrical engineering from the National Defense Academy, graduated from the Royal Australian Naval Staff College, and received a Graduate Certificate in Management from the Queensland University of Technology. He also finished the International Intelligence Directors Course at the British Intelligence School, and received a master's degree in international relations from the Nihon University. During the service in the JMSDF, he commanded destroyer JS *Yuubetsu*, and four other destroyers including Aegis-equipped destroyer JS *Kirishima* of the Escort Division Eight. He also served as defense attaché in Russia and as the First Cybersecurity Coordinator in the Joint Staff Office. He is a specialist of Russia's national security and military policy as well as cyber and information warfare.

Ikuo Takahashi is a lawyer and the president of IT Research Art. He is also a founder of the Komazawa Legal Chambers (Daiichi Tokyo Bar Association). He received an Information Security Culture Award hosted by the Institute of Information Security in 2012. He has co-authored "Digital Evidence Legal Practice Q&A," "Virtual Currency," and "IT security Café."

Kazuo Tokito is Major General (retired) of the Japan Air Self-Defense Force (JASDF), an advisor at the Defense Systems Group of Hitachi Ltd., and visiting fellow at the Japan Air Self-Defense Force Command and Staff College. He graduated from the National Defense Academy, majoring in electrical engineering. He also graduated from the JASDF Officer Candidate School. He acquired a master's degree in computer science at the National Defense Academy, and a doctorate in engineering from the Shinshu University. As for the service career, he worked at several radar sites and JASDF's Sector Operation Centers as a communications and systems officer. He worked as a chief of C4 systems division (A6) at the Air Staff Office, and as a commanding officer of Patriot Missile Group and Air Wing. His significant careers were Director of C4 and cyber (J6) at the Joint Staff Office and a base commander of the Matsushima Air Base. He retired from JASDF as a vice commander of the Northern Air Defense Command.

Contents

Executive Summary

contributed by Kohei Takahashi.

The novel coronavirus pandemic has illustrated the significant role of states in enacting effective multilateral responses toward the pandemic, which has transformed the relationship between individuals and states. However, the pandemic has also revealed the vulnerability of international governmental and non-governmental organizations, where the United Nations appears to be somewhat uninvolved. The World Health Organization (WHO) is supposed to play a central role in response to the pandemic. Instead, the pandemic has escalated geopolitical tensions that consequently reoriented geopolitics. Moreover, distrust and suspicions have been simmering among rival states – for example, the tension between the United States and China that unfolded at the annual UN General Assembly in New York on September 22, 2020. The US President Donald Trump argued that China was responsible for the pandemic as he called it the "China virus." Trump asserted: "as we pursue this bright future, we must hold accountable the nation which unleashed this plague onto the world: China … The Chinese government and the World Health Organization – which is virtually controlled by China – falsely declared that there was no evidence of human-to-human transmission. Later, they falsely said that people without symptoms would not spread the disease."[1] In response, China denounced the US global campaign to rally other states against China. In addition, Chinese President Xi Jinping argued that "we should enhance solidarity and get this through together… Any attempt of politicizing the issue or stigmatization must be rejected."[2]

Several rivals are taking advantage of the pandemic to advance "gray-zone" strategies, such as economic coercion, cyber operations, and low-intensity violence.[3] The United States Special Operations Command defines the gray zone as "competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality."[4] In other words, invisible threats are characterized as gray-zone conflicts, where the boundaries between peace and war become increasingly blurred.

In this context, the Chinese government economically pressured Australia to soften the nation's policy against China when Australia called for an independent inquiry into the origin of COVID-19. The Chinese government suspended meat imports from Australian suppliers and issued a travel warning for its citizens against Australia.[5] Accordingly, the United States has expanded what it considers to be matters of national security, which now includes medical supplies, surgical face masks, and other items essential for handling of the pandemic. However, Chinese corporations dominate the market of these products and have become integral parts of US supply chains. Bill Greenwalt, a senior fellow at the Atlantic Council and a former Pentagon official, argues that "these are now national security needs and we probably should have been thinking about it a long time ago in terms of biowarfare that we should have a trusted industrial base or a set of trusted allies – the UK, or NATO allies or Japan or Korea."[6] Therefore, the pandemic reveals the risk of China-centered supply chains.

Cyber attacks, which are one of the gray-zone methods, have become widespread during the pandemic. Australian Prime Minister Scott Morrison revealed that the government and institutions were being targeted in a "sophisticated state-based" cyber attack.[7] Although the prime minister refused to disclose the identity of the state, it is widely believed that China was responsible for the cyber attack. Similarly, India has confronted an increased number of cyber attacks from both China and Pakistan. Attacks from China surged dramatically in March 2020, mainly targeting health care and educational institutions during the pandemic.[8]

Thus, similarly inclined democratic states should cooperate and coordinate effective multilateral responses against such gray-zone tactics. Primarily, experts from academia and think tanks should be able to discuss such issues among their counterparts from allied democratic states in a forum where all participants respect the principles of transparency and freedom of expression. The Quad Tech Network (QTN) has the potential to provide such a platform. The QTN is also expected to promote engagement with academic and think tank partners for research on cyber and critical technology issues that reflect Australia's interests as a liberal democracy committed to the international rules-based order. The QTN should aim to be a platform where allies and cooperative states can collectively respond to gray-zone warfare. Consequently, it will be beneficial for the four member democracies, including Australia. In this context, Japan is one of the states that will play a vital role in this platform. Accordingly, this paper shares insights and experiences on this subject from a Japanese perspective. This paper discusses key issues in national security, cyber security, and critical technologies for Japan. It has four sections: (1) Critical Technology in the Field of Defense: A Comparison between NATO and Japan (2) Laws and Policies for Cyber and Critical Technologies in Japan; (3) Deterrence and Arms Races in Cyber Space; and (4) Chinese Cyber Warfare and Japan's Response.

The protection of critical technology, intellectual property, and data from theft or acquisition by a rival state is imperative. In the first section, Dr. Tatsuo Ide uses documents on NATO and Japan's critical technologies to clarify the critical technologies that will be vital for future defense. In addition, he compares the similarities and differences between the critical technologies approaches of Japan and other NATO countries. In the second section, Mr. Ikuo Takahashi further discusses cyber and critical technologies from the perspective of Japan's laws and policies. In addition, Dr. Takahashi describes Japan's challenges in cooperating with allied democratic states in the field of cyber security and critical technologies.

As mentioned above, cyber operations are significant in gray-zone warfare. These operations include cyber-driven cognitive attacks, such as dissemination of fake news. In the third section, Dr. Kazuo Tokito discusses deterrence and arms races in cyber space with the help of examples (Russia and Japan). Moreover, Dr. Tokito discusses the indispensable role of critical technologies such as AI and quantum science in cyber operations. In the last section, Professor Takahiro Sasaki discusses China's cyber warfare and Japan's response to it. Professor Sasaki takes up cases of cyber attacks against Japan in which China was supposedly involved and analyzes their characteristics and trends. In addition, he focuses on the future direction of China's cyber warfare and how AI will be used in such cyber warfare. Furthermore, he examines Japan's tactical responses to Chinese cyber threats. Finally, he proposes recommendations for the QTN in attenuating cyber warfare and securing global cyber space.

Common interests are autonomy, space, and hypersonics, and although there are differences, many of these technologies are expected to evolve in the future. Picture: Bill Ingalls / NASA, https://flic.kr/p/JtiLU7

A Study of Critical Technology in the Field of Defense

contributed by Tatsuo Ide.

Recently, every country has been making great effort to obtain new technologies. The acquisition of, for example, revolutionary space or hypersonic technologies will bring competitive advantages to both business and defense.

What is a critical technology? What technologies are attracting attention in the field of defense? How do countries' definitions of critical technologies differ? This section will examine these points by comparing two published documents of NATO and Japan:

- "Science & Technology Trends 2020–2040," which was published by NATO's Science Technology Organization (STO) in March 2020, and covers the period 202-02040
- "R&D Vision," which was published by Japan's Acquisition, Technology & Logistics Agency (ATLA), an auxiliary agency (external bureau) of the Ministry of Defense of Japan, in August 2019, and covers the period 2019–2038.

Although there are differences between an international organization and a national organization, the documents are suitable for comparing the views of Europe, the United States, and Japan in view of the universality of science and technology.

Definitions of Critical Technology

There are many similarities between the "Science & Technology Trends 2020–2040" and the "R&D Vision". The former was published by STO, which is an auxiliary body of NATO, while the latter was published by ATLA, which is an auxiliary agency (external bureau) of the Ministry of Defense of Japan.[9] The former was published in March 2020, and the latter was published around the same time, in August 2019. The former covers the period 2020–2040, and the latter 2019–2038.

NATO identifies three categories of technologies that will have a significant impact on future defense[10]:

1. **Emerging:** Those technologies or scientific discoveries that are expected to reach maturity in the period 2020–2040 and are not widely in use currently or whose effects on Alliance defense, security, and enterprise functions are not entirely clear.
2. **Disruptive:** Those technologies or scientific discoveries that are expected to have a major, or perhaps revolutionary, effect on NATO defense, security, or enterprise functions in the period 2020–2040.
3. **Convergent:** A combination of technologies that are combined in a novel manner to create a disruptive effect.

These three are together called "emerging and disruptive technologies." On the other hand, in Japan's "R&D Vision," innovative technologies are called "game-changers" without any particular definitions. Both are terms that mean bringing about complete changes in future defense – and so are defined here as "critical technologies."

NATO's Critical Technologies

NATO's "Science Technology & Trends 2020–2040" identifies four characteristics common to many defense technologies over the next 20 years:

1. **Intelligent:** Technologies that exploit integrated AI, knowledge-focused analytic capabilities, and symbiotic AI/human intelligence to provide disruptive applications across the technological spectrum.
2. **Interconnected:** Technologies that exploit the network of virtual and physical domains, including networks of sensors, organizations, individuals, and autonomous agents, linked via new encryption methods and distributed ledger technologies.
3. **Distributed:** Technologies that employ decentralized and ubiquitous large-scale sensing, storage, and computation to achieve new disruptive military effects.
4. **Digital:** Technologies that digitally blend the human, physical, and information domains to support novel disruptive effects.

The NATO document recognizes eight closely related areas as critical technologies for the next 20 years[11]:

1. data
2. artificial intelligence
3. autonomy
4. space
5. hypersonics
6. quantum
7. biotechnology
8. materials.

In particular, the document points out the enormous impact of the following six synergistic effects:

1. data–AI–autonomy
2. data–AI–biotechnology
3. data–AI–material
4. data–quantum
5. space–quantum
6. space–hypersonic–material.

To keep pace with these science and technology trends, NATO militaries are working together with companies to expand their capabilities, taking into account legal, policy, economic, and organizational constraints.[12]

Critical Technologies in Japan

While NATO documents are written without any particular framework, Japan's "R&D Vision" describes three areas for strengthening capability acquisition in new areas necessary for cross-area operations, and two areas for strengthening capacity in conventional areas, each of which will be implemented by 2038.

Electromagnetic Spectrum Technologies

According to "R&D Vision," the electromagnetic spectrum (EMS domain) is an important area related to wide-ranging defense activities such as Intelligence Surveillance and Reconnaissance (ISR,), information sharing, and precise guidance. It is necessary to endeavour to achieve effective and efficient use of the EMS. Technologies that the Ministry of Defense (MoD) should acquire are as follows:[13]

- Electronic attack technologies – including high-energy laser, high-power microwave, and jamming technologies.
- Electronic protection technologies – including Low Probability of Intercept/Detection (LPI/LPD) communication, anti-jamming, and electromagnetic pulse (EMP) protection technologies.
- Electronic warfare support technologies – including electronic intelligence (ELINT) technology.
- Electromagnetic spectrum technologies (EMS) – including EMS domain awareness; and optimization of frequency allocation technologies.

Technologies for Persistent ISR including Space

According to "R&D Vision," in light of nearby countries' activities and expansion of ISR targets and domains, there is a need to realize efficient and effective ISR based on improvement of sensors' detecting capability and an increase of sensor platforms. Technologies that the MoD should acquire are as follows:[14]

- Sensing and radar technologies – including over-the-horizon radar, advanced multi-static radar, ultra-long-range radar, and imaging radar technologies.
- Electro-optical and infrared sensors – including satellite-borne (EO/IR) sensors.

Cyber Defense Technologies

According to "R&D Vision," the stable use of cyber space is imperative for the Ministry of Defense (MoD) and Self-Defense Forces (SDF). It is necessary to advance research of the latest technology centered on operation continuity to support MoD/SDF activities, while strengthening collaboration with relevant ministries and agencies. Technologies that the MoD should acquire are as follows[15]:

- Manual operation continuity measures.
- Automatic operation continuity measures – including cyber and mobile cyber resilience technologies.
- Preventative measures – including cyber countermeasure for platform computer systems, anti-tamper, supply chain integrity, anti-malware and firewall, and vulnerability inspection technologies.
- Disruption capabilities.

Underwater Warfare Technologies

According to "R&D Vision," it is fundamental to develop multi-mission unmanned vehicles, as well as technology for unmanned and manned vehicles to collaborate organically as underwater defense systems, in order to drastically improve underwater defense capability and efficiency. Technologies that the MoD should acquire are as follows[16]:

- Autonomy – including situational awareness and high-reliability technologies, and behavior decision technologies for unmanned underwater vehicles.
- ISR – including detection and underwater communication technologies.
- Support technologies – including automatic docking; charge, supply, and maneuver technologies.
- Countermeasure technology – including signature reduction technology.

Stand-off Defense Technologies

According to "R&D Vision," it is necessary to acquire a stand-off capability out of an adversary's effective range that can secure personnel safety due to its high survivability, long range, and hypersonic velocity. Technologies that the MoD should acquire are as follows:[17]

- Fire control – including satellite guidance technologies, and infrared radar seekers compatible with hypersonic missile technology.
- Propulsion technologies – including scramjet engine, and high-performance rocket motor technologies.
- Airframe and warhead technologies – including advanced warheads for anti-surface missiles, aerodynamic airframe design for gliding projectiles at high altitude, and gliding flight control aerodynamic design technologies.

Similarities and Differences

While NATO's "Science & Technology Trends" document focuses on elemental technologies, Japan's R&D strategy is centered on developing and applied technologies.

Comparing the critical technologies of interest between the two, the following commonalities were revealed. It should be noted that the granularity of the items is finer in Japan, so to facilitate the comparison only the large items in Japan were covered. Table 1 summarizes the common areas.

Differences in NATO, where there is no equivalent in Japan, were data, artificial intelligence, quantum, biotechnology, and materials. Also in Japan, areas where there is no equivalent in NATO were electronic spectrum (EMS) technologies and cyber defense technologies. These technologies are expected to be used universally in society in the future.[18] Although they are not central issues, they will be used in both countries.

While NATO's documents describe emerging and disruptive technologies, Japan's documents describe in detail technologies that are required in connection with future operational and defense needs. In other words, NATO uses a technology-based approach, whereas Japan uses an operational-based approach. In preparing for the future, there is a need to involve a wide range of stakeholders, including technology experts and companies, and to position them in a policy approach, but Japan's approach is to position them in operations.[19] However, the game-changer that Japan is looking for is not a needs-based one, but a seeds-based one, and the seeds-based approach like that of NATO is likely to be suitable. NATO and Japan will be able to find common interests in the fields of autonomy, space, and hypersonics, where research cooperation may also be possible.

Table 1: Common areas in critical technologies

"Science & Technology Trends 2020–2040" (NATO)	"R&D Vision" (Japan)
Autonomy	**Autonomy** • Situational awareness technology • High-reliability technology • Behavior decision technology for unmanned underwater vehicles
Space	**EO/IR sensor** • Satellite-borne EO/IR sensor technology **Fire control** • Midcourse guidance via satellites technology
Hypersonics	**Propulsion** • Scramjet engine technology • High-performance rocket motor technology **Airframe and warhead** • Aerodynamic airframe design of gliding projectile at high-altitude technology • Gliding flight control aerodynamic design technology

Conclusion

Japan's "R&D Vision" mainly describes operations in five fields, while NATO's "Science & Technology Trends 2020–2040" describes mainly the technologies without setting a particular framework. Common interests are autonomy, space, and hypersonics, and although there are differences, many of these technologies are expected to evolve in the future, and the differences are simply those of perspective.

In summary, NATO focuses on seeds, and Japan considers operations as needs, and each approach has its own advantages. However, if Japan is looking for a game-changer, the seeds-based approach that comes from examining technology, rather than the needs-based approach that comes from operations, is more flexible and purpose-based.

Cyber and Critical Technologies: Law and Policy in Japan

contributed by Ikuo Takahashi.

Cyber Laws and Policies

In 2000, the "Basic Act on the Formation of an Advanced Information and Telecommunications Network Society" (the "IT Basic Law") was enacted, encouraging society to use the internet. In January 2001, the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society was established in the Cabinet to formulate specific strategies.[20] Then, a new IT strategy was announced in 2019. In addition, a new IT strategy for 2020 has been announced that incorporates many perspectives on changes in society and values and issues brought about by the coronavirus pandemic and responses to it.

Regarding cyber security, the Cyber Security Basic Law forms the basic legal framework.[21] In January 2015, the Cyber Security Strategic Headquarters was established based on this framework, and the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) plays a practical role in Japan's cyber security strategy as its secretariat. The NISC includes the Government Security Operation Coordination Team (GSOC) and the Cyber Incident Mobile Assistant Team (CYMAT).

The cyber security scene is changing rapidly, and two recent legal changes are worth noting. First is an amendment to the Cyber Security Basic Law, which established an information-sharing council to discuss the promotion of cyber security measures by various public and private-sector entities in cooperation with each other. The law clarifies that the members of the council include national administrative bodies, local governments, critical infrastructure providers, cyber-related businesses, educational and research institutions, experts, etc., and also stipulates measures such as applying the duty of confidentiality and information sharing to the council members.

Second is the "Act to Amend the Telecommunications Business Act" which gave the National Institute of Information and Communications Technology the right of access to Internet of Things (IoT) sites under limited conditions. The amendment also requests telecommunications providers that administer vulnerable IoT sites to take measures against cyber attacks.

Critical Technology Law and Policy

The "Basic Act on the Advancement of Public and Private Sector Data Utilization" was enacted in 2016 to support the drastic reform of society.[22] Further, regarding critical technologies, the new IT strategy (2020) states the following goals: "social implementation of digital technology," "realization of an inclusive society through data utilization," and "improvement of social infrastructure." It lists the following technologies as basic technologies for "improvement of social infrastructure":

1. AI-ready social infrastructure creation
2. cloud utilization and evolution of edge computing
3. security measures in the digital age, and
4. the use of new technologies such as blockchains.

Further, states that edge computing power, 5G technology, which can send and receive high-speed data, and the blockchain with its excellent recordability, are increasingly likely to be added to the basic technologies.

The following is an overview of policies in Japan in three key areas: artificial intelligence, robotics, and quantum computing.

Artificial Intelligence

The new IT strategy (2020) states, "Although discussions on the ethical aspects of AI are progressing in the international community, Japan is also actively promoting AI social principles in UNESCO, OECD, G7, G20, etc. It leads international discussions." Japan's "AI Strategy 2019" was decided by the Integrated Innovation Strategy Promotion Council on June 11, 2019. To that end, the "Human-Centered AI Social Principles" (decided by the Integrated Innovation Strategy Promotion Council on March 29, 2019) summarized seven AI principles regarding social frameworks in an AI-ready society: (1) human-centered principles; (2) education and literacy principles; (3) privacy principles; (4) security principles; (5) fair competition assurance principles; (6) fairness, accountability, and transparency principles; and (7) innovation principles. The AI strategy is being strongly promoted by the Integrated Innovation Strategy Promotion Council, as well as the AI Strategy Execution Council established under the Council.

Robotics

Legally, industrial robots are defined in Article 36, No. 31 of the Ordinance on Industrial Safety and Health. However, what is recognized as a critical technology is defined as a "next-generation robot" in Japan. Next-generation robots are defined as non-industrial robots – that is, "robots that share the operating domain with the human domain."

Although there is no specific description in the IT strategy (2020), the Ministry of Economy, Trade and Industry (METI) held the "Next Generation Robot Vision Roundtable" (2003–2016) and published technical guidelines on safety standards such as for the use of robots, guidelines on comprehensive safety standards for machines, and guidelines for ensuring the safety of next-generation robots.

Quantum Computing

The IT strategy (2020) states that "we will work on technological development such as next-generation computing technologies

(quantum computers, brain-type computers etc.) that achieve both high speed and low power consumption." METI will promote technological development based on the "Technology Development Project for AI Chips and Next-Generation Computing that Enables High-Efficiency and High-Speed Processing" (FY2018 – FY2019).

In addition, the emergence of quantum computers is promoting the emergence of quantum-safe computing (that is, algorithms that are resistant to attacks by quantum computers) based on the same strategy.

Enabling and Protecting Cyber and Critical Technologies

This section examines specific legal issues in relation to how Japan responds to security challenges in the areas of cyber security, AI, and robotics.

Legal Issues in Cyber Security

Japan is resported to have suffered a number of cyber security breaches by state-sponsored actors (hereinafter referred to as "cyber operations"). These include: the Mitsubishi Heavy Industries incident[23] (July 2009 to September 2011), targeted attacks on METI (November 2010), cyber attacks on the National Police Agency (around July 2011), intrusions into the House of Representatives (July 25, 2011), cyber attacks on the House of Councillors (2011 and July 2006), cyber operations against the Japanese Pension Scheme[24] (2015) and operations against major electronics manufacturers (2019).

Japan's response to such cyber operations is based on the most standard interpretation of international law in accordance with the severity of the damage, and the country is prepared to respond on the basis of domestic law. Moreover, it responds based on such rules in order to contribute to the development of state practice.

Japan's response can be discussed in terms of armed attack, emergency, and lesser cases depending on the severity of the damage. For situations corresponding to armed attacks per Article 51 of the UN Charter, domestic laws have been developed such as the "Act on the Peace and Independence of Japan and Maintenance of the Nation and the People's Security in Armed Attack Situations, etc." Such situations are called "armed attack situations and anticipated armed attack situations" and the Japanese government has acknowledged that this law may be applied in the event of situations resulting from cyber methods as well.[25]

In addition, countermeasures can be taken against violations of sovereignty even when cyber attacks do not constitute armed attacks. This principle of international law is of course accepted in Japan as well.

However, it is unclear whether tangible force can be used against the source of the attack in a state of emergency and, if so, which entity may use it and under what domestic law. Matters necessary for police officers to perform their duties are regulated by the "Police Duties Execution Act."[26] The purpose of the Act is to provide for the necessary means for the faithful performance of ex-officio duties. The Act authorizes: questioning (Article 2); protection (Article 3); measures for refugees, etc. (Article 4); prevention and suppression of crimes (Article 5); entry (Article 6); and use of weapons (Article 7). The question here is whether the provisions for the prevention and cessation of crime of Article 5 of the Act can be applied to serious cyber crimes. The Article states that "A police official may, when he or she notices that a crime is about to occur, give necessary warning to the persons concerned in order to prevent such occurrence, and may restrain the actions of such persons in the event that such actions may endanger the lives or bodies of persons or cause serious damage to property and if the matter is urgent." The term "restraint" is used here, but restraint is considered to mean "to prevent an attempted crime from being committed by force" and generally includes measures such as primary restraint of the body and taking away a weapon. However, there is no mention of any of the above-mentioned acts of restraint that would deter cyber crimes, and thus the Act cannot be said to address cyber crimes. Anything less would generally be dealt with as a mere international cyber crime.

As for state-sponsored attackers, the Japanese government condemns specific attacks by clearly attributing the attack to the state. The WannaCry incident is a concrete example.[27]

Safe and Ethical Use of AI

On June 11, 2019, the AI Strategy Executive Committee announced its 2019 Strategy, "AI for Everyone: People, Industries, Regions and Government." This strategy sets out three principles: dignity, diversity and inclusion, and sustainability; and four strategic objectives: human resources; industrial competitiveness; a sustainable society that incorporates diversity; and international leadership and cooperation in R&D, education, and building research networks.

As part of these efforts, the Office will examine the nature of Japan's AI governance, including ethical frameworks, regulations, standardization, and audits, which will contribute to strengthening Japan's industrial competitiveness and improving social acceptance of AI, while keeping a close eye on domestic and international trends, with the aim of implementing the social principles of AI. Japan's Cabinet Office also promulgated its "Social Principles of Human-centric AI," and is participating in a number of multilateral discussions on AI ethical frameworks.

METI has formulated "Contractual Guidelines for the Use of AI/Data" (Version 1.1), which presents the main issues and points of contention for each type of data contract for which no standard template has been established, and also presents examples of contractual clauses and factors to be considered when drafting the clauses. These are intended to be easy for the public to use, in order to reduce transaction costs. The purpose is to reduce the number of data contracts and promote the spread of data contracts and, in turn, the effective use of data.

Also related to cyber security, projects are underway to encour-

age the private sector to build cyber defenses using AI, and to develop measures to support the practical application and technology transfer of national research.

Safe and Secure Use of Robotics

The Japanese government established the Council for the Realization of the Robotic Revolution in 2014, and ministries and agencies are actively working to make this happen.

Regarding individual applications, there are already many projects working toward the practical application of self-driving vehicles, and discussions are underway to establish vehicle safety standards, such as for automatic braking and cyber security measures for passenger cars. In addition, guidelines were published in September 2018, summarizing the safety requirements to be met by self-driving vehicles at level 3 of autonomy and above. The guidelines set the goal of "achieving a society in which self-driving systems cause zero fatalities," and are designed to promote the development and commercialization of safe automated vehicles.[28] In addition, the "Road Transport Vehicle Act" was amended in 2019 to ensure the safety of automated vehicles.

Prospects for International Cooperation in Cyber Security

The challenges to promoting cyber security in Japan include the lack of a centralized response organization, the inadequacy of the analysis organization, the lack of a security clearance system, the weakness of the posture on active cyber defensive actions, and the ambiguous status of active cyber defense.

Absence of a Centralized Response Organization

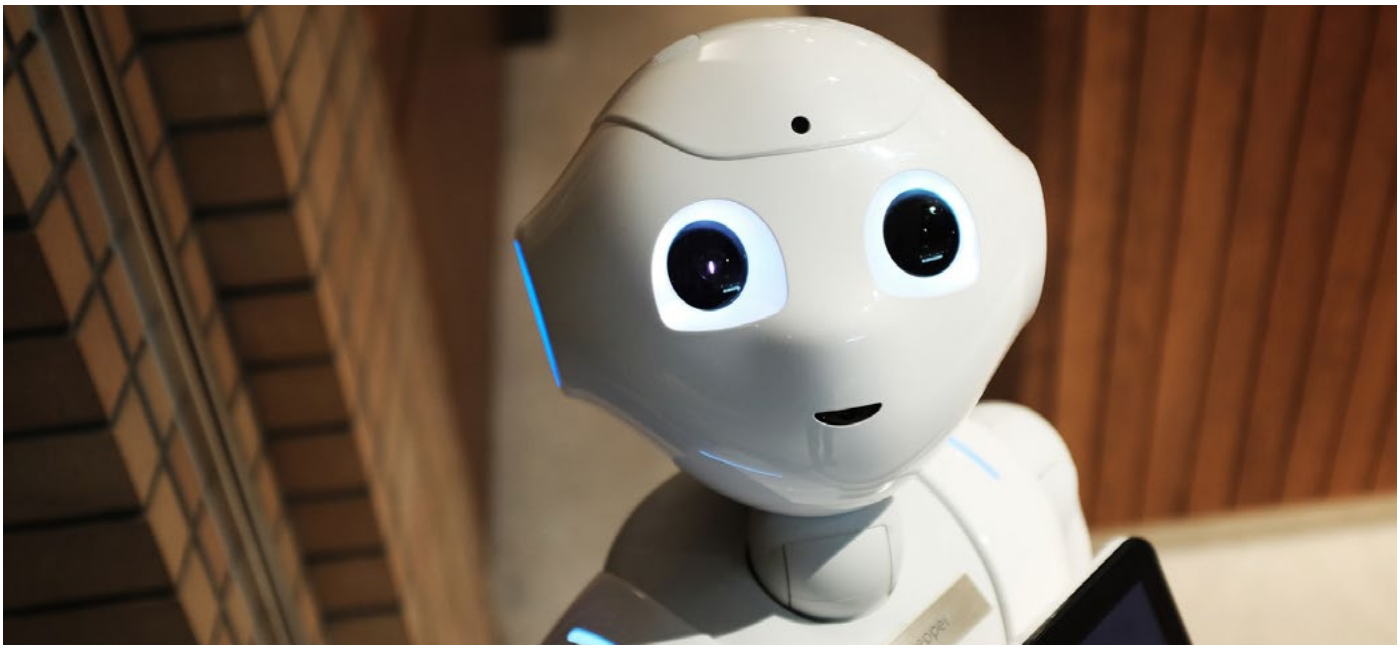
Currently, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) is responsible for responding to cyber attacks, but its budget, personnel, and authority are deemed insufficient. The Sasakawa Peace Foundation has proposed that a Cyber Security Agency, which would be a reorganized and strengthened version of NISC, should be established under the Cabinet Office External Bureau as a practical organization to deal with cyber attacks. The new agency should deal with cyber attacks in a unified manner to carry out the detection, analysis, judgment, and response of cyber attacks in a unified and prompt manner, as well as carry out various other tasks.

Inadequate Analytical Organization

In Japan, there is no mechanism or governmental intelligence organization responsible for analyzing cyber-related information and there is no specific organization responsible for analyzing the related international situation. Globally, there is Cyber Command and the National Counterintelligence and Security Center (NCSC) in the United States and Government Communications Headquarters (GCHQ) in the United Kingdom, yet there is no such analytical intelligence agency in Japan for cyber-related matters. There is no denying the insufficiency in terms of organization and human resources, even if a certain level of information analysis is done.

Clearance System

The clearance system in Japan is inadequate. The "Act on the Protection of Specified Confidential Information" designates information that needs to be kept secret for Japan's security as "specified secrets," and has provisions for assessing the suitability of the handler and penalties in the event of mishandling. However, its actual operation is not well suited to identifying information related to cyber security as a specified secret. In particular, in August 2020, it was reported that Defense Minister Taro Kohno expressed his desire to expand cooperation with the Five Eyes, a framework for sharing classified information among five countries,



A white robot with human-like features serves restaurant customers in Japan. Picture: Alex Knight / Unsplash, https://bit.ly/2YlfoM2

including the United States and Britain, in an interview with the *Nihon Keizai Shimbun*. However, there is concern that the lack of a system for clearance, which is a qualification for sharing classified information in the private sector, may hinder the exchange of information with other alliance countries.[29]

Clarifying the Position on Active Cyber Defensive Actions

In the United States, a law titled the "Active Cyber Defense Certainty Act" has been proposed, and in the military a doctrine called "defend forward" has been made. However, in Japan, there has been no discussion on how law enforcement agencies and others can adopt active methods against criminals to deter them from committing cyber crimes, to disrupt them, or to obtain evidence. Also, as mentioned above, legally, the provisions of the "Police Officers Duties Execution Act" do not address cyber crime; there needs to be a debate on the extent to what can be done about such active conduct.

Interpretation of the 9th Amendment and Active Defense

Article 9 of the Constitution of Japan provides for the renunciation of war. As for the question of whether or not the effects of acts for the defense of Japan may extend beyond Japan's territorial sovereignty, the government's interpretation is that if an attack is carried out against Japan, the use of tangible force against the source of the attack is permissible, but the government cannot exert its influence beyond Japan's territory. There is also a prevailing position that Japan is not able to engage in counterattacks. Until Japan clarifies its interpretation of this point, legal obstacles may arise in the event of a counterattack against the source of a cyber attack coordinated by a foreign state actor.

Status of Vulnerability Information

In Japan, the Information Security Early Warning Partnership has been established and is in operation in order to process and support vulnerability-related information based on the principle of "responsible disclosure."[30] On the other hand, the government is not believed to acquire vulnerability-related information and use it proactively for information sharing and crime deterrence. There is a significant difference in attitude between the government and industry about the need to proactively acquire vulnerability and threat information and make use of it.

Discussion of Collective Countermeasures

Generally speaking, under international law, countermeasures are to be undertaken on a country-by-country basis. However, there is a debate on whether collective countermeasures should be considered. In Japan, this issue has not yet been considered, and it may become a legal obstacle in the case of coordinated countermeasures on a global scale.

Review of the Secrecy of Communications

In Japan, the Telecommunications Business Law provides for the protection of the secrecy of communications. At present, there is a worldwide trend to allow intermediaries to play an active role in cyber security. If Internet Service Providers (ISPs) are required to play an active role to protect the security of the internet on a global scale, Japan may not be able to play an active role for the ISPs.

Prospects for International Cooperation in Critical Technologies

Prospects for cooperation in critical technologies is more limited, as Japan's domestic approach to regulating these areas is more immature.

Regarding the use of AI, regulatory frameworks have not yet reached a specific practical level, there has been no concrete effort to identify problems regarding the use of AI and to prepare a regulatory framework for resolving these problems. Technologies used more specifically beyond abstract AI are discussed in terms of, for example, the issue of the applicability of product liability laws to self-driving vehicles. The "Act on Protection of Personal Information" is being amended to strengthen data protection, but discussions on specific issues have only just begun. Moreover, specific regulations on facial recognition have not been discussed, and the issues of gender and racial bias have also not yet been discussed. Regarding robots, there is some discussion on specific issues based on the premise of self-driving vehicles, and these discussions could be used in international cooperation. However, other aspects of robotics have not yet been sufficiently discussed. There is a debate on the use of medical robots and to what extent autonomous processing should be allowed in the case of autonomous robots, but this issue has not yet been specifically discussed. Also, the relationship between medical robots and safety standards has not yet been discussed. In addition, when considering communication robots, what kind of problems may occur with the data acquired, and what kind of regulations should be imposed to address those problems, are issues that need to be addressed in the future.

Deterrence and Arms Races in Cyber Space

contributed by Kazuo Tokito.

Deterrence

Deterrence is to disincentive what the other party would have done. Closely related to the development of Cold War nuclear strategy, it can manifest itself in many forms.[31] Generally speaking, deterrence occurs when the expected cost of a failed attack exceeds the expected cost of a successful attack.

There are two main ways that deterrence works:

- **deterrence by denial**; and
- **deterrence by punishment.**

The former means a useless attack that has no effect on the opponent even if it is implemented. An example of the latter could be a counterattack by a nuclear weapon that may cause an immeasurable loss.

In order to discourage the other party from attacking and achieve deterrence, it is necessary to make the other party understand these situations in advance, which includes the component of **credibility**.

Characteristics and Problems of Deterrence in the Cyber Domain

Characteristics of the Cyber Domain

In addition to land, sea, air, and space, the cyber domain, which is said to be "the fifth area," is often divided into attack and defense as a battle area. However, the real world and the cyber domain, which is a virtual space, have somewhat different characteristics. Generally speaking, the cyber domain has five characteristics:[32]

1. **Diversity**. Individuals, organizations, and nations can take the lead in launching cyber attacks from anywhere.
2. **Anonymity**. It is easy to conceal or disguise who carried out an attack. This characteristic is a major factor regarding the effectiveness of deterrence, as the premise of deterrence by punishment is the ability to identify the attacker.
3. **Secrecy**. While some attacks, such as Distributed Denial of Service (DDoS) attacks, are easily recognized when they occur, attack methods that sneak malware deep into systems are detected when there has already been an invasion or information has been stolen. These attacks are so covert that they are not even noticed.
4. **Attacker advantage**. Advanced means of attack can be easily obtained on the black market. Because it is difficult to completely eliminate software vulnerabilities, especially if an attacker aims for the weakest part of a network system, an effective attack gives an overwhelming advantage to the attacking side.
5. **Deterrence difficulty**. In the context of attribution problems, where it is difficult to identify the source of an attack, and situations where even rapidly advancing technology can be easily utilized with enough funds, cyber attacks are extremely effective because information and communication technologies are the core of society and weapons systems, and it is easy to find situations where the expected value of the cost of a failed attack exceeds the expected value of the cost of a successful attack.

Evolutions in Cyber Deterrence Policy

Within these characteristics of cyber domains, there is a major change in how cyber deterrence has been implemented so far. For example, in the United States the concept of cyber deterrence started to be mentioned in 2009. While a concrete cyber deterrence policy was not clarified, it was stated that there was a problem of **attribution**, which is one of the characteristics of the cyber domain, where the source of an attack cannot be immediately identified. This additional problem was that even if a counterattack was carried out as a deterrent by punishment, the target for attack could not be identified. It is not possible to own complete capability for targeting in cyber space. Therefore, the most useful form of deterrence was deterrence-by-denial, in order to invalidate the effect of the attack.[33]

As a policy, the concept of active defense was introduced, in which threats and system vulnerabilities were identified in advance, and attacks were detected, analyzed, and handled concurrently in real time to reduce the damage. In order for deterrence by denial to actually work, it is necessary to make the other party aware of not only the concept but also the high defense ability of the attacked side. It is also necessary to possess high-performance equipment to defend against attacks that are carried out during peacetime.

Deterrence works by letting the other party evaluate the superiority of a wide range of coping abilities, that is, defense ability, including the operation of networks and systems. For that purpose, it is essential to collect and analyze a wide range of information on attacks and share it with other departments, and constantly update programs to close necessary vulnerabilities. Deterrence that requires such practical power is inherently different in nature from deterrence that functions by possessing a conventional nuclear weapon. The United States is also pursuing deterrence by punishment, given that the cost of achieving deterrence by denial in the cyber domain will only rise. The 2011 Department of Defense cyberspace policy report to Congress mentions deterrence by punishment in addition to deterrence,[34] and behind this lies the physics of large investments in forensics. It can further be inferred that there has been progress in attribution due to technological advances, such as methods for tracking typical sources and behavior to identify attackers.

One example of retaliation is the 2014 cyber attack on Sony Pictures Entertainment. The source of the attack was identified as North Korea, and financial sanctions were imposed on the attacking organizations and individuals. Thereafter, sanctions such as freezing assets and imposing bans on trade and travel were enforced in the US against cyber attacks from foreign countries, and deterrence by punishment was expected to be effective.

The US Department of Defense International Security Advisory Board Report identifies three core elements of deterrence: 1) deterrence by denial, 2) deterrence by threat of reprisal, and 3) deterrence by resilience.[35] The focus is being put on early recovery under the premise of attacks and damage to the system. Behind this, the US military can no longer defend against all cyber attacks, and it is also not possible to completely identify the source of all attacks, so there is a limit to deterrence. Therefore, even if a cyber attack is suffered, the deterrence-by-denial ability has evolved and improved on the premise of damage, to allow early recovery and to continue necessary procedures even if some functions are lost.

In order to implement deterrence in the cyber domain, the concept of **resilience** was introduced in addition to deterrence by denial and deterrence by punishment. In the field of information and communications, the speed of change has accelerated due to dramatic improvements in processing power and network performance.

The cyber domain is expanding dramatically due to industrial control systems and IoT, which also affects the structure of systems. With cloud migration, it is necessary to consider a zero-trust model as the situation continues to evolve. Even with the measures taken so far, the number of cyber attacks has been increasing, so it is hard to say that deterrence, in combination with these backgrounds, is functioning effectively.

In 2020 the United States' Cyber Solarium Commission reported the threat of recent cyber attacks, mentioning the formation of a code of conduct before exerting denial and disciplinary power. That is to say, action with the speed and agility is necessary to defend the country in cyberspace. We must get faster and smarter, improving the government's ability to organize concurrent, continuous, and collaborative efforts to build resilience, respond to cyber threats, and preserve military options that signal a capability and willingness to impose costs on adversaries.

It is necessary to adopt the idea of hierarchy as a concept of deterrence. This new strategic approach is layered cyber deterrence consisting of three layers:

1. **Shape behavior:** the United States must work with allies and partners to promote responsible behavior in cyberspace.
2. **Deny benefits:** the United States must deny benefits to adversaries who have long exploited cyberspace to their advantage. This approach requires securing critical networks in collaboration with the private sector to promote national resilience and increase the security of the cyber ecosystem.
3. **Impose costs:** the United States must maintain the capability, capacity, and credibility needed to retaliate against actors who target the US in and through cyberspace.

These three deterrent layers are supported by six pillars, which represent the means to implement layered cyber deterrence:[36]

1. reform the US government's structure and organization for cyberspace
2. strengthen norm and non-military tools
3. promote national resilience
4. reshape the cyber ecosystem toward greater security
5. operationalize cybersecurity collaboration with the private sector preserve and employ the military instrument of power and all other options to deter cyber attackers at any level.

In this manner, cyber deterrence policy is evolving and respond according to the situation. However, the problem of the attacker's advantage in the cyber domain still remains.

From Single Domain to All Domain

There has been some debate about conducting counterattacks in the cyber domain in the event of a cyber attack in order to exert deterrence by punishment, but there have been few cases. Even if forensic technology develops and the attack source can be identified, in reality it has become more difficult to narrow down the counterattack target in the cyber domain due to virtualization technology and decentralized technology.

Also, the attack method may not be announced because of the risk of revealing one's own capabilities. Counterattacks for deterrence by punishment are being carried out by means different from the cyber domain, such as economic sanctions, when it is possible to identify the source of the attack, as in the 2014 Sony Pictures case. This is one of the effective methods to make the cost of attacking an opponent higher than the attack itself. Cross-domain counterattacks with synergistic effects are based on the premise that the cyber domain, which is a single domain, will be dealt with more effectively, and that the strategy will be expanded to all areas at once.[37] This is a process of evolution into the "all-domain."[38]

Therefore, instead of considering the cyber attack itself as occurring within a single domain – the cyber domain – it is necessary to shift to the idea of dealing with attacks from and to all areas so that deterrence by punishment can work more effectively. For this purpose, it is necessary to add the human domain to the land, sea, air, space, and cyber/electromagnetic spectrum domains. Cognitive ability in the human domain is important against pernicious effects of misinformation like "fake news."

Regarding this, various studies on multi-domain operations have been conducted.[39] In the case of the US military, the architecture is undergoing major changes, including accelerating demonstrations

toward the practical application of Joint All-Domain Command & Control (JADC2). At this point, this trend is considered to be the most effective for deterrence against cyber attacks. Japan's Ministry of Defense is also strengthening own defense capability, and has been introduced in National Defense Program Guidelines.[40] Multi-domain defense force architecture for national defense has become vitally important to adapt to warfare that combines capabilities in new domains – space, cyberspace, and electromagnetic spectrum – and traditional domains – land, sea, and air.

Japan needs to develop a defense capability that can execute cross-domain operations that organically fuse capabilities in all domains to generate synergy and amplify the overall strength.

Further, Japan's defense capability needs to be capable of strengthening the ability of the Japan–US alliance to deter and counter threats as well as promoting multi-faceted and multi-layered security cooperation.

Applying Deterrence Theory in Practice: Two Examples

Russia's Intervention in Ukraine

The hybrid warfare in which Russia occupied and annexed the Crimean Peninsula in 2014 combined formal, non-regular, terrorist, and criminal groups, as well as jamming of military networks. Ukraine suffered great damage due to cross-domain tactics such as eavesdropping on mobile phone networks, which were used as an alternative for communications; confusion due to fake information; and accurate targeting based on GPS information. In a sense, this case exposed the vulnerability to electronic warfare.

There are a number of possible factors that could have caused a great deal of damage. One was the weak security of private communication networks used as an alternative for communications, as well as the resistance to interference of the military network. In this case, it seems that security measures were taken in the cyber domain, but they were easily invalidated by another method called jamming. Thus, a bird's-eye view is necessary.

It has therefore become even harder to make deterrence work. In securing the resilience of functions, it is necessary to build a structure that carefully considers the balance between functionality and security across domains, as well as an all-domain offensive method, not only a defensive one.

It must also be taken into consideration that the other side will also make good use of its available resources. In particular, when sharing information between the public and private sectors in the cyber domain and securing a cooperative system, special attention must be paid to ensuring security.

Building a Missile Defense System in the Japan Self-Defense Forces

The Self-Defense Forces have an integrated operation system for conducting land, sea, and air operations in an integrated manner in order to carry out missions quickly and effectively. In dealing with ballistic missiles, it has organized a Ballistic Missile Defense (BMD) joint mission unit commanded by the Commander of the Japan Air Self-Defense Force, and has a track record of carrying out joint operations mainly on land and sea under a unified system.[41]

In the future, the Ministry of Defense will work to expand the BMD integrated mission unit by improving the capabilities of the Ground Self-Defense Force equipment and strengthen the system for carrying out multi-domain operations, including new areas such as space, cyber, and electromagnetic waves. This is an evolving field in which to invest resources.[42]

By enhancing this system, the Japan Self-Defense Forces will exert an increasing number of functions in all domains; this is a valuable system to consider in future joint exercises between Japan and Australia.

An Arms Race for Cyber Deterrence

In the arms race for technologies of cyber deterrence, it is important to both develop high-performance equipment and expand core information and communication technology. In particular, in addition to manufacturing, a sense of speed and scale will be important in the future.[43] In order to realize the deterrent power to demonstrate force in all domains, the following issues should be emphasized.

Building an AI Technology Force

One feature of AI technology is that it can quickly perform complex processing using a large amount of data, and significant results have been achieved in voice, image, and language recognition. On the other hand, due to the inability to verify the process, the accumulated credibility of the results obtained by AI has not been validated, since understanding and judging human emotions cannot be reduced to zeros and ones. Regarding the deterrence of cyber attacks, complex log analysis and similar processes can be performed by AI in a short time. This is an extremely effective technology for deterrence by denial, and has produced results such as analysis, detection of vulnerabilities, and automation of countermeasures.[44]

Recently, attempts have also been made to use AI in decision-making processes.[45] Methodologies are being developed to assess the extent to which AI can be trusted for quick and effective decision-making in all-domain operations.[46] Unlike a wide range of general fields, in order for AI to function effectively in a specific security-related area, a large amount of data is required.

In addition, it is necessary to develop and operate an AI environment that correctly evaluates the results and makes necessary corrections based on feedback.[47] Additionally, since the quality of data greatly affects the reliability of AI capabilities, it is necessary to substantially improve the technology for removing fraudulent or fake data.

Enhanced Data Security

A network is essential for all-domain operations, and information sharing with various departments is also necessary. In particular, regarding cyber attacks, it is important to share information such as the means, signs, and attributes of attacks by other parties with the private sector and industry, both nationally and internationally. It is also necessary to formulate a solid security policy for information sharing between departments with different security standards and implement technology towards this goal.[48]

Furthermore, building a trust anchor system, which is the basis of security, and strengthening wide-ranging and reliable data security will enable effective implementation of all-domain operations. It could also be the road to establishing deterrence by punishment in the cyber domain.

Human Resource Development

Human resource development is important, and the Ministry of Defense is currently investing in securing human resources by training highly technical personnel and promoting projects towards this objective.[49] Studies have also shown that training human resources who are good at cyber security reduces cyber attacks, resulting in deterrence by denial.

Cyber education is necessary in order to improve early recovery from cyber attacks, including the ability to deter by resilience – that is, being able to carry out missions even with limited functions. It is also necessary to train human resources with practical skills in the operational field to respond according to their original duties in all-domain operations, even under attack. Having a clear set of priorities and force reconstruction skills to minimize the effects of cyber attacks is also desired.

Development of a Decision-making System for All-domain Operations

The US Department of Defense is developing the Joint All-Domain Command & Control concept – the concept of a single network system that can connect the sensors from all military services and equipment of the air force, army, marine corps, navy, and space force.

The US Air Force is one step ahead in development by linking with the Advanced Battle Management System (ABMS).[50] This development uses field information to promptly give feedback for decision-making. The addition of countries closely allied to the United States in the system will be considered in the near future. It is necessary to continue discussions regarding effective technologies within the Five Eyes alliance and with other countries.

Building an Architecture Adapted to Mosaic Strategy

According to the mosaic strategy, there is a need to develop multiple overlapping systems that can be quickly reconfigured and deployed in a variety of different combinations, rather than relying on centralized systems that could become a single point of failure.[51] New technology and equipment should be quickly deployed. This concept emerged from the background of not only improving the performance, but also on how to utilize technological advancement to quickly demonstrate force.

For that purpose, it is necessary to introduce an architecture to flexibly use equipment as a military IoT, develop enablers to enhance the capabilities of that equipment, and combine it with decision tools.

Application of Next-generation Cryptography

Quantum technology is also evolving steadily, and the security of currently used cryptography will be jeopardized when quantum computing enters practical use. Accordingly, quantum cryptography as a new cryptographic technology is already being realized.[52]

By combining key exchange and physical encryption using quantum technology, there is a great advantage in using this technology from the start, especially in domains where it is difficult to update equipment such as in space. In the future, there will be increasing interest in system construction using many lightweight satellites in low Earth orbit, such as “Megaconstellation,” and networks will become essential in space as well. Regarding cryptography, it is necessary to consider not only the introduction of new technologies but also how to operate them.

Other Technologies

Various technologies, such as drones and robots, are beginning to find practical uses, and the domain of space is also about to evolve significantly with the introduction of new sensors and networks, and development of new attack vectors.[53] It is necessary to pay close attention to how to incorporate them into all-domain operations.

Trends of Japan–Australia Cyber Cooperation

The Japan–Australia Cyber Policy Conference was established at the Japan–Australia Summit held in Tokyo in April 2014.[54] Four meetings have been held since then. Both countries are continuing to enhance cooperation and information sharing to deal with malicious cyber activities. Additionally, these actions lead to deterrence, and can help foster reliability and ensure stable

operation of the cyber region in the Indo-Pacific region. Implementation will be carried out whenever possible to strengthen the Quad structure of Japan, the United States, Australia, and India, building equipment backed by technology and exercises, which will be reflected not only in the system but also in the execution ability, while improving human and organizational response capabilities. Further efforts are needed toward this end, such as building a command and control system.

For deterrence to work effectively, it is essential to fight in all domains. This field is still under development, so it is necessary to closely monitor the trends, increase trust between Japan and Australia, and continue to share information, while considering how to cooperate with the United States.

Australian, Indian, Japanese and American maritime forces routinely operate together in the Indo-Pacific, fostering a cooperative approach toward regional security and stability. Picture: Markus Castaneda / US Navy, https://bit.ly/2Mej3bU

Chinese Cyber Warfare and Japan's Response

contributed by Takahiro Sasaki.

Chinese Cyber Attacks against Japan[55]

Cyber attacks on Japan have increased dramatically since the 2000s, and China is suspected to have been involved in many of these. It is difficult to determine the source of a cyber attack because the attack does not leave a trace, or may intentionally leave a trace to appear to be the work of another country. This section focuses on cases in which China clearly stated that it was the source of the attack, and cases in which China's involvement was extremely doubtful because there were certain signs of such involvement.

- **Cyber attacks on Japanese government websites in February 2005**

  On February 24, 2005, the Chinese hacker group "China Iron and Blood Federation" declared that from 8 p.m. to 10 p.m. on February 23 they had attacked the "Little Japan website" (China uses this term when it looks down on Japan). The group said that, in protest against the Japanese government's claim to the Senkaku and Uotsurijima islands in the East China Sea, they had targeted the websites of the Japanese government and the SDF.

- **DDoS attack on Japanese government websites by "Honker Union of China" in September 2010**

  Referring to the Senkaku Islands issue, the "Honker Union" attacked Japanese government agencies and other websites for two weeks until September 18. This was the day of the Lake Liutiaohu Incident 89 years ago, which triggered the Manchurian Incident. The National Police Agency website was inaccessible for three hours.[56]

- **9/18 Major Japanese Website Attack in September 2011[57]**

  On the anniversary of the Lake Liutiaohu Incident, the 9/18 Major Japanese Website Attack, in which the Chinese hacker organization "Admin8.us" played a leading role, started. The hackers' website listed the National Police Agency, Okinawa Prefectural Construction Technology Center and MDRT Japan Association Secretariat as targets. As many as 19 hacker organizations supported the anti-Japan campaign, including the "China Red Customer Federation."

- **Cyber attacks on Mitsubishi Heavy Industries (defense industry) in September 2011**

  At least 80 servers and personal computers at a plant that produces state-of-the-art submarines, missiles, and nuclear power plants were infected with the virus. The company reported to the police that there was a high probability that the purpose of the targeted attack was spying. This was the first time that a cyber attack targeting Japan's defense industry had been revealed. According to sources, eight shipyards, including Kobe Shipyard & Machinery Works, Nagasaki Shipyard & Machinery Works, and Nagoya Guidance & Propulsion Systems Works, and the head office of the company, were infected with malware. In this case, there was evidence that the attacker used simplified Chinese characters, which are used in China, and it seems that China was involved as a state, or at least a person who was familiar with Chinese was involved.

- **Pension data breach by Chinese Cyber Unit in May 2015**

  The Japan Pension Service discovered the problem on May 8, 2015, when it asked a computer antivirus software company to analyze a problem. On May 19, the Metropolitan Police Department was asked to investigate. The media reported that as a result of analyzing the emails and communications used in this case, some physical evidence was found to point to China. An official in the Prime Minister's Office said, "Cyber attacks have frequently occurred, and information has been obtained from foreign intelligence agencies that have compiled databases of the data and communications used." The investigation found that the hackers were concentrated in a number of cities, including Shanghai, China. The group is considered to be effectively operated by Cyber Attack Unit 61398 of the People's Liberation Army.[58]

- **Suspected data breach concerning research on a high-speed gliding missile in a large-scale attack on Mitsubishi Electric in January 2020**

  Mitsubishi Electric suspects that information on the performance of a high-speed gliding missile it is studying for the MoD was exposed after a massive cyber attack on the company in January 2020. The company initially said that personal and internal information may have been compromised, but that sensitive information was not. However, on February 10, the company changed its explanation, saying that the data breach "included the Defense Ministry's 'restricted information'." It is unusual to reveal information about specific equipment targeted by a cyber attack on the Defense Ministry or the defense industry.[59]

- **Suspected data breach concerning SDF equipment in a cyber attack on NEC in January 2020**

  The cyber attack on Japanese multinational information technology and electronics company NEC in January 2020 was most likely the work of hacker group APT 10, which the US Justice Department believes is linked to the Chinese government. According to government officials and experts, APT 10 was identified by a package of malware, network exploits, and communications records sent to NEC. APT 10 is one of a group of high-profile, persistent threats identified by cyber security firm FireEye, which is under the direction and support of state organizations and known for stealing data from a wide range of foreign governments and private companies, raising the possibility that critical data on Japan's civilian and defense sectors could have been stolen in the attack.[60]

Trends in Chinese Cyber Attacks

In the early stages of China's cyber attacks on Japan, the main focus was on the defacement of websites of government agencies for political purposes. The subsequent proliferation of countermeasures against website tampering has led to an increase in DDoS attacks.

No large-scale cyber attacks against Japan by China were confirmed until 2015, but the number has been increasing since the breach of pension information in the same year was confirmed. In recent years, it has been confirmed that APT 10 is working to exploit defense information and advanced technology information.

In addition, it is likely that China will step up its influence operations. This has been demonstrated in public opinion campaigns using the new coronavirus pandemic. In response to the outpouring of criticism against China's handling of the outbreak, China wants to now position itself as the world's savior for its efforts to suppress the virus.

Regarding methods, one of the characteristics of cyber attacks against Japan by China is the frequency of insider attacks by Chinese employees. This is due to the large influx of Chinese workers and foreign students into Japan as a result of recent globalization. These categories of people cannot be assumed at first glance to be spies, but it should be noted that they constitute insider threats.

Future Trajectory of Cyber Warfare by China

Cyber Defense Using AI

Conventional cyber security technology cannot cope with unknown threats. Recently, however, in order to detect unknown malware, a technique to deeply analyze the behavior and attributes of malware using machine learning has been developed. By collecting information on transactions on the dark web and analyzing it using techniques such as machine learning and natural language processing, it is possible to grasp future attack techniques in advance.

At present, AI is used as a technology to understand the trends of criminals in cyber space. AI monitors large amounts of communication traffic in real time using deep learning, accumulates and analyzes data common to cyber attacks and information such as the source and number of connections, and detects abnormalities in the data to predict new threats and take quick countermeasures.

Analysis by AI using deep learning involves extracting a large number of features to be tracked in the data, and to obtain knowledge on malware from the analysis. For example, when analyzing malware, AI determines feature quantities from file sizes, file header information, character strings, etc., and learns about 500 million pieces of malware to perform highly accurate detection. It also reduces the lag between creating malware signatures and creating effective countermeasures to achieve high detection rates.

In the future, cyber defense using AI will form an intelligent platform that can detect and defend against sophisticated cyber attacks, and automatically monitor information related to cyber attacks from vast amounts of open data. In addition, high-precision attack monitoring, which detects, classifies, predicts, and visualizes abnormalities, will advance, and autonomous learning functions, such as additional learning, online feature extraction, automatic data collection, and automatic labeling, will advance and enhance defense capabilities.

Advantages of machine learning include the ability to acquire knowledge from large amounts of high-dimensional observation data, and the ability to detect, classify, and predict anomalies in response to attacks by additional learning of observation data. Of course, AI can run 24/7, 365 days a year, and anything that can be determined by machine learning can be automated, reducing the burden on administrators.[61]

Attacks Using AI

Regarding cyber attacks, advances in AI and machine learning are expected to promote the automation of tasks that previously had to be done manually. As a result, more attacks could be automated, such as the creation and sending of effective phishing emails. While spear-phishing attacks require attackers to be given detailed information about which companies and organizations are vulnerable to deception when identifying a target, AI systems can collect, organize, and process large databases to link identification information, give attackers more detailed information, and make attacks more rapid and accurate. AI can also help pinpoint and identify targets. Multiple sources can identify people who are particularly vulnerable to attack.

AI can also use machine learning to disrupt spam filters in an enterprise. Machine learning algorithms are used to mimic the behavior of users in the network to avoid detection of abnormal behavior. There is still no good way to know how an attacker will break into a corporate network and attack, so it is difficult to find early warning signs.

In addition, AI can make existing forms of cyber attack such as identity theft, DDoS attack, and password cracking more powerful and efficient, make complex attacks faster and more effective than human hackers, and help human cyber criminals customize their attacks.

In particular, in China, it is expected that it will become more important to use AI in cyber space for offensive than for defense.[62]

Attacks Against AI

One of the characteristics of AI itself is that it is easily fooled. Malicious people can use the wrong learning data, or cyber attacks can distort decisions and actions by using certain input patterns that can fool AI. One issue for the safety of AI is to remove in-

ternal and external factors that can cause AI to malfunction, but research in this area has not progressed yet. In China, this may be a challenge to using AI in cyber warfare.

As a result, the future of AI in cyber space is likely to be AI on the attacking side versus AI on the defending side – in other words, warfare without human intervention.[63]

Using AI for Influence Operations

China and Russia are working to manipulate information in order to affect the psychological aspects of the public, with a focus on weakening the state institutions of their opponents. Technological advances in AI have the potential to further the influence maneuvers of China and Russia using disinformation.

Regarding the exercise of influence operations, such as election interference, machine learning can be used to collect, analyze, and microtarget all available data, including race, ethnicity, ideology, demographics, and geographic conditions. In coming years, these countries may be able to engage in influence operations autonomously without human involvement.

In order to spread information, synthetic accounts created by AI and accounts stolen by cyber attacks are used, and thus false or misleading information can spread rapidly.

Japan's Response

Japan's Cyber Security Strategy – Insufficient for National Security

In 2018, the government enacted the Cybersecurity Strategy based on the Basic Act on Cybersecurity. Part of Chapter 4 of this Cybersecurity Strategy describes the "Field of fighting in cyberspace." Section 2 of Chapter 4, "Measures to achieve the objectives," proposes, as concrete measures "to protect citizens and society," the following: (1) to build preventive measures against threats (active cyber defense); and (2) to take measures against cyber crime. The term "active cyber defense" here means "active defense" in Europe and America, which means analyzing the actions of attackers and taking measures in advance. It does not mean aggressive activity in cyber space.

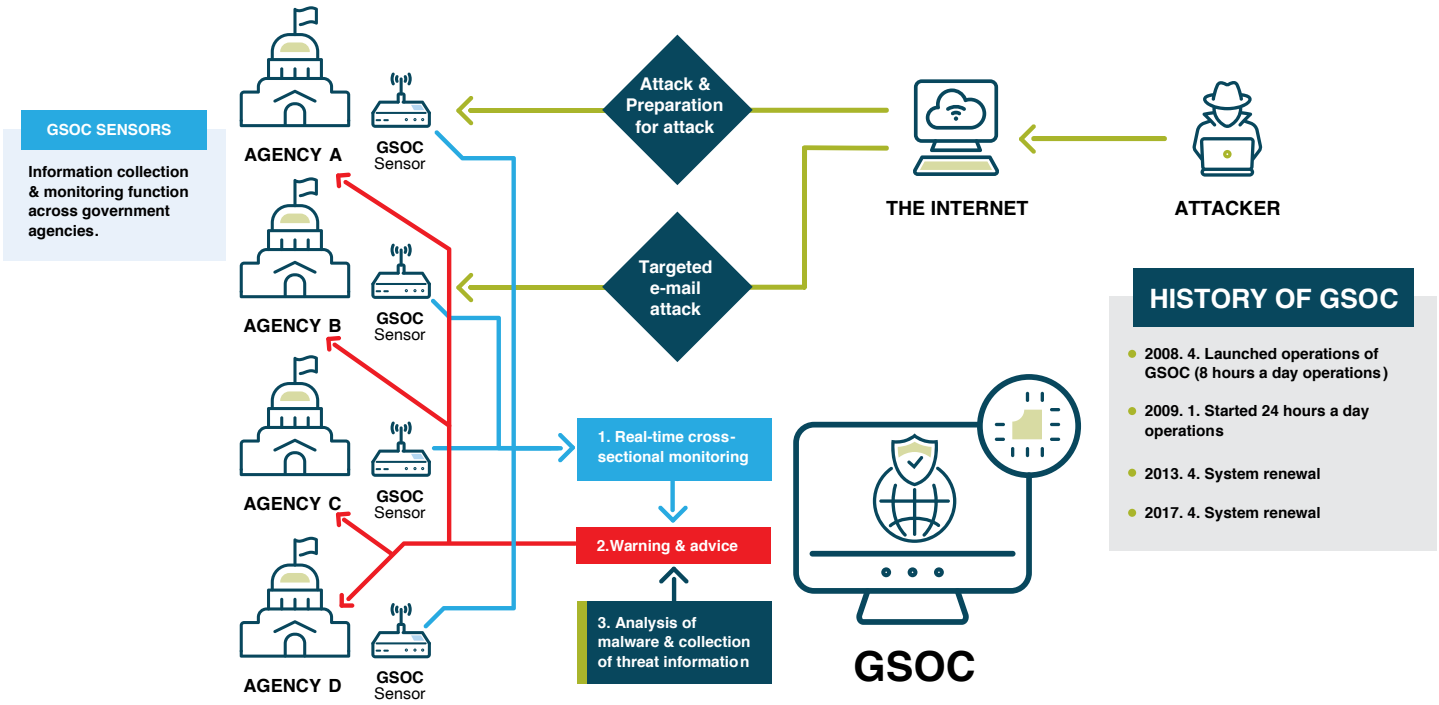


Figure 1: Framework for cyber security coordination in government agencies

In cyber warfare, it is overwhelmingly disadvantageous to use "exclusively defensive defense" where a preemptive attack operation is impossible. If the government fails to solve this problem, it will be a failure as a national security strategy.

Section 2 of Chapter 4 also mentions specific measures for "Strengthening the response system to large-scale cyber attacks," and recommends that the government "Strengthen the preparedness to deal with large-scale cyber-attack situations, etc. in order to undertake crisis management in both cyber space and real space." This, too, does not go beyond crisis management in the event of an attack, and is insufficient as a strategy to realize the key point of the National Defense Program Guidelines to "secure superiority in cyber space."[64]

MoD/SDF Guidelines for Responding to Cyber Attacks

In 2012, six years before the Cybersecurity Strategy was enacted, the MoD and the SDF released a document entitled "Toward the Stable and Effective Use of Cyberspace by the Ministry of Defense and the Self-Defense Forces," which provided guidelines for the MoD and the SDF when responding to cyber attacks.[65]

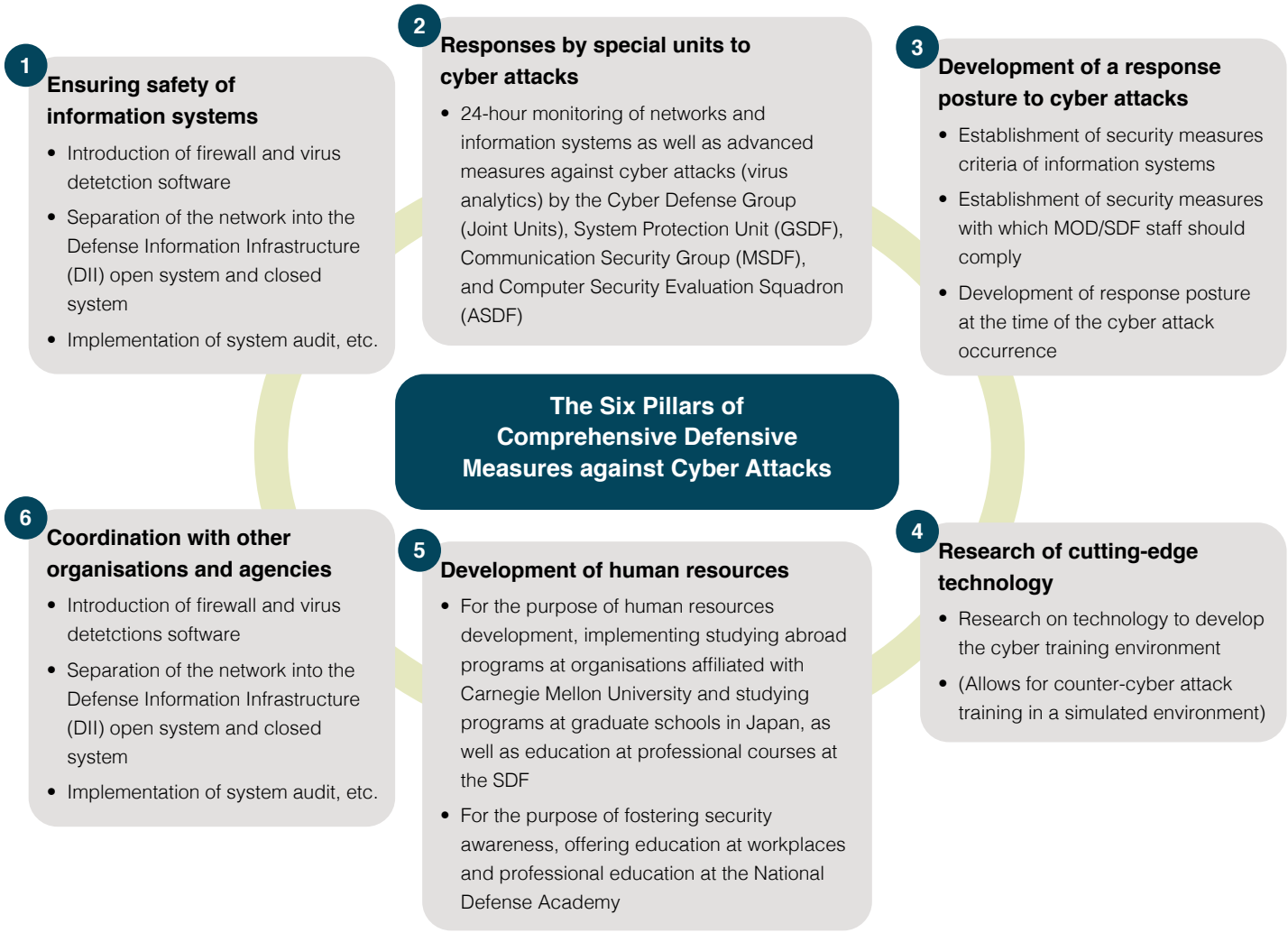


Figure 2: MoD/SDF Comprehensive Measures to Deal with Cyber Attacks[70]

There are three key points in this document:

1. It mentions cyber space for the first time not only as infrastructure but also as a fifth domain in which warfare will take place.

2. It explicitly notes "the possibility of the need to deny an opponent the use of cyberspace in order for the SDF to effectively dispel an armed attack against Japan," and reserves the right to conduct cyber operations. These concepts and expressions are also used in the revised National Defense Program Outline.

3. In this document, the MoD mentioned for the first time the legal status of cyber attacks. It states for the first time that if a cyber attack is carried out as part of an armed attack, it is appropriate to treat it as if it were a physical attack. Therefore, it can be "assumed that the first requirement of exercising the right of self-defense will be met in the event of a cyber attack as part of an armed attack."

These three points have been mentioned in US cyber strategy since 2012, and were epoch-making guidelines in that they were enacted at the same time. However, unclear points such as "What are the specific ways to prevent other countries from weaponizing cyber space?", "Which organizations are responsible for it?", "When is a cyber attack part of an armed attack?", and "Who will determine this?" have not been resolved even after the revision of the National Defense Program Guidelines in 2018.

Japan's Cyber Security Framework

Figure 1 shows Japan's national cyber security framework.[66] As can be seen, there is a Government Security Operation Coordination (GSOC) team that monitors cyber threats from government agencies and incorporated administrative agencies. In the event of a cyber attack, the response is entrusted to the Computer Security Incident Response Team (CSIRT) of each organization. When the response capability of each organization is exceeded, an organization called CYMAT (Information Security Emergency Support Team) is established and supported.

This framework is expected to play a role at the cyber security (safety and maintenance) level. However, this framework is unlikely to be able to effectively deal with the challenge of "battle." The problem is that there is no agency for overall cyber security, including national security.[67]

According to Hiroshi Ito, former deputy director-general of the Ministry of Economy, Trade and Industry, the challenges of cyber warfare in Japan are as follows:

- The national agencies in charge of cyber security include the Ministry of Internal Affairs and Communications (information and communications technology), the Ministry of Economy, Trade and Industry (jurisdiction over critical infrastructure), and the National Police Agency (jurisdiction over cyber terrorism in cyber crime, critical infrastructure, etc.). However, there is no agency in charge of overall cyber security, including national security.

- Japan's Basic Law on Cybersecurity was enacted in 2014. Article 19 describes responses to national security and states that "The State shall take necessary measures to strengthen mutual coordination among relevant organizations and clarify the sharing of roles with regard to measures for matters that may have a serious impact on the safety of Japan." Six years have passed since 2014, but "measures necessary to strengthen cooperation among relevant organizations and to clarify the division of roles" have not been taken yet.

In other words, there is no agency in charge of cyber security, including national security. This is a challenge for cyber security, including Japan's national security.

Cyber Attack Response Framework for Defense

At present, the Cyber Defense Group exists under the command of the Self-Defense Forces C4 Systems Command, which is a joint unit of the Ground, Maritime, and Air Self-Defense Forces.[68] However, this Cyber Defense Group is basically just for defense against cyber attacks; it does not have an offensive capability, which is essential for fighting. However, it could possess the basic capability of attacking as a training/exercise function and a research function. Figure 2 shows the current response framework to cyber attacks at the Ministry of Defense.[69]

By the end of 2023, the SDF will review its framework and establish a new Cyber Defense Group under the direct control of the Minister of Defense. This new group will retain functions to prevent the use of cyber space by other countries in an emergency, as well as functions to protect against cyber attacks. That means not only cyber-defense but also cyber-attack capabilities. This is considered to be a major step in the history of cyber warfare in Japan.

It would appear that concrete measures have been taken only after items related to cyber attack were specified in the Cyber Attack Handling Guidelines in 2012. However, even at this stage, the guidelines for how to fight cyber warfare are not clear, and specific measures concerning the extent to which the Ministry of Defense is responsible for cyber warfare, which affects the entire nation, and how to introduce capacity-building and equipment for that purpose, are not clear.

Recommendations for Quad Cooperation

As mentioned above, it is difficult for only one country to counter the increasing threat of China (and also the threat of Russia cooperating in many security areas) in recent years. Accordingly, security cooperation between Japan, the United States, Australia, and India (the so-called Quad relationship) is vital. Because these four countries have different levels of security relations, it is difficult to say what kind of cooperative relations they should pursue as a whole. However, in order to compete with China and Russia in cyber space, it will be necessary to deepen cooperation, at least in the following areas:

1. **Sharing cyber threat intelligence:** In terms of sharing threat intelligence, since the United States and Australia belong to the Five Eyes intelligence community, and Japan and India are outside this category, it may be difficult to establish a cooperative relationship. However, a new framework for effective information sharing should be established, and intelligence on cyber threats from China and Russia should be shared among the four countries to counter such threats.
2. **Fact-checking monitoring system:**[71] As mentioned above, influence maneuvering using cyber space has become an issue in recent years. In order to counter this threat, we believe that a fact-checking system should be established with the cooperation of the four countries.
3. **Research on using AI:** It is estimated that AI will be used in cyber space in the future. It will be necessary to promote research and studies in the four countries in this field to enhance their interoperability capabilities and to raise the level of the four countries as a whole. Both China and Russia are using AI to seek hegemony in cyber space.
4. **Joint exercises are conducted in each of the four countries**, but each country has its own strengths and weaknesses. It is also important to conduct joint exercises in order to learn the strengths of other potential allies and partners and to dramatically improve their resilience. Joint exercises that demonstrated the depth of our alliance would help deter China and Russia.
5. **Cooperation in human resource education:** The four countries should contribute to building the foundation for implementing the above four items by dispatching human resources to each other and cooperating in education.

It is necessary to promote the above items in the four countries or in two or three countries at the initial stage.

Conclusion

contributed by Kohei Takahashi.

In previous sections, each of our team members discussed their theme based on their expertise and experiences and gave some suggestions. In this section, we offer more specific suggestions to develop Australia's forthcoming International Cyber and Critical Technology Engagement Strategy, as well as the Quad Tech Network (QTN).

Suggestions on the QTN

Like-minded states such as Australia, India, Japan and the United States should cooperate and coordinate multilateral responses against the gray-zone tactics that have been discussed. The QTN has the potential to provide a platform where experts from academia and think tanks can discuss such issues. Through its cyber and critical technology diplomacy, Australia should aim to build this platform – at both the Track 2 and formal diplomatic levels. In fact, the four major democratic states should attempt to develop an international framework that is the Quadrilateral, or "the Quad," to enable dialogue among the states on issues of regional security. Although the Quad's dialogue would be at the minister- and working-level, we can learn something to build an expert forum.

The antecedent Quad is the Tsunami Core Group from 2004–2005, in which officials from the four countries coordinated the effective multilateral response to the 2004 tsunami in the Indian Ocean.[72] According to Grossman, this core group was "an ad hoc coalition that ignored traditional groupings.[73] We pulled these specific countries together simply because they were the ones with the resources and the desire to act effectively and quickly." The efficacy of the response among the four countries may lead to further cooperation. Japan's Prime Minister Shinzo Abe initiated the idea of a quadrilateral. Abe visited India in 2007 and then gave a speech titled "Confluence of the Two Seas" in the Parliament of the Republic of India. Abe said that:

> "the Pacific and the Indian Oceans are now bringing about a dynamic coupling as seas of freedom and of prosperity. A 'broader Asia' that broke away geographical boundaries is now beginning to take on a distinct form. Our two countries have the ability – and the responsibility – to ensure that it broadens yet further and to nurture and enrich these seas to become seas of clearest transparence."[74]

Abe highlighted a "values-based diplomacy" approach to foreign affairs that embraces an "arc of freedom and prosperity." This central idea was in line with the tenets of the US foreign policy at that time (during the George W. Bush administration). Consequently, there was a working-level meeting and a maritime exercise in 2007. However, the Quad was not active because of China's negative reaction.

Due to the rise of China in this region, the Quad was revived. Since 2017, the four states have set up discussions at the working and ministerial levels. On October 6, 2020, Japan hosted the second ministerial of the Quad, attended by Australian Foreign Minister Marise Payne, Indian External Affairs Minister S. Jaishankar, Japanese Foreign Minister Toshimitsu Motegi, and the US Secretary of State Michael Pompeo in Tokyo.[75] These four major Indo-Pacific democracies attempted to step up coordination for a free and open Indo-Pacific, and to make the Quad function as a bulwark against China's emerging regional influence. Before the meeting, Pompeo mentioned China, saying: "it is more critical now than ever that we collaborate to protect our people and partnerships from the Chinese Communist Party's exploitation, corruption and coercion."[76] All other countries avoided mentioning China directly.

Learning lessons from the Quad, we would like to provide suggestions for establishing the network as follows:

1. identify what the QTN can do and specify what Australia would like to do
2. identify what each member state can contribute to the QTN
3. identify common interests among the members
4. identify the principles and values of the QTN
5. identify stakeholders.

One of the criticisms of the Quad is that it lacks purpose.[77] In order to establish the forum, the purpose and scope of the QTN should be defined by seeking common interests among the members. At the same time, each of the participants should clarify what they can contribute to the network. These principles are imperative to ensuring sustained activity on the platform. The principle of transparency and freedom of expression should be fundamental. In particular, it is better to maintain the principle of transparency if the Quad attempts to avoid being symbolized as an anti-China clique.[78] After identifying the above, we can clarify stakeholders such as universities, think tanks, startups, accelerators, investors, large corporations, and public sectors.

Suggestions on Critical Technology

The first section of this paper compared compared the critical technology between NATO and Japan in the defense field and discussed how the term "criticality" relies heavily on context. Critical technology carries a certain amount of ambiguity. How can we identify critical technology? For whom is the technology critical? Even if we identify what technology is critical, the question of what to do with it remains unclear. We should clarify these questions to identify critical technologies.

Most lists of critical technology place too much emphasis on originality (invention). Rather, successful application of critical technologies will be more beneficial to society. The cost-effective production process will be the key to diffusing technology in markets.

Nelson defines innovation as "the processes by which firms master and get into practice product designs and manufacturing processes that are new to them, whether or not they are new to the universe, or even to the nation."[79] The conventional critical technology paradigm is characterized by less consideration of innovation: "the critical technologies paradigm behind the making of critical technologies lists fails to address the circumstances and processes necessary for a technology to be incorporated in a successful innovation."[80] Policymakers should note that examining the process used to diffuse the technologies is essential to making policies on critical technology.

Startups play a significant role in diffusing critical technologies that catalyze disruptive innovation. On the other hand, established corporations pay significant attention to technologies that aim to sustain innovation. Shane points out the reason: "they [large corporations] focus their activities on enhancing the returns from their existing operations, and early stage technology that is not yet commercially useful does not do this."[81] In the same vein, Christensen argues:[82]

> Within a value network, each firm's competitive strategy, and particularly its past choices of markets, determines its perceptions of the economic value of a new technology. These perceptions, in turn, shape the rewards different firms expect to obtain through pursuit of sustaining and disruptive innovations. In established firms, expected rewards, in their turn, drive the allocation of resources toward sustaining innovations and away from disruptive ones. This pattern of resource allocation accounts for established firm's consistent leadership in the former and their dismal performance in the latter.

Export controls rationalized by national security are used to pursue industrial policy goals. Taking up the case of confrontation between China and Japan on rare earth, Marukawa discusses that Japan rationalized its restriction on direct investments due to security concerns.[83] However, the restriction had a negative impact on Japanese manufacturers' competitive abilities. Accordingly, the Japanese government had to relax its restrictions. Marukawa concludes that export restrictions do not contribute to achieving industrial policy goals.[84] Branscomb also points out the dangers of coupling promotion with protection: "such lists [of critical technologies] might become instruments of trade protection as well as a guide for domestic technology promotion, causing inevitable conflicts."[85]

This discussion points to the importance for policymakers to consider how to:

1. Base policy on innovation rather than invention
2. Place more focus on startups than on large companies
3. Avoid coupling promotion with protection.

Endnotes

1. The White House. (2020, 22 September) “Remarks by President Trump to the 75th Session of the United Nations General Assembly.” https://www.whitehouse.gov/briefings-statements/remarks-president-trump-75th-session-united-nations-general-assembly/
2. UN Audiovisual Library. (2020) Chinese President Xi Jinping Speech. https://www.unmultimedia.org/avlibrary/asset/2560/2560743/
3. Rahman, M. (2020, July 17) “COVID-19 and Future of Cyber Conflict.” *The Diplomat.* https://thediplomat.com/2020/07/covid-19-and-future-of-cyber-conflict/
4. United States Special Operations Command. (2015, September 9) “White Paper – The Gray Zone.” https://info.publicintelligence.net/USSOCOM-GrayZones.pdf
5. Ang, K. (2020, June 15) “Malcolm Turnbull argues Australia can withstand China’s Pressure.” *NIKKEI Asia.* https://asia.nikkei.com/Editor-s-Picks/Interview/Malcolm-Turnbull-argues-Australia-can-withstand-China-s-pressure
6. Gaouette, N. (2020, June 16) “Pentagon warns China is exploiting the coronavirus pandemic to wage ‘economic warfare’ on the US.*” CNN politics*. https://edition.cnn.com/2020/06/16/politics/pentagon-china-economic-warfare/index.html
7. Oliveri, N. (2020, June 19) “‘Sophisticated state-based’ cyber attack hits Australian government, business in major breach.” *9NEWS*. https://www.9news.com.au/national/cyber-attack-australia-scott-morrison-government-private-sector-breach-of-security/e621ae47-f810-4fa7-9c11-3caa3b09f4dc
8. Chandrashekhar, A. & Agarwal, S. (2020, July 15) “India facing more cyber attacks from China and Pakistan since nationwide lockdown.” *The Economic Times. https://economictimes.indiatimes.com/tech/internet/india-facing-more-cyber-attacks-from-china-and-pakistan-since-nationwide-lockdown/article*show/76962155.cms?from=mdr
9. Acquisition, Technology & Logistics Agency. (n.d.). 防衛装備庁の概要. https://www.mod.go.jp/atla/soubichou_gaiyou.html North Atlantic Treaty Organization Science and Technology Organization (NATO STO). (n.d.). “About the STO.” https://www.sto.nato.int/Pages/organization.aspx
10. Reding, D.F. & Eaton, J. (2020). *Science Technology Trends 2020–2040: Exploring the S&T Edge*. NATO Science & Technology Organization. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf
11. References to critical technologies in the US are found in the *National Defense Strategy*, published in 2018, which mentions the following eight critical technologies: 1) advanced computing, 2) big data analytics, 3) artificial intelligence, 4) autonomy, 5) robotics, 6) directed energy, 7) hypersonics, 8) biotechnology. Accessed via US Department of Defense. (2018). *National Defense Strategy of the United States of America.*
12. Reding & Eaton, *Science Technology Trends 2020–2040.*
13. Japan Ministry of Defense. (2019). *R&D Vision: Toward Realization of Multi-Domain Defense Force and Beyond*. https://www.mod.go.jp/atla/en/policy/pdf/rd_vision_full.pdf
14. Ibid.
15. Ibid.
16. Ibid.
17. Ibid.
18. Nikkei BP (2019). “100 Technologies which Changed World [Japanese].” Nikkei BP.
19. Interview with Dr. Akaike Shinichi of NISTEP on July 2, 2020.
20. These strategies are as follows: e-Japan Strategy (2001), e-Japan Strategy II (2003), World’s Most Advanced IT Nation Declaration (2013), and World’s Most Advanced IT Nation Declaration (Prime Minister’s Office of Japan. (2017). Declaration to Be the World’s Most Advanced IT Nation Basic Plan for the Advancement of Public and Private Sector Data Utilization. http://japan.kantei.go.jp/policy/it/2017/20170530_full.pdf) / Public–Private Data Utilization Promotion Basic Plan (2017–2018).
21. Japanese Law Translation. The Basic Act on Cybersecurity (Tentative translation) (2014). Japan. http://www.japaneselawtranslation.go.jp/law/detail/?id=3591&vm=04&re=01
22. Japanese Law Translation. Basic Act on the Advancement of Public and Private Sector Data Utilization, Pub. L. No. 103 (2016). Japan.
23. BBC. (2011, September 20). “Japan defence firm Mitsubishi Heavy in cyber attack.”
24. Otake, T. (2015, January 1). “1.25 million affected by Japan Pension Service hack.” *The Japan Times.*
25. Akimoto, D. (2020). “Cybersecurity and Japan’s Right to Self-Defense.” *Institute for Security & Development Policy.* https://isdp.se/cybersecurity-japans-right-to-self-defense/
26. Japanese Law Translation. The Police Duties Execution Act, Pub. L. No. 136 (1948). Japan.
27. Ministry of Foreign Affairs of Japan. (2017) “The U.S. Statement on North Korea’s Cyberattacks.” Statement by Press Secretary Norio Maruyama. https://www.mofa.go.jp/press/release/press4e_001850.html
28. Specifically, the 10 requirements for the safety of self-driving vehicles are as follows: 1) establishment of operation design domain (ODD); 2) safety of self-driving systems; 3) compliance with safety standards, etc.; 4) human-machine interface (installation of driver status monitoring function, etc.); 5) installation of data-recording device; 6) cyber security; 7) safety of the vehicle for unmanned automated mobile services (additional requirements); 8) safety assessment; 9) ensuring safety during use; and 10) provision of information to users of self-driving vehicles.

29. Glosserman, B. (2020, August 24). “From ‘Five Eyes’ to six — a good idea, but not the best. *“The Japan Times.*

30. Information Technology Promotion Agency. (2017). “Information Security Early Warning Partnership – Overview of Vulnerability Handling Process.” https://www.ipa.go.jp/files/000044732.pdf

31. Kawaguchi, T. (2015). “Renewing Cyber-Deterrence Policy in the US ‘Attribution’ and ‘Resilience’.” *KEIO SFC JOURNAL, **15***(2), 78–95.

32. Japan Ministry of Defense. (2012). “For stable and effective cyberspace usage in MoD and Selef Defense Forces” (防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて). https://www.mod.go.jp/j/approach/defense/cyber/riyou/index.html

33. Lynn III, W.J. (2010). “Defending a New Domain: The Pentagon’s Cyberstrategy.” *Foreign Affairs,* 89(5), 98–108.

34. Department of Defense. (2011). *Department of Defense Strategy for Operating in Cyberspace.* https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

35. International Security Advisory Board. (2014). “International Security Advisory Board Report on A Framework for International Cyber Stability.” https://2009-2017.state.gov/documents/organization/229235.pdf

36. U.S. Cyberspace Solarium Commission. (2020). “Final Report.” https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

37. Japan Ministry of Defense. (2018). *Medium Term Defense Program (FY2019 – FY2023).*

38. Congressional Research Service. (2020). *Joint All-Domain Command and Control (JADC2).* https://crsreports.congress.gov/product/pdf/IF/IF11493

39. Nisperos, E. (2020). “Joint All Domain Effects Convergence: Evolving C2 Teams.” *Over The Horizon.* https://othjournal.com/2020/03/10/joint-all-domain-effects-convergence-evolving-c2-teams/

40. Japan Ministry of Defense (2018). *National Defense Program Guidelines for FY2019 and beyond.*

41. Japan Ministry of Defense. (2018). *Defense of Japan 2018.*

42. Japan Ministry of Defense, *Medium Term Defense Program (FY2019 – FY2023).*

43. *Air Force Magazine.* (2020, October 28). “Giving Airmen the Edge: The Promise of JADC2.” https://www.airforcemag.com/giving-airmen-the-edge-the-promise-of-jadc2/

44. Data Flair (n.d.). “Impact of Artificial Intelligence in Cyber Security.” https://data-flair.training/blogs/ai-and-cyber-security/

45. Voke, M.R. (2019). *Artificial Intelligence for Command and Control of the Air Power.* Wright Flyer Papers. Department of Research and Publications, Air Command and Staff College. https://media.defense.gov/2019/Nov/27/2002218265/-1/-1/0/WF_72_VOKE_ ARTIFICIAL_INTELLIGENCE_FOR_COMMAND_AND_CONTROL_OF_AIR_POWER.PDF

46. Lingel, S., Hagen, J., Hastings, E., Lee, M., Sargent, M., Walsh, M., Zhang, L.A. & Blancett, D. (2020). *Joint All-Domain Command and Control for Modern Warfare: An Analytic Framework for Identifying and Developing Artificial Intelligence Applications.* Rand Corporation. https://www.rand.org/pubs/research_reports/RR4408z1.html

47. Columbus, L. (2020, July 9). “10 Ways AI is Improving New Product Development.” *Forbes.* https://www.forbes.com/sites/louiscolumbus/2020/07/09/10-ways-ai-is-improving-new-product-development/?sh=73b822bb5d3c

48. Freedberg Jr., S. & Hitchens, T. (2020, October). “Army, Air Force Get Serious On JADC2: Joint Exercises In 2021.” *Breaking Defense.*

49. Japan Ministry of Defense. (2020). *Defense of Japan 2020.*

50. Maucione, S. (2020, January). “Air Force using agile approach to connect systems for battle.” *Federal News Network.*

51. Clark, B., Patt, D. & Schramm, H. (2020). *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations.* Center for Strategic and Budgetary Assessments. https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations/publication/1

52. Hirota, O. (2007). “Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol.” *Physical Review A, 76*(3); International Telecommunication Union. (2019). *Overview on networks supporting quantum key distribution.* Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities. https://www.itu.int/rec/T-REC-Y.3800-201910-I

53. National Space Policy Secretariat. (2020). *Outline of the Basic Plan on Space Policy.*

54. Ministry of Foreign Affairs of Japan. (2019). *The 4th Japan-Australia Cyber Policy Dialogue Joint Statement.*

55. This section is based on LAC Co., L., & Defense Structure Improvement Foundation. (2016). 中国のサイバー攻撃の実態（平成***28***年度）. https://ssl.bsk-z.or.jp/kakusyu/pdf/jyousekikenkyu29.2.pdf

56. 情報セキュリティ年表. (n.d.). Retrieved September 29, 2020, from https://scan.netsecurity.ne.jp/feature/security-chronology/#2000

57. ScanNetSecurity. (2011, 20 September) 9月18日「大規模日本Webサイト攻撃活動」の成果（Far East Research)https://scan.netsecurity.ne.jp/article/2011/09/20/27330.html

58. LAC Co., L., & Defense Structure Improvement Foundation. (2016). 中国のサイバー攻撃の実態.

59. Sudo, T., & Sato, T. (2020, May 20). Mitsubishi Electric attack likely stole data on new missile. THE ASAHI SHIMBUN. http://www.asahi.com/ajw/articles/13388776

60. 日本の防衛機密・企業技術を危うくするハッカー集団 中国政府の関与と狙いを読む. (2020, April 26). 毎日新聞. https://mainichi.jp/articles/20200426/k00/00m/040/113000c

61. Harada, I. (2019). サイバー強国中国と如何に向き合うか. *Crisis & Risk Management Review, 27*, 1–10. https://crmsj.org/journal/27/crmsj_journal_27_1.pdf
62. Ibid.
63. Ibid.
64. National Center of Incident Readiness and Strategy for Cybersecurity. (2018). サイバーセキュリティー戦略. https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf
65. The author was a member of the group that formulated these guidelines. Japan Ministry of Defense. (2012). *Toward Stable and Effective Use of Cyberspace (*防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて*)*. https://www.mod.go.jp/j/approach/defense/cyber/riyou/index.html
66. National Center of Incident Readiness and Strategy for Cybersecurity. (2019). サイバーセキュリティ*2019* (*2018*年度報告・*2019*年度計画). https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf
67. Watanabe, Y. & Sasaki, T. (2020). 現代戦争論ー超「超限戦」- これが*21*世紀の戦いだ. Wani Books Co., Ltd. https://www.wani.co.jp/event.php?id=6695
68. The author was the chief officer of the Joint Staff Office when the unit was established.
69. Japan Ministry of Defense. (n.d.). "Regarding Response to a Cyber Attack." Retrieved September 29, 2020, from https://www.mod.go.jp/e/publ/answers/cyber/index.html
70. Adapted from Japan Ministry of Defense. (2019). *Defense of Japan Pamphlet. MoD HP*. https://www.mod.go.jp/e/publ/w_paper/wp2019/DOJ2019_Digest_EN.pdf
71. "Establishment of a fact-checking framework" was a major agenda item at the AFCEA Intelligence and National Security Summit conference held in Washington DC in September 2019, which this author attended for countering influence operations by China and Russia.
72. Madan, T. (2017, November 16). "The Rise, Fall, and Rebirth of the 'Quad'." *War on the Rocks.* https://warontherocks.com/2017/11/rise-fall-rebirth-quad/; Ministry of Foreign Affairs of Japan. (2007). "Confluence of the Two Seas." Speech by Shinzo Abe, Prime Minister of Japan at the Parliament of the Republic of India. https://www.mofa.go.jp/region/asia-paci/pmv0708/speech-2.html
73. Grossman., M. (2005). "The Tsunami Core Group: A Step Toward a Transformed Diplomacy in Asia and Beyond." *Security Challenges, 1*(1).
74. Ministry of Foreign Affairs Japan. (2007). "Confluence of the Two Seas" Speech by Mr Shinzo Abe https://www.mofa.go.jp/region/asia-paci/pmv0708/speech-2.html
75. Kyodo (2020, October 6) "Quad nations vow to step up coordination for free and open Indo-Pacific" *Kyodo.* https://www.japantimes.co.jp/news/2020/10/06/national/politics-diplomacy/quad-free-open-indo-pacific-china/
76. Ibid.
77. Dobson, J. (2020, October 10). "What's the point of the Quad?" *Sunday Guardian Live.*
78. Hui, T.M & Hussain, N. (2018). "Quad:2.0: Facing China's Belt & Road?" *RSIS COMMENTARY.*
79. Nelson, R.R. (1993). *National Innovation Systems: A Comparative Analysis.* New York: Oxford University Press.
80. Bransomb, L.M. (1995). *Empowering Technology.* Cambridge: MIT Press.
81. Shane, A. (2005). *Academic Entrepreneurship University Spinoffs and Wealth Creation.* Cheltenham, UK: Edward Elgar.
82. Christensen, C.M. (1997) *The Innovator's Dilemma.* Harvard Business Review Press.
83. Marukawa, T. (2020). "Export Restrictions in the Japan–China–U.S. Trilateral Relationship." *The Japanese Political Economy*.
84. Ibid.
85. Bransomb, *Empowering Technology*.

About the National Security College

The National Security College (NSC) is a joint initiative of The Australian National University and Commonwealth Government. The NSC offers specialist graduate studies, professional and executive education, futures analysis, and a national platform for trusted and independent policy dialogue.

T +61 2 6125 1219

E national.security.college@anu.edu.au

W nsc.anu.edu.au

 @NSC_ANU

 National Security College

CRICOS Provider #00120C