CYBERDEFENSE REPORT

Japan's National Cybersecurity and Defense Posture

Policy and Organizations

Zürich, September 2020

Cyber Defense Project (CDP)
Center for Security Studies (CSS), ETH Zürich

CSS ETH Zurich

ETH zürich

Available online at: css.ethz.ch/en/publications/risk-and-resilience-reports.html

Author: Stefan Soesanto

ETH-CSS project management: Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Benjamin Scharte, Head of the Risk and Resilience Research Group; Andreas Wenger, Director of the CSS.

Editor: Jakob Bund
Layout and graphics: Miriam Dahinden-Ganzoni

DOI: 10.3929/ethz-b-000437790

Table of Contents

1 Introduction

The goal of this study is to provide the reader with a deeper understanding of the evolutionary path Japan's national cybersecurity and cyber defense posture has taken since the year 2000. To do so, the study explains trigger events, major policy documents, and outlines the current organizational government structure. Please note that this study is non-exhaustive, meaning, there are numerous sectoral developments, specialized regulations, and smaller governmental organizations that this study does not specifically touch upon.

Following this introduction, section two contextualizes the cyber-relevant policy areas that the Japanese government is currently working on. Section three expands on this by explaining the trigger events that have spurred the necessity for government involvement. Section four analyzes the main policy documents that have been and are still shaping Japan's behavior and thinking pertaining to cyberspace. And section five takes a deep dive into the organizational structure by outlining and connecting more than 45 Japanese government and government-affiliated organizations that make up the nation's cybersecurity and defense posture (ministries, agencies, councils, units etc.).

Please note that this study only looks at organizations and instruments the Japanese government is involved in. It does not comprehensively touch upon the evolution and dynamics within the private sector in Japan.

2 Policy Areas

2.1 Cybersecurity

In January 2000, the Japanese government discovered cybersecurity as a policy area and – as a foundational first step – published the "Action Plan to Protect Information Systems against Cyber-attacks" (NISC 2007, p. 37). In mid- to late-2000, the government embarked on a dual-pronged policy approach to strategically tackle cybersecurity in more detail. The first policy arrow was dedicated to ensure IT security within the government itself, while the second arrow was exclusively aimed at critical infrastructure protection. Throughout the decade, this dual-pronged strategy was continuously refined with the creation of new institutions, new information sharing pathways, and underpinned by new information security strategies and regulations.

In 2014, The "Basic Act on Cybersecurity" for the first time legally defined the term "cybersecurity" in Japan. According to the Basic Act – which as the name implies is a basic law – cybersecurity encompasses: "the necessary measures that are needed to be taken to safely manage information, such as prevention against the leak, disappearance, or damage of information which is stored, sent, in transmission, or received by electronic, magnetic, or other means unrecognizable by natural perceptive functions […]; and to guarantee the safety and reliability of information systems and information and telecommunications networks (including necessary preventive measures against malicious activities toward electronic computers through information network or storage media for information created by electronic or magnetic means […], and that those states are appropriately maintained" (Japanese Government, 2014).

To achieve these goals, the Basic Act lays out several foundational responsibilities for the Japanese government, local authorities, critical information infrastructure providers (initially spanning ten sectors, currently consisting of 14 sectors), cyber-related business operators, and educational and research institutions.[1]

While government ministries, agencies, and organizations are responsible for their own cybersecurity posture, they do closely cooperate with the National Center for Incident Readiness and Strategy for Cybersecurity (NISC). For this purpose, the NISC maintains two operational components: The Government Security Operation Coordination Team

[1] On May 19, 2014, the Basic Policy for Critical Information Infrastructure Protection (3rd edition), added chemical, credit card, and petroleum industries as critical information infrastructure sectors. On July 25, 2018, revisions to the 4th edition of the Basic Policy for Critical Information Infrastructure Protection (CIIP) added airports as the 14th CIIP sector.

(GSOC) and the Cyber Incident Mobile Assistant Team (CYMAT).

Public-private cooperation is practiced on all levels of government. On the cabinet level the IT Strategic Council (within the IT Strategic HQ) and the four committees within the Cybersecurity Strategic HQ, are the most prominent elements. On the ministerial level, the Cyber Defense Council of the Ministry of Defense (MoD), the Cyber Attack Analysis Council co-led by the Ministry of Economy, Trade and Industry (METI) and the Ministry of Internal Affairs and Communications (MIC), as well as the National Police Agency's numerous Cyber Terrorism Countermeasure Councils, play crucial roles in advancing Japan's cybersecurity posture down to the prefecture level. Similarly, as its newest addition since April 2019, the Cybersecurity Council facilitates public-private cooperation in a unique voluntary way.

By definition, cybersecurity in Japan is inseparable from the protection of personally identifiable information (PII). The Act on Protection of Personal Information of May 2003 (APPI) forms the legal backbone for safeguarding PII in Japan. Going through substantial revisions over the past 16 years, the APPI now encompasses fines – similar to the EU's General Data Protection Regulation (GDPR) – and even imprisonment for up to six months for ignoring an order by Japan's Personal Information Protection Commission. On 23 January 2019, the EU Commission adopted its adequacy decision on Japan, allowing "personal data to flow freely between the two economies on the basis of strong protection guarantees" (EU Commission, 2019). Věra Jourová, then Commissioner for Justice, Consumers and Gender Equality, noted that "this adequacy decision creates the world's largest area of safe data flows. Europeans' data will benefit from high privacy standards when their data is transferred to Japan" (EU Commission, 2019). Apart from Japan, only Argentina, Canada (commercial organizations), Israel, Switzerland, Uruguay, and five smaller countries provide adequate privacy protections as recognized by the European Commission (EU Commission, n.d.).

2.2 Cybercrime

In November 2001, the Japanese government signed the "Convention on Cybercrime of the Council of Europe" (better known as the Budapest Convention). The Convention is the first and most important international treaty on "crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security" (Council of Europe, n.d.). Its main objective is to "pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation" (Council of Europe, n.d.). Between 2004 and 2006, the Japanese government submitted three bills to the Diet to ratify the Convention, but eventually dropped all three in the process. In 2011 – ten years after the government's initial signature – a bill was finally submitted to and passed by the Diet, leading to the ratification of the Convention on 3 July 2012.[2]

Operationally, Japan's National Police Agency (NPA), in conjunction with the Ministry of Justice, is primarily responsible for combatting cybercrime in Japan. In the maritime arena, the Ministry of Land, Infrastructure, Transport, and Tourism adds to the mix as it oversees the Japan Coast Guard – which is also in the business of data forensics in the context of fighting maritime crime.

2.3 Cyber Terror (サイバーテロ)

Spurred by a combination of cyber-related incidents, caused by Japanese left-wing extremists, Chinese nationalistic hacktivist, and the *Aum Shinrikyo* doomsday sect, the Japanese government embarked on a mission to combat what it termed "cyber terror."

In December 2000, the "Special Action Plan for Cyber Terrorism Countermeasures for Critical Infrastructure" defined cyber terror as "any attacks using information and communication networks and information systems that could have a significant impact on people's lives and socio-economic activities" (ISMPO, 2000).

In practice, cyber terrorism thus includes everything from denial-of-service (DDoS) attacks and defacements of websites, to the deployment of highly advanced sabotage tooling like Stuxnet. The NPA literally uses these three categories to officially explain cyber terror (NPA, n.d.). Interestingly enough, Google Trends shows two significant spikes for the search term "サイバーテロ" in 2010 (Google Trends, n.d.). The first spike occurred in March and relates to the online conflict between the Japanese image board 2channel (2ch) and the Terror Action Association (TAA) – a loose alliance of various South Korean online communities. The confrontation commenced on 1 May, when 2ch users insulted South Korea's Olympic ice-skating queen Kim Yuna and celebrated the death of Kang Byung Kil – a Korean student who was lynched by Russian skinheads on February 19, 2010 (Kim, 2010). TAA's actions included DDoS attacks and defacements of 2ch, and even the Blue House (South Korea's presidential residence) took precautionary measures by blocking all

[2] Note: Two amendments were included: (1) Revisions to Japan's Penal Code and (2) Revisions to Japan's Criminal Procedure Law. See: Tsuboi, n.d.

Japanese internet protocol (IP) addresses from connecting to its website. Overall, 2ch was unable to successfully retaliate against TAA and the stand-off ended after a mere nine hours (Kim, 2010). The second spike occurred in September 2010 and is most likely related to the heightened media coverage surrounding Stuxnet.

Over the years, the cyber terror narrative has naturally crumbled as more precise definitions, distinctions, and insights negated the terrorism aspect as a targeted outcome in most cyber incidents. Notwithstanding these developments, the term cyber terror is still widely used in Japan, and has practical implications for public-private cooperation. For example, the NPA's "Cyber Terrorism Countermeasure Councils" facilitate public-private partnerships on the prefecture level, while the Cyber Terrorism Countermeasures Council maintained by the Tokyo Metropolitan Police is a coordinating hub to secure all big events in Japan – such as the 2021 Tokyo Olympics and Paralympics.

Note: The terror aspect of cyberattacks – e.g. psychological aftermath effects – has slowly been gaining traction as medical health is increasingly being discussed within the cybersecurity community. It might well be that Japan's terror narrative got it right for the past 20 years, and terror is turning into an adversary's primary/secondary tactical objective for campaigns running below the threshold of the use of force.

2.4 Cyber Diplomacy

The Ministry of Foreign Affairs (MOFA) leads Japan's cyber diplomacy efforts.

Back in the year 2000, MOFA was primarily tasked with fostering international cooperation in the area of internet governance (standards and rules) and protecting critical infrastructure (combatting cyber terror). The government's second "National Strategy on Information Security" of 2009 expanded on that mission, and by 2013 MOFA was in charge of a whole-of-government approach to turn Japan into a "world-leading" part of cyberspace. The Strategy specifically put MOFA in charge of (a) promoting the rule of law in cyberspace, (b) developing confidence-building measures, and (c) facilitating cooperation on capacity building for developing countries.

In February 2012, the post of Ambassador in charge of Cyber Policy was created, and in June a Japanese government delegation led by the Ambassador embarked on its first bilateral cyber dialogue. Since 2012/13 Japan has also been an avid member of every United Nations Group of Governmental Experts (UN GGE) on Advancing responsible State behavior in cyberspace in the context of international security.

In May 2016, Japan hosted the G7 Ise-Shima Summit, which produced the declaration of the "G7 Principles and Actions on Cyber" and the Ise-Shima Cyber Group – a G7 working group exclusively focused on "how to promote international law, norms, confidence building measures and capacity building in order to increase stability and security in cyberspace" (G7, 2016; MOFA, 2016a).

On 12 July 2016, MOFA eventually established a dedicated Cyber Security Policy Division within the Foreign Policy Bureau to "lead international discussions on how to ensure a safe and secure cyberspace, [and] strengthening coordination with other countries (MOFA 2016b)."

While it is often said that Japan's (and the EU's) cyber diplomacy efforts are predominately a normative project, this holds true for almost the entire field of cyber diplomacy. What makes Japan stand apart from the normative narrative is the Japan-US Cyber Dialogue – which is led by MOFA and was created as a vehicle for closer alliance cooperation with the US in cyberspace (see p. 24).

2.5 Cyber Defense

While there is no official Japanese definition as to what the term "cyber defense" actually entails, it is primarily used in reference to cyber-related activities conducted by the MOD, the Self-Defense Forces (SDF), and the Japanese intelligence community.

Since September 1951, Japan maintains a military alliance with the United States.[3]Prior to 2010, none of Japan's annual defense white papers contained any references to cyberspace in general or cyber warfare in specific. Spurred by the cyberattacks against Georgia in 2008 and the establishment of US Cyber Command in June 2009, the 2010 Japanese defense white paper eventually raised the issue upfront with a dedicated section on "trends concerning cyber warfare capabilities" (MoD, 2010).

In the aftermath of Stuxnet, cooperation in cyberspace was raised in the joint declaration of the US-Japan Security Consultative Committee (2+2) in 2011. And by 2015, the alliance agreed to: (a) "share information on threats and vulnerabilities in cyberspace in a timely and routine manner, as appropriate," to ensure the safe and stable use of cyberspace, (b) "share, as appropriate, information on the development of various capabilities in cyberspace, including the exchange of best practices on training and education," and (c) "cooperate to protect critical infrastructure and the services upon which the Self-Defense Forces and the

[3] In force since April 28, 1952

United States Armed Forces depend to accomplish their missions, including through information sharing with the private sector, as appropriate" (MOFA, 2015).

In April 2019, the US and Japan eventually agreed and officially proclaimed that "a cyber-attack could, in certain circumstances, constitute an armed attack for the purposes of Article 5 of the Japan-U.S. Security Treaty" (MoD, 2019a). The US-Japan Cyber Defense Cooperation framework is the primary vehicle for policy coordination and information exchanges between the two allies.

In terms of cyber defense operations, the SDF are primarily tasked with monitoring and protecting their own information systems, and – in case of an armed attack – are allowed to "block and eliminate the attack by leveraging capabilities in space, cyber, and electromagnetic domains" (MoD 2018a, p. 12). For this purpose, the MoD has outsourced the development of offensive cyber capabilities in 2019 to one or several unnamed private Japanese companies – mirroring the MoD's cooperation with Fujitsu in 2012.[4] According to the Japan Times, the delivery date for this offensive cyber capability was set for March 2020 (Japan Times, 2019).

The conceptual idea behind the move is that the SDF will utilize these offensive cyber capabilities for defensive purposes during wartime and deterrence purposes during peacetime. Yet, how this will actually work in practice is currently unclear

In terms of major cyber defense exercises, Japan has sent several representatives to observe the US Department of Homeland Security's Cyber Storm III and IV exercises in 2010 and 2013 (CISA, n.d.). In 2016, Japan's National Information Center (NISC) and Japan Computer Emergency Response Team/Coordination Center (JPCERT/CC) actively participated in Cyber Storm V (US DHS 2016, p. 21).[5]

In 2015, Japan also for the first time participated in NATO's annual Cyber Coalition exercise.[6] Run remotely and at NATO's cyber range in Tartu, Estonia, Cyber Coalition is the alliance's largest cyber exercise since November 2008. In 2019 it brought together 900 participants from 28 NATO member states and three partner nations (Japan, the Ukraine, and Georgia) for a period of five days (SHAPE, 2019).

On 15 January 2018, Prime Minister Abe Shinzo announced Japan's intention to become a contributing participant at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn. As of this writing, Japan still maintains observer status.[7]

Apart from the intelligence cooperation within the context of the US-Japan alliance, Tokyo is closely exchanging information with the Five Eyes (US, UK, AUS, NZ, CAN) on Chinese influence operations, cyber espionage, foreign investments, and Beijing's growing military muscle. It also reportedly tackles North Korea's ballistic missile and nuclear program, Pyongyang's illicit trade activities, and the regime's cyberattacks and cybercriminal campaigns across the globe (Japan Times, 2020; Barking, 2018). As of 2020, Tokyo is considered a "sixth eye" under the expanded "Five Eyes plus" framework (JP, ROK, GER/FRA) (Ryall, 2020).

[4] Note: Back in 2012, the MoD outsource the development of a 'seek and destroy' malware to Fujitsu (Leyden, 2012). Open source reporting is not entirely clear as to whether the Fujitsu malware failed to produce the expected results or why exactly the product was shelved in end.

[5] Note: It is unclear from the data available whether Japan participated in Cyber Storm VI in 2018.

[6] Spurred by the 2007 DDoS attacks against Estonia, NATO commenced the first Cyber Coalition exercise in November 2008.

[7] Note: The NATO CCDCOE is not directly funded by the alliance and is not part of NATO's command structure (NATO 2019, Role of Centres of Excellence).

3 Evolution (Trigger Events)

3.1 Cyber Terror

30 November 1985 – The roughly 300-member strong Japan Revolutionary Communist League – also known as the *Chukaku-ha* or Middle Core Faction – simultaneously targets 35 key rail communication and signal systems in and around Tokyo and Osaka. They slash vital cables in gutters along tracks and set fire to signal boxes at key sections of Japan National Railways (Haberman, 1985). The group subsequently succeeded to knock out numerous switching systems, telephone hookups, computerized booking operations, and effectively shut down "23 commuter lines during the morning rush hour" for approximately 6.5 to 12 million commuters (Haberman, 1985; Moosa, 1985). According to Littleton, the group also "jammed police and rescue radio frequencies in an attempt to hamper and delay response by the authorities" (Littleton 1995, p. 77). The LA Times additionally reported that, "commuters who switched to automobiles in an attempt to get to work created traffic jams of as long as 28 miles on expressways leading into Tokyo," and that "more than 50 schools in the Tokyo area closed for the day" (Jameson, 1985).

Although no one was injured and the severed cables were repaired within 24 hours, the incident marked the first and to-date only occurrence in Japan of what at the time was coined "techno terrorism." The *de-facto* pinpoint strategy was not aimed at blowing up infrastructure but at severing critical control circuits to disconnect command and control systems and causing massive real space disruptions.[8]

23 January 2000 – Tokyo allows the conference on "The Verification of the Rape of Nanking: The Biggest Lie of the 20th Century" to go ahead. In reaction, Chinese nationalistic hacktivists deface numerous Japanese government websites, redirect queries to porn sites, and email bombard government inboxes (BBC 2000).

2 March 2000 – Japanese police investigators announce that computer companies affiliated with the *Aum Shinrikyo* doomsday sect "developed software programs for at least 10 government agencies, including the Defense [Agency]," and "more than 80 major Japanese companies" (Sims, 2000). According to George Wehrfritz at Newsweek, the investigators also determined that "the first contracts were awarded in 1996--one year after the cult mounted a nerve-gas attack on Tokyo's subway system that killed 12, injured 5,000 and stunned the nation" (Wehrfritz, 2000). Calvin Sims at the New York Times aptly explains the significance of this revelation by noting that "underscoring the immense fear that the sect provokes in Japan, the Defense [Agency] and the Nippon Telegraph and Telephone Corporation, the country's main provider of telephone and internet service, immediately suspended the use of all computer software developed by companies linked to *Aum*" (Sims, 2000).

September 2012 – The Japanese government purchases the Senkaku/Diayu islands. In reaction, China's Honker Union conducts DDoS attacks, doxing campaigns, and defacements against 19 Japanese websites, including the MoD, the Ministry of Internal Affairs, and the Japanese Supreme Court (Muncaster, 2012).

3.2 Cyberespionage

July 2011 – Servers at the Japanese House of Representatives are infected by the Chinese advanced persistent threat (APT) group Icefog (Kaspersky Labs 2013, p. 14). The incident is made public when the Asahi Shimbun reports on it on October 25, 2011.

August, 2011 – Japanese defense contractor Mitsubishi Heavy Industries (MHI) is breached. Citing internal MHI documents media outlets report on the breach in September. The Japanese government is furious, as MHI did not inform them about the breach. On 21 September, Mitsubishi publicly confirmed the incident but notes that no classified information was leaked (MHI, 2011). Overall, 83 computers in at least 11 locations were infected with eight different malware products. On 24 October, Asahi reports that the attackers "likely netted military data on warplanes and information on nuclear power plants" (Kubota, 2011).

June 2015 – The Japanese Pension Service (JPS) announces that it was breached and the personal information of 1.25 million Japanese citizens was exfiltrated (JPS, 2015). In the same month, the US Office of Personnel Management announces that it was breached and the personal information of 22.1 million US government employees was exfiltrated.

November 2016 – The Japanese Business Foundation (Keidanren) officially reports that its network were breached. According to Kyodo News, the "investigative team found a large amount of suspicious

[8] Note: According to the LA Times, "by noon, 48 people, including the three top leaders of the Chukaku-ha […] had been arrested" (Jameson, 1985)

data communications between 10 external servers and 23 infected PCs" (Kyodo News, 2019).

December 2018 – MOFA releases a public attribution statement, noting that "Japan has identified continuous attacks by the group known as **APT10** to various domestic targets including private companies and academic institutions and expresses resolute condemnation of such attacks" (MOFA, 2018). Canada, Australia, New Zealand, the UK, and the US (Five Eyes) coordinate the release of official statements attributing the APT10 campaign to the Chinese Ministry of State Securitys.

3.3 Cybercrime

2006 – Various versions of the Antinny worm spread through the Japanese peer-to-peer file sharing network Winny and infect numerous systems at Japan's Defense Agency, the SDF, various police departments, power plants, Internet service providers (ISPs), mobile phone companies, Japan Airlines, and even antivirus software manufacturers. Once infected, Antinny randomly select files from the users' hard disk and makes them available on the Winny file-sharing network (Gradijan, 2006; Freire, 2006). According to NBC News, Antinny was "the most talked about in Japan as it generate[d] headline after headline, month after month" (Freire, 2006). To combat Antinny, the government and the private sector took the unusual step of banning Winny from work computers and even firing employees who refused to comply. Several organizations "also demanded that staff not take work home and delete Winny from any PCs at home they used for work" (NBC, 2006).

Note**:** Winny was developed by Isamu Kaneko in 2002. The then 33-year-old research assistant at the University of Tokyo was arrested in 2004 – which marked the first arrest in Japan of a suspected developer of file-sharing software (Wired, 2004). Initially found guilty and fined 1.5 million Yen, the Osaka High Court overturned the ruling in 2009, and two years later the Supreme Court of Japan held up the acquittal (Japan Times, 2011).

July 2012-February 2013 – After a seven-month investigation, numerous death threats, four false arrests, and an embarrassing display of Japan's police, the most bizarre cybercriminal case Japan has ever witnessed ended when 30-year old IT office worker Yusuke Katayama was arrested on February 11, 2013.

The case began in the summer of 2012, when numerous death threats were posted on Japanese websites and send out via email. Eventually an announcement to commit mass murder posted on the Yokohama city website was traced and led to the arrest of a 19-year old student at Meiji University.

In July, postings threating mass killings appeared on the Osaka city website, which were traced back to anime creative director Masaki Kitamura, who was subsequently indicted although strenuously professing his innocence. By September, two more individuals were arrested for similar offenses in Mie and Fukuoka.

The cases took a rapid turn when in October, an email was sent to a Tokyo-based lawyer and several Japanese media outlets which stated that "I am the real culprit" and included numerous details on how the four crimes were committed that only the real culprit could know. According to the email the four individuals arrested were infected with a Trojan horse which allowed the criminal to remotely control their computers and post the death threats. The culprit also stated that his motive was not to put innocent people behind bars, but to solely "entrap the police and prosecutors and expose their shameful status to the world" (Adelstein, 2017).

In reaction to the email, the police reopened the investigation and admitted that there might have been several false arrests. By December, all four individuals were cleared of all charges against them. As Adelstein explains, "according to NPA sources, the cybercrime squads in each police department had determined the IP addresses of the computers that were used to make the threats but hadn't gone further to see if the computers had been affected by viruses or had malicious software installed that would make them platforms for cybercrime" (Adelstein, 2017). Even more troubling than this lack of forensic investigative standards was the fact that in two cases the arrested individuals were coerced into making false confessions.

The hunt for the criminal also got the US Federal Bureau of Investigation (FBI) involved as one email was sent through a US server. The FBI eventually found a copy of the Trojan horse which included information that would eventually connect it to Yusuke Katayama.

Realizing that the police would catch him sooner rather than later, Katayama announced in December 2012 that he would commit suicide, but then changed his mind and sent the police on a wild puzzle spree whose solution led to a cat on Enoshima Island which had a micro SD card embedded in its collar (Blaster, 2014). On the card was the source code for the Trojan horse. A security camera on Enoshima captured Katayama playing with the cat, which in combination with the SD card and the information gained by the FBI, led to the arrest of Katayama. In 2015, Katayama was sentenced to eight years in prison (BBC, 2015).

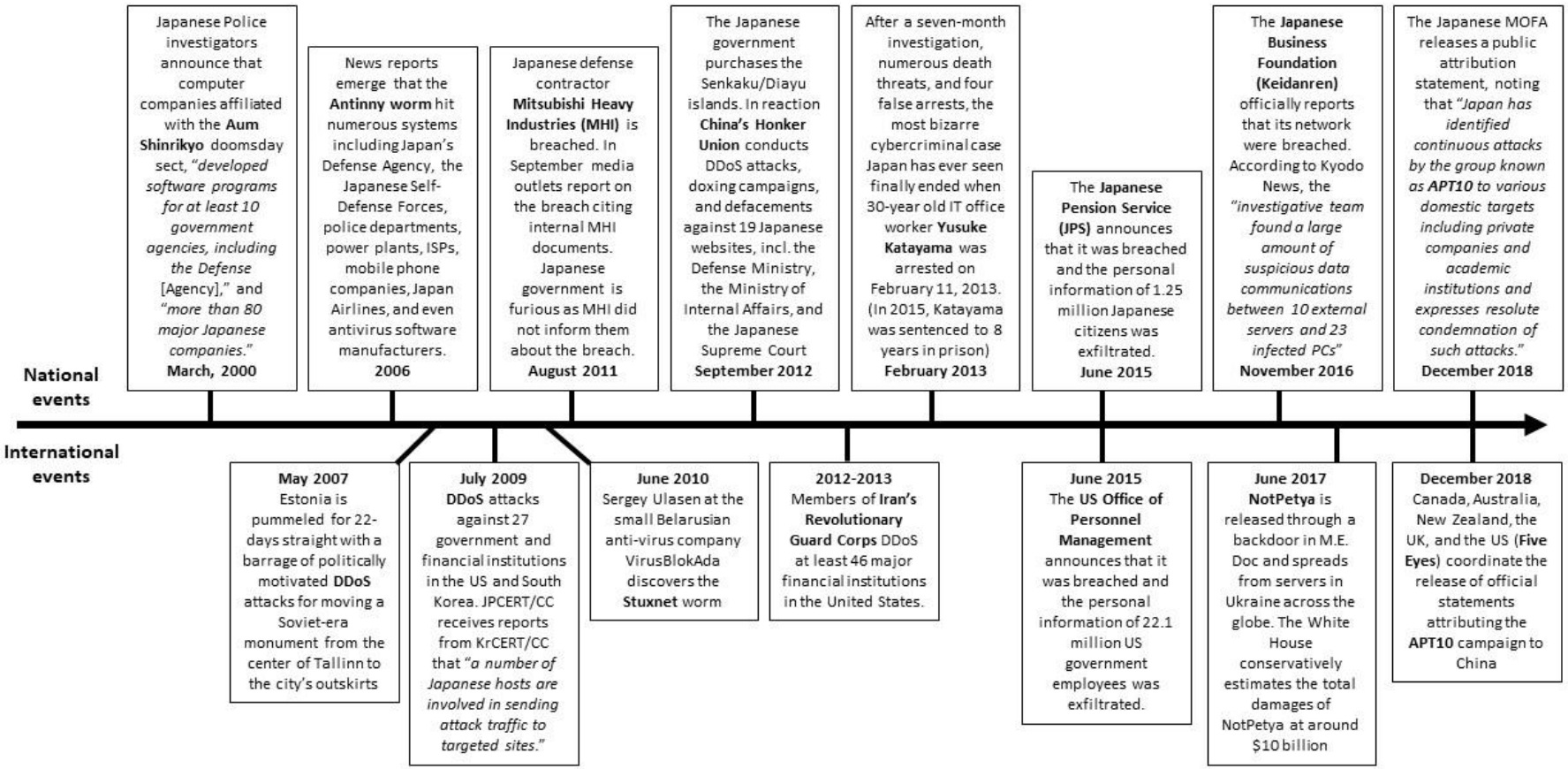
Note: While the exact fallout of the case is still understudied, it is safe to say that it had significant impact on the conduct of the Ministry of Justice and NPA, and most likely kicked-off a complete overhaul of the agency's cybercriminal investigative procedures.

2014 – Tokyo-based Mt. Gox – the world's largest cryptocurrency exchange at the time – announced its bankruptcy. Leaked corporate documents revealed that hackers raided Mt. Gox as early as September 2011 and skimmed 850,000 bitcoins (roughly equivalent to 460 million USD at the time) (McMillan, 2015). In August 2015, Mt. Gox founder – and French national – Mark Karpelès was arrested and released on bail in July 2016. In March 2019, the Tokyo District Court found Karpelès guilty of producing illegal records but also not-guilty of embezzlement and not-guilty of abuse of his position at Mt. Gox for personal gain (Dooley, 2019).

The trail of the stolen Mt. Gox bitcoins most prominently also involved Russian national Alexander Vinnik. Vinnik was indicted by the US Department of Justice in January 2017 and arrested in Greece six months later for running the cryptocurrency exchange BTC-e and engaging in money laundering at the scale of 4 billion USD – including laundering funds from the Mt. Gox hack (DoJ, 2017). According to bitcoin security specialist group WizSec, the wallets the stolen Mt. Gox bitcoins were transferred to and sold on BTC-e belonged to Vinnki himself (WizSec, 2017). For more than two years, Vinnik was detained in Greece as the US, Russia, and France battled over his extradition. On 24 January 2020, Vinnik was extradited to France on the charges of extortion, aggravated money laundering, conspiracy, and harming automatic data-processing systems. Once Vinnik's case is completed in France, he will be extradited back to Greece, then extradited to the US, and then extradited to Russia (Gaspard, 2020).

Note: Following the Mueller report on Russian interference in the 2016 US Presidential election – which identified wallets on the bitcoin exchange platform CEX.io as a GRU fund to "purchase computer infrastructure used in hacking operations" – speculation on a Vinnik connection has been swirling due to rudimental links between CEX.io and BTC-e wallets (DoJ 2019, p. 36-37; Cotton, 2019).

According to statistics released by the NPA in September 2019, the number of cybercriminal cases in Japan (including cases of child pornography and fraud) have increased from 9014 in 2017 to 9040 in 2018 (NPA 2019, p. 7). In 2016, the number of cases stood at 8324. The number of solved cases stood at 4251 in 2018 – with 181 arrests made – and 4243 in 2019, with 182 arrests made.


National events
International events
Japanese Police investigators announce that computer companies affiliated with the **Aum Shinrikyo** doomsday sect, *"developed software programs for at least 10 government agencies, including the Defense* [Agency]," and *"more than 80 major Japanese companies."* **March, 2000**
News reports emerge that the **Antinny worm** hit numerous systems including Japan's Defense Agency, the Japanese Self-Defense Forces, police departments, power plants, ISPs, mobile phone companies, Japan Airlines, and even antivirus software manufacturers. **2006**
Japanese defense contractor **Mitsubishi Heavy Industries (MHI)** is breached. In September media outlets report on the breach citing internal MHI documents. Japanese government is furious as MHI did not inform them about the breach. **August 2011**
The Japanese government purchases the Senkaku/Diayu islands. In reaction **China's Honker Union** conducts DDoS attacks, doxing campaigns, and defacements against 19 Japanese websites, incl. the Defense Ministry, the Ministry of Internal Affairs, and the Japanese Supreme Court **September 2012**
After a seven-month investigation, numerous death threats, and four false arrests, the most bizarre cybercriminal case Japan has ever seen finally ended when 30-year old IT office worker **Yusuke Katayama** was arrested on February 11, 2013. (In 2015, Katayama was sentenced to 8 years in prison) **February 2013**
The **Japanese Pension Service (JPS)** announces that it was breached and the personal information of 1.25 million Japanese citizens was exfiltrated. **June 2015**
The **Japanese Business Foundation (Keidanren)** officially reports that its network were breached. According to Kyodo News, the *"investigative team found a large amount of suspicious data communications between 10 external servers and 23 infected PCs"* **November 2016**
The Japanese MOFA releases a public attribution statement, noting that *"Japan has identified continuous attacks by the group known as **APT10** to various domestic targets including private companies and academic institutions and expresses resolute condemnation of such attacks."* **December 2018**
May 2007 Estonia is pummeled for 22-days straight with a barrage of politically motivated **DDoS** attacks for moving a Soviet-era monument from the center of Tallinn to the city's outskirts
July 2009 **DDoS** attacks against 27 government and financial institutions in the US and South Korea. JPCERT/CC receives reports from KrCERT/CC that *"a number of Japanese hosts are involved in sending attack traffic to targeted sites."*
June 2010 Sergey Ulasen at the small Belarusian anti-virus company VirusBlokAda discovers the **Stuxnet** worm
2012-2013 Members of **Iran's Revolutionary Guard Corps** DDoS at least 46 major financial institutions in the United States.
June 2015 The **US Office of Personnel Management** announces that it was breached and the personal information of 22.1 million US government employees was exfiltrated.
June 2017 **NotPetya** is released through a backdoor in M.E. Doc and spreads from servers in Ukraine across the globe. The White House conservatively estimates the total damages of NotPetya at around $10 billion
December 2018 Canada, Australia, New Zealand, the UK, and the US (**Five Eyes**) coordinate the release of official statements attributing the **APT10** campaign to China

4 Relevant Policy Documents

This section dives into the various policy documents that are relevant for tracing and understanding the evolution of Japan's cybersecurity and defense posture.

4.1 Key Policy Documents

4.1.1 **2000 Basic Act**

The "Basic Act on the Formation of an Advanced Information and Telecommunications Network Society" of 6 December 2000 outlines fundamental strategic principles and policies for the creation of a society in which creativity and development are enabled by obtaining, sharing or globally transmitting a variety of information and knowledge via the Internet (Japanese Government, 2000). To achieve this goal, the Act defines broad government responsibilities and establishes the IT Strategic Headquarters (then called the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society).

Article 3 to 9 stipulate basic principles, which among others include the promotion of electronic commerce, the improvement of convenience for everyday life, the promotion of diversity of lifestyle, the circulation of high-quality information to facilitate independent and rational consumer choices, as well as improving welfare and re-vitalizing local communities.

Articles 10 to 15 lay out how these principles ought to be achieved, by for example allowing local authorities to develop autonomous strategies that reflect distinctive features of their own areas, dictating close cooperation between the national and local authorities, and stipulating the publication of statistics and public awareness campaigns.

Articles 16 to 24 articulate basic development policies, ranging from the promotion of fair competition among business operators, increasing the informatization of government administration processes, ensuring security and reliability of networks, protecting personal information, and actively engaging in international collaboration efforts to develop international standards and rules.

Articles 25 to 36 establish the IT Strategic Headquarters in the Cabinet, whose purpose it is to "swiftly and thoroughly pursue strategies to form an advanced information and telecommunications network society" (ibid.).

4.1.2 **2000 Special Action Plan**

The "Special Action Plan for Cyber Terrorism Countermeasures for Critical Infrastructure" of 15 December 2000 was created to protect Japan from all cyber incidents that "could significantly impact people's lives and socio-economic activities" (ISMPO, 2000). The plan starts by outlining measures to improve the level of cybersecurity within the critical infrastructure sectors by stipulating risk analysis, re-examining security guidelines, and pushing for better information exchange between the government and critical infrastructure providers. It also instructs government ministries and agencies to improve their own level of security – within in the context of Japan's e-government kick-off – and directs the technical research teams within the Cabinet Secretariat to "conduct technical research and advice on security measures for information systems of each ministry and agency" (ibid.).

Sections 5 and 6 highlight measures to establish and strengthen public-private partnerships. Measures include the sharing of threat indicators and communicating network breaches through existing communication channels. Setting up procedures to determine whether an incident/failure was actually caused by a cyberattack or not, and how to communicate information in an emergency. It also pushes for an emergency response plan that will streamline damage mitigation, forensic evidence preservation, system restoration, and preventing the reoccurrence of the same attack.

Section 7 stipulates the promotion of education and training for staffers, raising awareness, promoting research and development (R&D), and developing Japan's legal system and criminal law to walk in tandem with the technological revolution.

Section 8 outlines the need for international cooperation to counter cyber terrorism by promoting information exchanges and joint training with OECD countries, the G8, and security organizations outside of Japan.

Note: There are several other documents that are relevant to fully comprehend Japan's cybersecurity and -defense posture and their evolution. For example, the "Basic Act on the Advancement of Public and Private Sector Data Utilization" (Japanese Government, 2016) and the 4th edition of the "Cybersecurity Policy for Critical Infrastructure Protection" (Cybersecurity Strategic Headquarters, 2017).

4.1.3 1st National Strategy

Japan's "First National Strategy on Information Security" – subtitled "toward the creation of a trustworthy society" – was published on 2 February 2006. The document's main objective was to draw up a systematic mid- and long-term plan for information security in Japan.

In contrast to the Basic Act, the National Strategy acknowledged that the coexistence of convenience and security is not a natural given. Thus, employing a "rationality-based approach" that can balance the two would be the way to go (ISPC 2006, p. 6). The document also highlights several problems that the Basic Act did not touch upon, including that the "(1) majority of [security] measures against problems detected in recent years is designed only to solve immediate problems and (2) each entity of IT society is thoroughly engaged in its own measures confined in the bureaucratic sectionalism" (ibid. p. 7).

Given these problems, the Strategy lays out the need for establishing a new public-private partnership model, in which every entity understands the importance of information security and is aware of its own responsibilities in the context of protecting the nation. While the document primarily focuses on the four categories of central/local government, critical infrastructure, businesses, and individuals, it also recognizes entities that indirectly support public-private partnerships through the promotion of understanding and discussion input – including the media, non-governmental organizations, and educational/research institutions.

For each of these entities, the Strategy sets out various aims, ranging from preventing the spoofing of government agencies, promoting information security auditing, developing a Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR) for each critical infrastructure sector, and conducting cross-sectoral exercises, to establishing a uniform qualification and certification system for information security.

4.1.4 2nd National Strategy

The "Second National Strategy on Information Security" – subtitled "aiming for strong 'Individual' and 'Society' in IT Age" – was published on 3 February 2009. With 76 pages the document is more than twice the length of the previous national strategy.

Naturally, the results of the first national strategy significantly informed the goals set out in the second. The government assessed that over the past three years, the first strategy succeeded in increasing information security awareness relating to the risks of peer-to-peer software (such as Antinny), risks of information theft, and risks of system malfunctions leading to the suspension of business operations. It also succeeded in creating a framework for policy promotion, including information sharing frameworks between government agencies and critical infrastructure providers, as well as international information sharing agreements between Japan and the US, and Japan and ASEAN. While some progress was made on preventative measures, the government acknowledged that new risks arise day after day and they constantly change – which makes preventative measures difficult to implement (NISC, n.d., p. 4).

Based on this assessment, the second national strategy set out measures that both continue and further develop the policies set out in 2003. The most important message the document conveys is its departure from emphasizing preventative measures and embarking toward strengthening the response to an "accident assumed society" – meaning that the "parties concerned must take particular care for post measures against accidents such as acknowledgement and analysis of cases, communication, immediate countermeasures and restoration […]" (ISPC 2009, p. 28).

4.1.5 Information Security Strategy

On 11 May 2010, the government published the "Information Security Strategy for Protecting the Nation". According to the document, the need for its publication emerged when in July 2009, 27 government and financial institutions in the US and South Korea were hit by a coordinated wave of DDoS attacks, and "numerous incidents of large-scale private information leaks occurred one after another" (ISPC 2009, p. 1). The document also references growing underground markets for credit card information and highlights the "gumblar" attacks that affected numerous Japanese websites in 2009 (ibid. p. 2).[9]

Apart from re-emphasizing existing information security policies, the 20-page document set out several concrete measures. Within the context of "preparing for a potential large-scale cyber attack," the document emphasized response drills, closer coordination between the public and private sector, comprehensively policing cybercrimes, and reinforcing international alliances (ibid. p. 8-9). The government also set out to consolidate the chief information security officer (CISO) functions within the various government agencies, strengthen the coordination with the Government Security Operation Coordination team (GSOC) team, and – untypically for Japan – "organize the telework

[9] Note: Gumblar was a JavaScript Trojan horse that was deployed against numerous Japanese websites to execute drive-by malware downloads, tamper with web traffic, and steal FTP credentials.

environment in government agencies" to promote cloud usage (ibid. p. 10). Interestingly, the strategy also called for "immediate action to clarify the legality of downloading or reverse engineering to analyze suspected malware samples," and states that "information concerning vulnerabilities and related remedies must be distributed promptly as a preventive measure against malicious activities" (ibid. p. 13).

The document additionally highlights the need to secure Internet of Things (IoT) devices, ensure information security in the medical and educational fields, and promotes the usage of encryption and even "anonymizing" privacy protection technology (ibid. p. 14).

Note: It is not entirely clear why the legality of reverse malware engineering pops-up in the strategy. It might be connected to the 2010 case of Masato Nakatsuji (see: page 28).

4.2 National Cybersecurity Strategy

4.2.1 **1st Cybersecurity Strategy**

On 10 June 2013, Japan's first Cybersecurity Strategy – dubbed "towards a world-leading, resilient and vigorous cyberspace – is published. The 55-page document summarizes numerous aspects that the 2000 Basic Act, the 2000 Special Act, and the two National Information Security Strategies already put in place.

What is new, is the emphasis on diplomacy and defense, which stands in stark contrast to all prior strategies that treated cybersecurity as a purely technical issue devoid of political and national security implications. For the first time ever, the Japanese government clearly articulated that "overseas, cyber attacks aimed at traffic message display signal devices and cyber attacks aimed at systems in critical infrastructures like control systems, with a degree of complexity and sophistication that raises suspicions about the involvement of government level organizations, have occurred and the risk of such attacks causing widespread and far-reaching social turmoil has become a real issue" (ISPC 2013a, p. 9). Similarly, the government points out that "information gathering activities are actively carried out against Japan, recently methods of using targeted attacks by email to steal information from government institutions, etc., have become more complex and sophisticated, and the risks of critical information in government institutions being leaked is increasing" (ibid. p. 33).

To defend Japan against these threats, the SDF are tasked with the protection of their own systems, responding to an armed attack, and providing mutual support in an emergency, including the sharing of classified information (ibid. p. 41-42). The strategy is very careful in articulating and defining the SDF's responsibilities due to Prime Minister Abe stating in the House of Representatives on 3 March 2013 that "a variety of discussions and debates are still ongoing regarding the relationship between cyber attacks and an armed attack and others, and it is difficult to provide a categorical answer at this time" (ibid. footnote 97).

On the diplomacy end, the strategy highlights the government's work toward (a) the application of international law in the cyber domain – specifically the UN Charter and International Humanitarian Law , (b) the continuing efforts to implement confidence-building measures, (c) bilateral and regional discussion and technical support, including within the ASEAN Regional Forum, and (d) ever closer coordination in the context of the US-Japan military alliance – ranging from joint training, sharing threat information, and cooperating on international rulemaking (ibid. p. 49-50).

4.2.2 **Basic Act on Cybersecurity**

On 12 November 2014, the Japanese Diet ratified the "Basic Act on Cybersecurity". The Act for the first time legally defines the term "cybersecurity" and lays out (a) the basic responsibilities for the creation of the Cybersecurity Strategy, (b) basic policies (echoing the Basic Act of 2000), and (c) creates the Cybersecurity Strategic HQ in the Cabinet – which is responsible for preparing the Cybersecurity Strategy and promoting its implementation (Japanese Government, 2014). In essence, the Basic Act forms the rudimentary baseline for Japan's cybersecurity policy.

In preparation for the 2021 Tokyo Olympics and Paralympics, the Act was amended in December 2018 to set up the Cybersecurity Council (サイバーセキュリティ協議会), which consists of national government agencies, local governments, critical information infrastructure operators, information security companies, and educational and research institutions. It also enabled the Cybersecurity Strategic HQ to delegate part of its functions to other government agencies, including "establishing standards for cybersecurity measures for national administrative organs; promoting the implementation of evaluative measures, including audits; and coordinating with relevant persons and entities in Japan and abroad when cybersecurity breaches and threats occur" (Umeda, 2018).

4.2.3 **2nd Cybersecurity Strategy**

On 4 September 2015, the government published its second Cybersecurity Strategy (or rather the first cybersecurity strategy since the Basic Act of 2014). In contrast to previous strategies, the new document is far better structured and concise in its messaging. It clearly articulates Japan's strategic objective in cyberspace, which is defined as to "ensure a free, fair, and secure cyberspace; and subsequently contribute to improving

socio-economic vitality and sustainable development, building a society where the people can live safe and secure lives, and ensuring peace and stability of the international community and national security" (Japanese Government 2015, p. 5).

To achieve this objective, the strategy sets out three approaches: (1) "Being Proactive, not Reactive" – meaning Japan will conduct analyses on future social changes and potential risks; (2) "Acting as a Catalyst, not Just a Passive Player" – stipulating that Japan will support private actors in building out cyberspace and actively contribute to peace and stability in cyberspace; and (3) "Envisaging Cyber-Physical Space, not Cyberspace Alone" – which recognizes that cyberspace has physical components and that "any event in cyberspace may affect society as a whole, producing a synergy effect with various events including those in physical space" (ibid. p. 11).

Three foundational pillars stick out from the strategy: first, its emphasis on creating a secure IoT industry/ecosystem; second, its notion that senior executive management should think about cybersecurity not as costs but as investments; and third, the promotion of supply-chain risks management in an effort to support Japanese enterprises in improving their global operations (ibid. p. 13-15; 16; 20).

While the document also connects cyberspace with national security and defense, the MoD and the SDF are only mentioned in a few paragraphs. These references dwarf in comparison to the sections on cyber diplomacy and international law, which span almost six pages (ibid. p. 38-44).

4.2.4 **3rd Cybersecurity Strategy**

On 27 July 2018, the Japanese government published the third Cybersecurity Strategy. One of the most important changes since 2015 is the notion that cyberspace and real space do not anymore exist independently, but are "mutually interacting entities, such that they cannot be considered separate anymore. Therefore, the two spaces should be seen as a single continuously evolving organic entity" (Japanese Government 2018, p. 2). Based on this notion, the "risk of economic and social loss or damage in real space is expected to expand and accelerate exponentially" (ibid. p. 2).

In regard to the threat environment, the third strategy specifically mentions attacks directed at IoT devices, the fintech sector – including cryptocurrency exchanges – critical infrastructure, and supply chains. It also raises concerns about the credibility of the global information infrastructure as a whole if parts of cyberspace are "controlled and managed by some countries from a superior position" (ibid. p. 7).

The strategy views the rise of Artificial Intelligence as a positive development in line with better optimization, analysis, increased precision in anomaly detection, and a move toward autonomous systems (e.g. automation of malware detection). Strangely, the report makes no direct reference to adversarial machine learning or the introduction of new vulnerabilities by relying on machine learning systems. Instead it worries about the broader aspect of data authenticity and data integrity.

In terms of policy approaches, the strategy re-emphasizes the observation that executive management still sees cybersecurity as a cost and not a necessary investment. To remediate this situation, the government literally put forward a plan to "discover and train personal who are capable of explaining and discussing cybersecurity measures with senior executives" (ibid. p. 16). It also builds out the promotion of supply chain risk management as a vehicle for a global Japanese footprint, by planning to build a cybersecurity framework for supply chain risk and creating and managing a "list of devices and services for which trustworthiness has been proven" (ibid. p. 19). To a degree, this pre-echoed the government's approach toward excluding Huawei in April 2019 from being assigned frequency spectra necessary to build Japan's 5G network.

In the context of securing IoT devices, the strategy also explicitly mentions the government's intention to "steadily improve necessary systems to survey and identify IoT devices that use flawed passwords and expeditiously warn users thereof by telecommunication carriers" (ibid. p. 21).

Note: In preparation for the 2021 Tokyo Olympics and Paralympics, the Japanese National Institute for Information and Communications Technology (NICT) was granted permission in February 2019 to commence the NOTICE project, e.g. executing dictionary attacks against the country's 200 million IoT devices to survey and identify vulnerable devices (MIC & NICT, 2019).[10]

Indeed, the protection of critical infrastructure and preparations for the 2021 Tokyo Olympics and Paralympics encompass a large part of the strategy. However, many of the items mentioned refine aspects already outlined in the government's Cybersecurity Policy for Critical Infrastructure Protection (4th edition).

[10] Dictionary attacks: "a brute-force attack based on selecting potential passwords from a pre-prepared list. The attacker creates a "dictionary" of the most likely sequences of characters and uses a malicious program to check them all in turn in the hope of finding a match. A special type of dictionary attack uses a list of possible password templates and automatically generates a variable component. For example, based on information about the victim's name, an attacker can test the password denisXXX, substituting XXX for the numbers 001 to 999" (see: Kaspersky IT Encyclopedia, n.d.)

Curiously, the third strategy has a much heavier focus on cyber defense than the second strategy. Meaning, it specifically mentions the need to "increase Japan's ability to defend the state (defense capabilities), deter cyberattacks (deterrence capabilities), and be aware of the situation in cyberspace (situational awareness capabilities)" (Japanese Government 2018, p. 37). It even includes the statement that "the acquisition of capabilities to prevent cyber actors from using cyberspace may be considered" (ibid. p. 39). This was an immense step up from the mere focus on diplomacy and enhancing cybersecurity of earlier strategies.

The strategy further mentions for the first time the need to prevent the malicious use of cyberspace by terrorist organizations. Yet, in striking contrast to Japan's official cyber terror definition, the strategy only calls out: the spread and demonstration of violent extremism, recruitment, and gathering of funds (Japanese Government 2018, p. 38).

4.3 National Cyber Defense Strategy

The Japanese government has so far not published a dedicated national cyber defense strategy paper. Instead, Tokyo's cyber defense policy is defined by a number of alliance and government guidelines. The most important of these are discussed below.

4.3.1 **Japan-US Defense Guidelines**

Back in November 1978, Washington and Tokyo drafted the "Guidelines for Japan-US Defense Cooperation." Initially, the document served as a vehicle to counter Japanese concerns that Washington might abandon Tokyo after President Nixon began normalizing relations with China in 1972. The fall of Saigon in April 1975 additionally spurred Tokyo's efforts to improve public support for its domestic defense policy and maintaining a credible US defense commitment to Japan (Green & Murata, n.d.).

With the end of the Cold War, the Guidelines were eventually reviewed in 1997 to realign the *raison d'être* for the US-Japan alliance.

In 27 April 2015, the Guidelines were reviewed for a second time as the alliance partners recognized the increasingly transnational nature of security threats. The new guidelines thus emphasize "seamless, robust, flexible, and effective" bilateral responses, a whole-of government alliance approach, and the global nature of the US-Japan alliance (MoD, 2015a).

For the first time, the Guidelines also specifically mention cross-domain operations to repel an armed attack against Japan and identify cyberspace as an area of defense cooperation.

Specifically, the Guidelines note that the SDF and US Armed Forces will:

- maintain a posture to monitor their respective networks and systems;
- share expertise and conduct educational exchanges in cybersecurity;
- ensure resiliency of their respective networks and systems to achieve mission assurance;
- contribute to whole-of-government efforts to improve cybersecurity; and
- conduct bilateral exercises to ensure effective cooperation for cybersecurity in all situations from peacetime to contingencies.

Importantly, the Guidelines also stipulate that in case of an armed attack against Japan in and through cyberspace – including against critical infrastructure and services utilized by the SDF and US Armed Forces in Japan – Tokyo will have the "primary responsibility to respond, and based on close bilateral coordination, the United States will provide appropriate support to Japan" (ibid.). In the event of "serious cyber incidents that affect the security of Japan" – meaning most likely either a coordinated campaign or precursor cyber incidents leading up to conventional war – the two governments "will consult closely and take appropriate cooperative actions to respond" (ibid.).

4.3.2 **National Defense Program Guidelines**

The "National Defense Program Guidelines for FY 2019 and beyond" (NDPG) were published on 18 December 2018, and serve to broadly define the nation's direction on defense policy and budgeting. The 2018 NDPG are also the first guidelines that were published under the auspices of Japan's newly established National Security Council – calling an end to the blue-ribbon panels consisting of scholars and experts that were previously responsible for developing the NDPG and the Mid-Term Defense Program (Schoff & Romei 2019, p. 1). Political policy consensus was thus now directly driving procurement decisions and vis-a-versa.

The NDPG identify the cyber domain as one of three new domains – including space and the electromagnetic spectrum – that are "poised to fundamentally change the existing paradigm of national security" (MoD 2018a, p. 1). To prepare for this change, the NPDG state that "it has become essential that Japan achieve superiority" in the three new domains. In contrast to US Cyber Command's 2018 vision of superiority – that emphasizes outward oriented persistent engagement wherever the adversary maneuvers – the Japanese interpretation of superiority is almost exclusively inward oriented and defensive as it emphasizes increased resilience and ever-faster remediation and recovery efforts. In essence, Tokyo is trying to build a posture under which "doing harm to Japan would be difficult and consequential" (ibid. p. 8).

To realize this posture, the NDPG set out the goal of building a "Multi-Domain Defence Force", which organically fuses capabilities in all domains, including space, cyberspace and the electromagnetic domain; and is capable of sustained conduct of flexible and strategic activities during all phases from peacetime to armed contingencies" (ibid. p. 11).

To support this jointness and provide an active defense posture, the NDPG stipulate that the SDF will maintain "a cyberspace defense unit [the Cyber Defense Group] as an integrated unit in order to […] fundamentally strengthen cyber defense capability, including capability to disrupt, during attack against Japan, opponent's use of cyberspace for the attack" (ibid. p. 27).

Note: It remains to be seen whether Japan's definition of superiority will survive over time as the cyber threat environment evolves and alliance pressures will increase. Within the context of building a defense posture under which "doing harm to Japan would be difficult and consequential, it is currently entirely unclear what consequences the Japanese government is envisioning.

4.3.3 Mid-Term Defense Program

The "Mid-term Defense Program FY 2019 – FY 2023'"(MTDP) was published together with the NDPG. As Schoff and Romei put it, the MTDP is a relatively detailed "shopping list" for the SDF's three service wings (Schoff & Romei 2019, p. 1).

Apart from re-emphasizing the strengthening of the Cyber Defense Group, the MTDP directs the Ground Self-Defense Forces to "establish cyberspace units and electromagnetic operation units as subordinate units of the Ground Component Command" (MoD 2018b, p. 4). Additionally, the SDF will enhance the resiliency of the SDF's C4 systems, strengthen information gathering capabilities, research and analysis, and develop a practical training environment to test the SDF's cyber defense capabilities (ibid. p. 8).

On the human resource side, the MTDP stipulates that the SDF "develops personnel with strong cyber security expertise, through efforts such as improving the in-house curriculum for specialized education, increasing learning opportunities at institutions of higher education at home and abroad, and conducting personnel management that cultivates expertise. In addition, the SDF will strengthen the cyber defense capability by utilizing superior outside expertise" (ibid. p. 8).

Finally, the MTDP references cyber as a part of the US-Japan Extended Deterrence Dialogue (EDD) (ibid. p. 27).[11]

5 Organizational Structures

Japan's cybersecurity and defense posture has undergone numerous reforms over the years that significantly reshaped and rearranged the government organizational structure. This section provides a non-exhaustive overview of Japan's current setup –meaning, apart from the institutions mentioned, there are several other government ministries and agencies that do play a significant role in various aspects of the cyber domain.

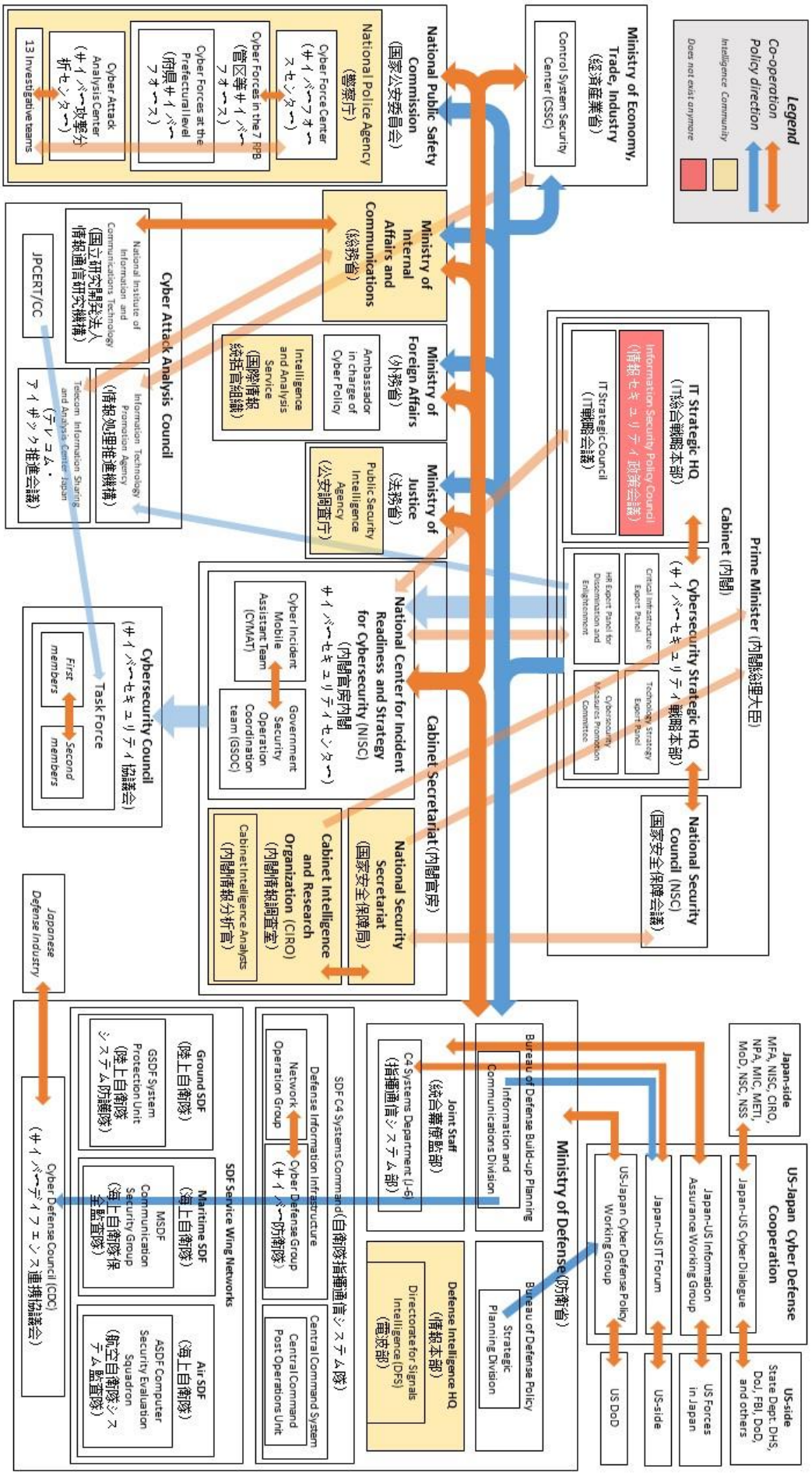
For example, the Financial Services Agency (FSA) (金融庁) is a key player in strengthening the cybersecurity posture across Japan's financial sector (FSA, 2019). On the one hand, it receives and collects incident reports from Japan's financial institutions, which it pushes up to the National Center for Incident Readiness and Strategy for Cybersecurity (NISC) for the purpose of accruing data and informing JPCERT/CC and others (FSA 2015, p. 5). On the other hand, the FSA also receives early warning information from NISC, which it disseminates to the financial institutions as needed, as well as informs the relevant CEPTOAR (Capability for Engineering of Protection, Technical Operation, Analysis and Response) which in turn conducts its own analysis to alert the financial sector.[12]

In the area of cyber defense and cybercrime, the Ministry of Land, Infrastructure, Transport, and Tourism (国土交通省) – which oversees the Japan Coast Guard (海上保安庁) – is often neglected. While the Japan Coast Guard monitors and maintains its own networks through its internal Information and Communication Division (情報通信課), it also conducts forensic investigations of mobile phones, navigational instruments, and radio transmissions, to investigate maritime crimes (JCG, n.d.).

Note: Japan's cybersecurity and defense posture are deeply intertwined with the country's intelligence community. This means that the historical fragmentation and stovepiping, which has been a feature of Japan's intelligence community since 1945, plays a significant factor in how today's cyber-relevant organizations are functioning. Samuels for example notes that "as late as 2012, […] CIRO's [Cabinet Intelligence and Research Organization] budget was only 20 million USD, and some one hundred of its core staff of 170 persons had been seconded from (and presumably had career-based loyalties to) other ministries and agencies, including forty from the [National Police Agency] alone" (Samuels 2019, p. 178).

[11] Note: Currently, there are no open sources available that could provide insights into the cyber-related EDD discussions.

[12] For a list of all 19 CEPTOARs in existence see: NISC. 2019. 'セプター特性把握マップ.'


Legend
Co-operation
Policy direction
Intelligence Community
Does not exist anymore
Prime Minister (内閣総理大臣)
Cabinet (内閣)
IT Strategic HQ (IT総合戦略本部)
Information Security Policy Council (情報セキュリティ政策会議)
IT Strategic Council (IT戦略会議)
Cybersecurity Strategic HQ (サイバーセキュリティ戦略本部)
Critical Infrastructure Expert Panel
Technology Strategy Expert Panel
HR Expert Panel for Dissemination and Enlightenment
Cybersecurity Measures Promotion Committee
National Security Council (NSC) (国家安全保障会議)
Cabinet Secretariat (内閣官房)
National Center for Incident Readiness and Strategy for Cybersecurity (NISC) (内閣官房内閣サイバーセキュリティセンター)
Cyber Incident Mobile Assistant Team (CYMAT)
Government Security Operation Coordination team (GSOC)
National Security Secretariat (国家安全保障局)
Cabinet Intelligence and Research Organization (CIRO) (内閣情報調査室)
Cabinet Intelligence Analysts (内閣情報分析官)
Ministry of Economy, Trade, Industry (経済産業省)
Control System Security Center (CSSC)
National Public Safety Commission (国家公安委員会)
National Police Agency (警察庁)
Cyber Force Center (サイバーフォース センター)
Cyber Forces in the 7 RPB (管区等サイバーフォース)
Cyber Forces at the Prefectural level (府県サイバーフォース)
Cyber Attack Analysis Center (サイバー攻撃分析センター)
13 Investigative teams
Ministry of Internal Affairs and Communications (総務省)
Ministry of Foreign Affairs (外務省)
Ambassador in charge of Cyber Policy
Intelligence and Analysis Service (国際情報統括官組織)
Ministry of Justice (法務省)
Public Security Intelligence Agency (公安調査庁)
Cyber Attack Analysis Council
National Institute of Information and Communications Technology (国立研究開発法人情報通信研究機構)
Information Technology Promotion Agency (情報処理推進機構)
Telecom Information Sharing and Analysis Center Japan (テレコム・アイザック推進会議)
JPCERT/CC
Cybersecurity Council (サイバーセキュリティ協議会)
Task Force
First members
Second members
Japanese Defense Industry
Japan-side
MFA, NISC, CIRO, NPA, MIC, METI, MoD, NSC, NSS
US-Japan Cyber Defense Cooperation
Japan-US Cyber Dialogue
Japan-US Information Assurance Working Group
Japan-US IT Forum
US-Japan Cyber Defense Policy Working Group
US-side
State Dept. DHS, DoJ, FBI, DoD, and others
US Forces in Japan
US-side
US DoD
Ministry of Defense (防衛省)
Bureau of Defense Build-up Planning
Information and Communications Division
Bureau of Defense Policy
Strategic Planning Division
Joint Staff (統合幕僚監部)
C4 Systems Department (J-6) (指揮通信システム部)
Defense Intelligence HQ (情報本部)
Directorate for Signals Intelligence (DFS) (電波部)
SDF C4 Systems Command (自衛隊指揮通信システム隊)
Defense Information Infrastructure
Network Operation Group
Cyber Defense Group (サイバー防衛隊)
Central Command System
Central Command Post Operations Unit
SDF Service Wing Networks
Ground SDF (陸上自衛隊)
GSDF System Protection Unit (陸上自衛隊システム防護隊)
Maritime SDF (海上自衛隊)
MSDF Communication Security Group (海上自衛隊保全監査隊)
Air SDF (海上自衛隊)
ASDF Computer Security Evaluation Squadron (航空自衛隊システム監査隊)
Cyber Defense Council (CDC) (サイバーディフェンス連携協議会)

5.1 The Cabinet (内閣)

IT Strategic Headquarters (IT総合戦略本部)
Based on the "Basic Act on the Formation of an Advanced Information and Telecommunications Network Society" of December 2000, the IT Strategic Headquarters was officially established within the Cabinet Office on 6 January 2001.[13] According to Article 25 of the Basic Act, the Headquarters purpose is to "swiftly and thoroughly pursu[e] strategies to form an advanced information and telecommunications network society" (Japanese Government, 2000). Organizationally, the Prime Minister of Japan serves as the Director-General of the IT Strategic Headquarters, and the Vice Director-General is appointed from among the Ministers of State. Members of the IT Strategic Headquarters include all Ministers of State as well as individuals with distinguished insights appointed by the Prime Minister. At its founding, the Headquarters encompassed more than 22 members (Kantei, n.d. 'Members').[14] As of 7 June 2019, the number has grown to over 29 (Kantei. 2019).

IT Strategic Council (IT戦略会議)
The IT Security Council was founded as part of the IT Strategic Headquarters. Its mission is to help "combine the forces of the public and private sectors and to undertake strategic, focused deliberations for the purpose of enabling all Japanese citizens to enjoy the benefits of the IT revolution and developing Japan into an internationally competitive 'nation built on IT'" (Kantei. 2000). Thus, while the IT Strategic Headquarters is primarily composed of government officials, the IT Strategic Council comprises only private-sector representatives. At its founding, the Council encompassed 20 members, ranging from the CEO of Sony and the President of the Toyota Motor Corporation, to the Chairman of the Board of IBM Japan and Professors from Keio University and the University of Tokyo (Kantei. n.d. 'Members').

Note: It is unclear to this author whether the IT Strategic Council still exists or whether its members have been partially absorbed into the IT Strategic Headquarters.

Information Security Policy Council (ISPC)
(情報セキュリティ政策会議) (2005-2015)
On 30 May 2005, the Prime Minister of Japan established the Information Security Policy Council (ISPC) within the IT Strategic Headquarters (NISC, 2005). The Council was chaired by the Chief Cabinet Secretary and its members encompassed: five ministers (MIC, MOFA, METI, MoD, and the Minister in charge of IT Policy), the Chairman of the National Public Safety Commission, as well as seven subject matter experts. The ISPC also oversaw four policy committees: the Critical Infrastructure Special Council, the Technological Strategy Special Committee, the Human Resource Expert Committee for Dissemination and Enlightenment, and the Information Security Measures Promotion Committee (Kawaguchi 2015, p. 5). In conjunction with the IT Strategic Headquarters, the ISPC's mission was to help formulate Japan's information security strategies. Most notably, the ISPC was responsible for publishing the 'Secure Japan' strategies (2006-2009), 'Information Security' strategies (2010-2012), and the nation's first 'Cybersecurity Strategy' (2013). Following the enactment of 'The Basic Act on Cybersecurity' in November 2014, the activities of the ISPC were transferred from the IT Strategic HQ to the Cybersecurity Strategic HQ on February 10, 2015 (NISC, 2015).

Cybersecurity Strategic Headquarters
(サイバーセキュリティ戦略本部)
In November 2014, the "Basic Act on Cybersecurity" outlined the establishment of a Cybersecurity Strategic Headquarters within the Cabinet. In January 2015, the Headquarter was created and is chaired by the Chief Cabinet Secretary. Its members include the Chairman of the National Public Safety Commission (law enforcement), the Minister for Internal Affairs and Communication, the Minister of Foreign Affairs, the Minister of Economy, Trade, and Industry, the Minister of Defense, and the Minister in charge of Information Technology policy. Additionally, seven experts are invited to the meetings. The mission of the Cybersecurity Strategic HQ encompasses four functions: (a) preparing Japan's Cybersecurity Strategy and promoting its implementation, (b) establishing cybersecurity standards and evaluation measures for government agencies, (c) evaluating response mechanisms, including fact-finding activities to determine the cause of an incident, and (d) engaging in research and the deliberation on program proposals, as well as establishing cross-governmental plans, budget, guidelines and carrying out overall coordination (Japanese Government 2014, Article 25(1)). Within the Cybersecurity Strategic Headquarters there are also three expert panels and one committee: the Critical Infrastructure Expert Panel, the Technological Strategy Expert Panel, the Human Resources Expert Panel for Dissemination and Enlightenment, and the Cybersecurity Measures Promotion Committee.
The Headquarters closely cooperates with the National Security Council and the IT Strategic Headquarters. The NISC serves as the Cybersecurity Strategic Headquarters' operational agency.

[13] Note: The Cabinet's decision to establish the IT Strategy Headquarters was already taken on July 7, 2000. See: Kantei. n.d. 'IT Strategic Headquarters.'

[14] Note: Deputy Chief Cabinet Secretaries (Parliamentary and Administrative) also attend the Headquarters meetings. See: Kantei. n.d. 'Establishment of the IT Strategy Headquarters.'

National Security Council (NSC)
(国家安全保障会議)
The Japanese National Security Council was established on 4 December 2013, after almost a year of deliberations to define and outline its jurisdiction, its use and policy judgement of intelligence, and overall purpose and form (MoD 2014a, p. 125). Foreign policy and defense experts have deemed the creation of the NSC "the most ambitious reorganization of Japan's foreign and security policy apparatus since the end of World War II" (Liff, 2018). According to the MoD, the NSC "functions as the control tower of [Japan's] foreign and defense policies," while MOFA defines it as "a forum which will undertake strategic discussions on various national security issues on a regular basis and as necessary under the Prime Minister with a strong political leadership" (MoD 2014a, p. 125; MOFA, 2016). Adam Liff at Brookings additionally notes that the NSC also serves "longer-term efforts by Japan's leaders to expand and strengthen the 'prime ministerial executive' at the expense of its historically powerful bureaucracy" (Liff, 2018). Two weeks after the Council's creation, the Japanese government approved Japan's first ever National Security Strategy, the National Defense Program Guidelines 2013, and the Medium-Term Defense Program 2013 (MoD 2014a, p. 132).

Note: The NSC's work is supported by the National Security Secretariat (NSS) within the Cabinet Secretariat.

5.2 The Cabinet Secretariat (内閣官房)

National Center for Incident Readiness and Strategy for Cybersecurity (NISC)
(内閣官房内閣サイバーセキュリティセンター)
On 25 April 2005, the IT Strategic Headquarters created the then National Information Security Center (NISC) within the Cabinet Secretariat. NISC functioned as the Secretariat for the Information Security Policy Council (ISPC) until the ISPC's was absorbed into the Cybersecurity Strategic Headquarters in January 2015. Together with this move, the National Information Security Center was renamed into the National Center for Incident Readiness and Strategy for Cybersecurity (NISC). The NISC is essentially responsible for the Cybersecurity Strategic Headquarters' ground game. Meaning it: (a) develops the baseline for fundamental strategies, (b) establishes information security measures for government agencies, (c) develops response capabilities, (d) analyzes and exercises critical infrastructure information protection, and (e) defines and promotes international relationships (NISC 2007, p. 3). To fulfill its missions, NISC closely cooperates with all relevant ministries and agencies.

Cybersecurity Council (サイバーセキュリティ協議会)
In preparation for the 2021 Tokyo Olympics and Paralympics, the "Basic Act on Cybersecurity" was amended in December 2018, to allow for the creation of the Cybersecurity Council under the auspices of NISC and JPCERT/CC (NISC 2020, p. 3). In April 2019, the Council was formed with the objective of further strengthening cooperation and information sharing between national government agencies, local governments, critical information infrastructure operators, information security companies, and educational and research institutions.
Designed as a complimentary element to the already wide range of existing information sharing frameworks, the Council largely relies on a Task Force – consisting of a small number of trusted security vendors and other specialized research organizations – to voluntarily analyze threat information and design countermeasures. To guide its workflow, the Task Force is divided into a two-tier hierarchical structure (ibid. p. 2). The first-tier organizations analyze the raw threat intelligence and design countermeasures. The second-tier organizations provide constant feedback on the accuracy of the countermeasures developed. The Task Force is specifically set up to prevent free-riding and encourage a give-and-take attitude between its members. As such, member can be kicked out.
JPCERT/CC serves as the coordinating node between the Task Force and the businesses and organizations that feed threat intelligence into the process (ibid. p. 17).

Note: It is highly likely that government agencies also feed information to the Task Force. Also, in principle, foreign corporations cannot participate in the Task Force, except for those that have been specially approved or achieved a high level of trust over the years (ibid. p. 17).

The countermeasure product coming out of the Task Force is subsequently fed to the Cybersecurity Council (the general members) for wider dissemination and implementation. In the Council's first recruitment stage, 91 members were accepted (ibid. p. 3). In the second round, 155 representatives gained membership. The third round commenced between 10-27 March 2020, and resulted in the acceptance of an overall 255 representatives (NISC, n.d. 'サイバーセキュリティ協議会').

Note: The work of the Council is not limited to threats against the 2021 Tokyo Olympics and Paralympics. According to NISC, the Task Force also contributed to securing the G20 summit in Osaka in June 2019 – only one month after the Council was officially created (NISC 2020, p. 7).

Government Security Operation Coordination team (GSOC)
The GSOC is one of NISC's operational capabilities that was created back in April 2008, in order to monitor and respond to cyberattacks against government ministries and agencies (NISC, 2012; ISPC 2013a, footnote 83). While there is little open source information available on GSOC's internal structure, it is highly likely that – similar to other SOCs – GSOC is divided into a network security monitoring team, a threat intelligence team, and an incident response team (Barrette, 2016).

Note: What remains unclear to this author is whether the GSOC is only responsible for the government's unclassified networks or also has an active role to play when classified government networks are affected.

Cyber Incident Mobile Assistant Team (CYMAT)
CYMAT was established on 29 June 2012, and serves as NISC's field unit, able to deploy to incident locations (NISC, 2012). Then Chief Cabinet Secretary Osamu Fujimura noted that CYMAT's first mission was to work on the damage caused by the hacktivist group Anonymous (SSRC, 2012).[15] According to Japan's 2013 Cybersecurity Strategy, CYMAT "provides technical support and advice related to preventing spread of damages, recovery, cause investigation and recurrence prevention in the event of cyber-attacks against ministries or other agencies under the National Information Security Center director who is the government CISO" (ISPC 2013a, footnote 84). Initially staffed with personnel contingent of 26, hailing from various ministries and agencies, CYMAT currently "consists of approximately 80 members and trainees."[16] According to NISC, "when an incident occurs or is deemed to be imminent, [a team of several persons is] dispatched on request of concerned ministries and government agencies. Details of their activities are not made public."[17] According to the MoD, personnel from the Bureau of Defense Policy (防衛政策局), the Bureau of Defence Buildup Planning (整備計画), and the Acquisition, Technology & Logistics Agency (防衛装備庁) are also regularly dispatched to CYMAT since 2015 (MoD. n.d., p. 13).

National Security Secretariat (NSS) (国家安全保障局)
The National Security Secretariat was established on 7 January 2014 (CAS, n.d.). It serves as the gatekeeper for the NSC and is responsible for "collecting and assessing raw intelligence from across the government on topics assigned by the NSC" (Samuels 2019, p. 212). According to the MoD, the NSS is also "dedicated to the planning and coordination of basic direction and important matters of foreign and defense policies concerning Japan's national security, using its general coordination authority" (MoD 2014a, 125). Overall, the logic for standing up the NSS is to gather intelligence for the Prime Minister, encourage intelligence sharing across the whole of government, and to break up the intelligence silos within the various ministries (Samuels 2019, p. 212).

Note: Samuels states that, in the case of the North Korean hack against Sony in November 2014, the US provided intelligence reports directly to the NSS (Samuels 2019, p. 215).

Cabinet Intelligence and Research Organization (CIRO) (内閣情報調査室)
The Cabinet Research Office was formed in 1952 as the only government body in Japan's first post-occupation administration that had an officially acknowledged foreign intelligence function (CIA, 1995). In 1986, it was renamed into the Cabinet Intelligence and Research Organization (CIRO). In 2012, it encompasses 70 full-time staff and another 100 from other agencies and ministries. Overall, CIRO serves as an information hub that primarily collects, processes, and interprets all source intelligence (Aranguren 2016, p. 35). In regard to the cyber domain, CIRO primarily cooperates with – and might to some degree even oversee the work of – the C4 Systems Department within the SDF Joint Staff and the Directorate for Signals Intelligence within the Defense Intelligence Headquarters (Gallagher, 2018). It also has close ties to the NPA and the Public Security Intelligence Agency on cyber-related domestic matters. CIRO informs the Cabinet through the NSC/NSS, and in sensitive circumstance – for example in the case of information that no ministry has an incentive to report – it can even bypass the NSS (Samuels 2019, p. 216). Given its role and standing in the cyber domain, CIRO is a key player in the Japan-US Cyber Dialogue within the US-Japan Cyber Cooperation framework.[18]

Note: CIRO's annual reports between 2017 and 2019 mention the need to increase "counter-cyber intelligence" (カウンター・サイバーインテリジェンス).[19] The usage of the term is particularly interesting given that its 2016 report merely mentions cyberspace once (サイバー空間), the 2015 report does not mention cyber

[15] In June 2012, Anonymous commenced 'Operation Japan' in reaction to the government's introduction of a new copyright law. Actions included DDoS attacks and defacements of numerous government websites. Curiously, one week after the onslaught, Anons in Japan organized a one-hour picking up litter campaign in Tokyo's Shibuya district to protest the stricter punishments for online piracy included in the law. This event marked the first ever physical public display of Anons in Japan. See: Phneah, 2012 & Phys.org, 2012

[16] January 21, 2020, NISC email response to research inquiry on CYMAT

[17] January 21, 2020, NISC email response to research inquiry on CYMAT

[18] This stands in stark contrast to the dynamics in real space, where the National Police Agency and the Public Security Intelligence Agency serve as the main points-of-contact for foreign intelligence services.

[19] See: CIRO 2019, p. 2; CIRO 2018, p. 2; CIRO 2017, p. 1

at all, and the 2014 report refers to cyber intelligence (サイバーインテリジェンス) once. Furthermore, the term "counter-cyber intelligence" is rarely used in other Japanese government documents. The only open source definition available seems to be a presentation by the Cabinet Secretariat in 2010 – which defines it as "protecting confidential information" (CAS 2010, p. 13). According to the 2010 presentation, the Counter Intelligence Center will be tasked with "analyzing information from ministries, government agencies, and foreign countries" to obtain and analyze information on foreign attackers and the characteristics of the methods used and clarify the intentions of the cyberattacks and adversarial cyber intelligence collection efforts over the medium and long term (ibid. p. 13). It is unclear to this author whether the Counter Intelligence Center referred to in the 2010 presentation is CIRO's Counter Intelligence Center (カウンターインテリジェンスセンター), and if so whether CIRO's definition of counter-cyber intelligence has evolved over the last decade. What is important to note, is that counter-cyber intelligence seems to be more broadly defined than mere cyber intelligence and has a distinct political connotation to it.

5.3 Ministry of Defense (防衛省)

On 1 July 1954, Japan's Defense Agency was established and the Ground, Maritime, and Air Self-Defense Forces were inaugurated (MoD. n.d. 'About Ministry'). On 9 January 2007 the Defense Agency was upgraded into the Ministry of Defense (Yoshida, 2007).

Bureau of Defense Build-up Planning (整備計画局)
On 1 October 2013, the Bureau of Defense Build-up and Planning was created to "enhance defense capabilities build-up functions" (MoD, 2015b). The Bureau is responsible for "basic policy related to structures, quotas of the personnel, organization, restructuring, equipment and deployment of the Self-Defense Forces (SDF); maintenance and management of the information system; basic policy related to communication including command communication; basic policy related to supervision of electric waves to be used; planning of basic policy related to acquisition, maintenance and management of SDF facilities; approval, improvement and management of construction plan, bidding and contract; basic policy related to management of national property; management of acquisition plan and construction of facilities and areas for use by the U.S. Forces in Japan; setting construction standards and technological research on facility construction" (CAS 2017, p. 105).

Information and Communications Division
(情報通信課)
The Information and Communication Division is part of the Bureau of Defense Build-up Planning and is responsible for matters relating to the maintenance and management of the MoD's information system, command and communication, and the supervision of radio waves used by the Ministry (e-Gov, n.d.). Given its role, it close cooperates with the Cyber Defense Council – to engage with Japan's defense industry – and together with the SDF's C4 Systems Department, the Division is a key player in the Japan-US IT Forum. Additionally, the Division also sends its officials abroad. In December 2017 for example, one official from the Information and Communications Division was part of a seven-member delegation to Vietnam. According to the MoD, this was "the first time for the JMOD to provide support in this field and contributed to advancing the capability of cyber security personnel in the Vietnam People's Army through exchanging ideas and sharing experiences" (MoD, n.d. 'Cyber Security').

Bureau of Defense Policy (防衛政策局)
For the period in which the Defense Agency operated as a stand-alone entity, the Bureau of Defense Policy was considered one of the centers of power and instrument of exercising civilian control over the Defense Agency. Therefore, it was often headed by an official from another ministry. The upgrade of the agency into the MoD halted this "interference". According to a 2017 Cabinet Office document, the Bureau is responsible for the following affairs: "basic policy related to defense and security; basic policy related to operations of the Self-Defense Forces; collection and management of information required for functions; information security in the field of defense and security; basic policy related to unit training of the Self-Defense Forces.; management and administration of the National Institute for Defense Studies; management and administration of the Defense Intelligence Headquarters; foreign relations" (CAS 2017, p. 104).

Strategic Planning Division (戦略企画課)
On 1 October 2013, the Strategic Planning Division was established within the Bureau of Defense Policy in order to "strengthen policy planning functions" (MoD, 2015b). The Strategic Planning Division is – in conjunction with other elements within the Ministry of Defense – leading the talks in the US-Japan Cyber Defense Policy Working Group. Similarly, the Strategic Planning Division is also directly engaged in talks with other partners around the world, including NATO. In October 2019 for example, the Director of the Strategic Planning Division met with the Head of the Cyber Defense Section at NATO Headquarters to "compare[d] notes on current efforts by NATO and Japan to become more resilient to cyber attacks. Another focus was on working together to

support a norms-based, predictable, and secure cyberspace" (NATO, 2019).

Joint Staff Office (統合幕僚監部)
The Joint Staff Office was created on 27 March 2006 in an effort to better integrate the operations of the three SDF service wings (Yoshida, 2006).

C4 Systems Department (J-6) (指揮通信システム部)
While there is no public information available on the activities of the C4 Systems Department, it is highly likely that the J-6 in the Japanese Joint Staff functions similarly to the J-6 in the US Joint Chiefs of Staff. If this is true, then the J-6 "represents the Joint Warfighter in support of the command, control, communications, and computers/cyber (C4) requirements validation and capability development processes while ensuring joint interoperability. To further this effort, the J-6 promulgates guidance and provides functional expertise to the Chairman in order to shape the joint information environment" (US JCS, n.d.).

Note: From the limited sources available, it is unclear whether the J-6 has any capabilities to become directly involved in "analyzing malware and developing countermeasures – such as firewalls – to prevent hacks of Japanese computer systems" – as asserted by The Intercept in 2018 (Gallagher, 2018).

Defense Intelligence Headquarters (DIH) (情報本部)
Established on 20 January 1997, the DIH is the MoD's central and largest intelligence agency (MoD, n.d. 'About Ministry'). It is broadly modeled on the US Defense Intelligence Agency. This means the DIH was created to consolidate the service-based intelligence assets and thereby provide military intelligence to warfighters, defense policymakers, and force planners within the MoD.

Directorate for Signals Intelligence (DFS) (電波部)
The DFS is the NSA/CSS's sister organization in Japan and primarily focuses on the electromagnetic spectrum to capture, collect, and analyze signal intelligence. According to the DIH's 2020 staff recruitment brochure, the DFS is "Japan's only radio information agency that processes and analyzes various radio waves collected by communication stations. We also conduct technical research and development of equipment necessary for collection, investigation and analysis of various radio waves" (DIH 2019, p. 12). Given the overlap between cyberspace and the electromagnetic spectrum (ex. Wi-Fi signals, satellite uplinks, mobile phone data transfers etc.), it is unclear to this author how far the DFS is able to reach outside of Japan to capture foreign signals, and to what degree its intelligence collection informs Japanese defensive efforts in cyberspace. The Intercept's 2018 release of several top-secret documents on the DFS' history and cooperation with the NSA back in 2013 provides little insight into the directorate's activities and mindset.[20]

SDF C4 Systems Command
(自衛隊指揮通信システム隊)
In 2008, the responsibility to maintain and manage the Central Command System (中央システム) (CCS) and the Defense Information Infrastructure (防衛情報通信基盤) (DII) moved from the Joint Staff Office to the SDF C4 Systems Command. The CCS and DII form the foundation of the "joint operations structure, communication of accurate commands, and prompt information sharing between the units in" the Ground, Maritime, and Air SDF(MoD 2014b, 131). The DII is the common network connecting major garrisons and bases of the MoD and the SDF. It is separated into an open system – which connects to the Internet – and a closed system – which handles classified data and is in principle not connected to the outside (MoD 2001, p. 6-7). The CCS meanwhile "supports [the] Defense Minister's command and supervision, [and] collecting intelligence by connecting with the primary command systems of each SDF Staff Office and other systems" (MoD 2014b, p. 131). The C4 Systems Command oversees three units: the Network Operation Group (ネットワーク運用隊) – which is in charge of maintaining and operating the DII; the Cyber Defense Group (サイバー防衛隊) – which is in charge of protecting the DII; and the Central Command Post Operations Unit (中央指揮所運営隊/中央システム通信隊) – which is responsible for the management and operation of the Central Command System.

Cyber Defense Group (サイバー防衛隊)
The Cyber Defense Group is a SDF joint unit which was created on 16 May 2013, with an initial staff of 90 (Nikkei, 2013). Drawn from the three SDF service wings, the Group is subordinate to the SDF C4 Systems Command and serves as the Computer Emergency Response Team (CERT) for the Defense Information Infrastructure (DII) – the SDF's joint network. According to the MoD's budget for FY2019, the Group is set to grow from 150 to 220 personnel (MoD 2019b, p. 5). In FY2020, the request is to increase that number by 70 to reach 290 staff (MoD 2020, p. 6). As outlined in the MoD's Medium-Term Defense Program (FY 2019 - FY 2023), the vision for the Cyber Defense Group is to grow to a squadron over time (~500 personnel), in order to "fundamentally strengthen cyber defense capabilities, including capability to disrupt, in the event of attack against Japan, opponent's use of cyberspace for the attack as well as to conduct persistent monitoring of SDF's information and communications networks" (MoD 2018b, p. 3).

[20] See: DIH 2013 & NSA 2013

Note: The Group's tentative name was Cyber Defense unit (small u). The official English name is Cyber Defense Group.

Ground (GSDF) System Protection Unit
(陸上自衛隊システム防護隊)
The System Protection Unit (SPU) was established in 2001 and functions as the Computer Emergency Response Team of the Japanese Ground Self-Defense Forces. Currently, subordinate to the GSDF C5 Command (システム通信団) headquartered at Ichigaya garrison, the SPU is set to be reorganized in FY2020 to fit into the newly established Ground Component Command (陸上総隊).[21] According to the MoD's draft budget request for FY2020, a new Cyber Protection Unit (preliminarily called 陸上自衛隊サイバー防護隊) will be established within the GSDF and will "serve under the System and Signal Brigade which belongs to the Ground Component Command (陸上総隊) in order to create a posture to effectively protect network systems of GSDF" (MoD 2020, p. 6; MoD 2018c, p. 1). The GSDF's new Cyber Protection Unit is set to encompass a staff of approximately 140 personnel. One of the unit's publicly known milestones dates to 22 August 2019, when the SPU organized – for the first time ever – a joint US-Japan Capture the Flag exercise called Cyber Thunder. 12 teams competed against each other – six GSDF teams from across Japan, and six teams from the US Army Cyber School (Augusta, Georgia) (MoD, 2019c; JWing, 2019).

Maritime (MSDF) Communication Security Group
(海上自衛隊保全監査隊)
The Communication Security Group (CSG) is the Computer Emergency Response Team of the Japanese Maritime Self-Defense Force. The unit was established in March 2002 as a result of a broad reorganization effort due to the newly created MSDF Systems Communication Command (システム通信隊). At its founding, the size of the CSG was defined as "分隊１以上," meaning one squadron or more (MoD 2002, p. 3). According to the budget request for FY2020, the CSG is set to encompass a staff of 130 personnel (MoD 2020, p. 6).

Air (ASDF) Computer Security Evaluation Squadron
(航空自衛隊システム監査隊)
The Computer Security Evaluation Squadron (CSES) is the Computer Emergency Response Team of the Japanese Air Self-Defense Force. It was stood up on 8 May 2000, after numerous Japanese websites were defaced in the month of January by Chinese nationalistic hacktivists (Watts, 2000). Organizationally, the squadron is subordinate to the Air Communications and Systems Wing (航空システム通信隊) located at Ichigaya (ACSW, n.d.). According to the Systems Wing website, the CSES is responsible for around the clock protection of the ASDF's information systems from cyberattacks (ACSW, n.d.). The MoD's budget request for FY2020 projects the CSES to encompass a staff of 100 personnel (MoD 2020, p. 6).

Cyber Defense Council (CDC)
(サイバーディフェンス連携協議会)
The MoD established the Cyber Defense Council on 12 July 2013, in cooperation with ten initial defense industry partners (Security Next, 2013). The CDC functions as the primary vehicle for the MoD to strengthen the Japanese defense industry's ability to respond to a cyberattack. As such, the CDC encourages information sharing and mutual cooperation between the CDC members and serves as a neutral hub for information that companies deem too sensitive to share directly with each other (MoD 2013a, p. 2). The CDC also conducts joint trainings between the MoD, SDF, and the defense industry to exercise system resilience and restoring defense industry functions amidst a cyberattack (MoD 2013a, p. 2-3).

5.4 US-Japan Cyber Defense Cooperation

Japan-US Cyber Dialogue (日米サイバー対話)
The Japan-US Cyber Dialogue is a consultation mechanism led by the Ministry of Foreign Affairs on the Japanese side and the State Department on the US side. The first US-Japan Cyber Dialogue was held during 9-10 May 2013 in Tokyo. Participants included, on the Japanese side: Japan's Ambassador in charge of Cyber Policy, senior officials from the Cabinet Secretariat, NISC, CIRO, NPA, MIC, METI, MoD, and the Information Technology Promotion Agency (IPA). On the US side, participants included: The US Secretary of State's Coordinator for Cyber Issues, senior officials from the Department of State, Department of Homeland Security (DHS), Department of Justice (DoJ), and the Department of Defense (DoD). According to the joint press release, the discussions involved consultations "for exchanging cyber threat information, aligning international cyber policies, comparing national cyber strategies, cooperating on planning and efforts to protect critical infrastructure, and discussing the cooperation on cyber areas in national defense and security policy" (MOFA, 2013). The 7th and latest Japan-US Cyber Dialogue occurred on 11 October 2019 in Tokyo. The topics discussed included "situational awareness, domestic cyber policy, cooperation in international fora, and capacity building" (MOFA, 2019).

[21] Note: The GSDF's Ground Component Command was launched on 28 March 2017. Its creation is part of the biggest restructuring of the Japanese ground forces since their formation in 1954 (Burke, 2018).

Japan-US Information Assurance Working Group (IAWG) (日米情報保証実務者定期会議/協議)
The IAWG was created after the Japan-US Defense Summit in 2006. According to NISC it has met 14 times between 2006 and 2014 and serves as a regular working-level meeting to discuss cooperation on information assurance and coping with cyberattacks (Director/Colonel level) (NISC 2014, p. 14). Although there is very little information as to who participated in the IAWG, open sources note that Scott Jarkoff, former Chief of the Cyber Security Department of the US Navy, served as the "U.S. Co-Chair of the DoD-CIO Information Assurance Working Group (IAWG) between U.S. and Japan" (Jarkoff, n.d.). And according to Vosse, the IAWG was designed to "deepen consultations between the SDF Joint Staff and US Forces in Japan" (Vosse 2019, p. 14).

Japan-US IT Forum (日米ITフォーラム)
The Japan-US IT Forum was created in response to the Japan-US Defense Summit Meeting in September 2000 and an agreement signed in 2002 (NISC 2014, p. 14; MoD, 2015c). On 14 March 2016, the IT Forum met for the 12th time (MoD 2016).[22] The Japanese delegation included the Director General of the Bureau of Defense Build-up Planning, representatives from various internal divisions (including the Information and Communications Division), the Joint Staff's C4 Systems Department, the SDF's three service wings, and other internal IT staff. From the US side, participants included: the DoD Chief Information Officer, representatives from the Office of the Secretary of Defense, the US Forces in Japan, as well as other IT staff (MoD 2015c; MoD 2016). NISC notes that the IT Forum revolves around an open exchange between practitioners on a wide range of information and communication measures and technology trends within the MoD and DoD (NISC 2014, p. 14). According to the 2018 Defense White Paper, the Japanese MoD also held IT Forums with the defense authorities in Singapore, Vietnam, and Indonesia to "exchange views on initiatives in the information communications area including cybersecurity and current trends in technology" (MoD 2018d, p. 334).

US-Japan Cyber Defense Policy Working Group (CDPWG) (日米サイバー防衛政策ワーキンググループ)
Based on an Agreement reached at the Japan-US Defense Minister's Meeting in August 2013, the US-Japan Cyber Defense Policy Working Group (CDPWG) had its first meeting on 21 January 2014 (MoD, n.d. 'CDPWG'). According to the MoD, the Working Group members included – on the Japanese-side – the Deputy Director of the Bureau of Defense Policy as chair, as well as members from the Bureau of Defense Policy, the Operational Planning Bureau, and the Joint Staff Office (MoD 2013b). The US was represented by the Assistant Secretary of Defense for Cyber Policy, the Assistant Secretary of Defense for East Asia, the Joint Chiefs of Staff, US Indo-Pacific Command, and the US Forces in Japan (ibid.). The core agenda items for the first meeting were: cyber defense policy, information sharing, cyber defense organizations, training exercises, recruitment and education, and the cooperation with other ministries and the private sector (ibid.). The CDPWG had its 7th and latest meeting on 23 October 2019 (MoD, 2019d).

5.5 National Public Safety Commission
(国家公安委員会)

The National Public Safety Commission was established in 1947 and consists of six members. The Commission chair holds the rank of a Minister of State and the five other members are appointed by the Prime Minister with the consent of both houses (NPSC, n.d. '概要'). The main mission of the Commission is to ensure the democratic administration and the political neutrality of Japan's police forces (Kantei, n.d. 'Government Offices'). As such, its current members include a politician, a diplomat, a corporate executive, a lawyer, a journalist, and a law professor (NPSC, n.d. '委員のプロフィール').[23] Similarly to the Financial Services Agency, the Commission is an external agency of the Cabinet Office (NPSC, n.d. '概要'). Overall, the Commission is responsible for the administrative supervision of the NPA. Meaning, it has the mandate to formulate basic policies and to oversee the operations of police forces, but it does not exercise direct command or control over daily operations.

Note: The Prime Minister is not empowered to exercise direct command or control over the Commission.[24]

National Policy Agency (NPA) (警察庁)
Disclaimer: The organigram on page 18 only displays – due to a lack of space – the cyber-relevant operational elements within the NPA's Info-Communications Bureau. Other bureaus, such as the Security Bureau (Foreign Affairs and Intelligence Department) and the Criminal Affairs Bureau (Investigation Division) maintain their own specialized cyber-relevant units.

Geographically, the NPA is divided into seven regional police bureaus (RPB). Each of the seven RPBs maintains a Cyber Force (管区等サイバーフォース), e.g. a technical police unit responsible for defending against cyber

[22] Note: The MoD does not seem to have published any public notifications on the US-Japan IT Forum since 2016.

[23] Note: To ensure political neutrality, no more than two members may belong to the same political party. See: NPA 2018, p. 3

[24] This is also why in the organigram on page 18 of this report the NPSC is not placed within the Cabinet Office

incidents (2013: 220 personnel).[25] Each RPB Cyber Force oversees the Cyber Forces on their prefecture level (府県サイバーフォース). The centralized command hub connecting the seven RPB Cyber Forces is called the Cyber Force Center (サイバーフォースセンター) and is located in Tokyo (2013: 40 personnel).[26] The combined mission of the Cyber Forces is to (a) map the cyber threat landscape in Japan, (b) conduct preventative measures to mitigate the damage of cyber incidents, and (c) conduct emergency response activities, including collecting, analyzing, and preserving technical evidence (NISC, n.d. '警察', p. 1).

Note: The Tokyo Metropolitan Police and the Hokkaido Prefectural Police Headquarters are not part of the RPBs jurisdiction (NPA 2018, p. 6).

The Cyber Forces closely cooperate with the Cyber Attack Special Investigation Team (サイバー攻撃特別捜査隊). 13 investigative teams exist across Japan within various prefectural police departments (2013: 140 personnel) (SSRC, 2013). Their mission is to (a) collect information related to cyberattacks, (b) investigate cyberattacks (digital forensics), and (c) implement preventative measures in cooperation with the private sector (NISC, n.d. '警察', p. 1). The Cyber Attack Analysis Center (サイバー攻撃分析センター) (2013: 20 personnel), serves as the central information hub for the 13 investigative teams. On the prefecture level, the NPA has also stood up so called "Cyber Terrorism Countermeasure Councils" (サイバーテロ対策協議会) to facilitate direct cooperation with critical infrastructure providers through discussions, lectures, and demonstrations (NPA, n.d. 'サイバー攻撃に対する警察', p. 8). The Tokyo Metropolitan Police, for example, established its council on 23 October 2001, and has held 23 meetings so far, including coordinating public-private collaboration for the Tokyo 2021 Olympic and Paralympic Games (TMP, n.d. 'サイバーテロ対策協議会'). The NPA also conducts individual visits to critical infrastructure providers, runs exercises with them, and will directly contact a critical infrastructure provider by phone or email if information is uncovered on a potential future cyberattack (NISC, n.d. '警察', p. 2). The Tokyo Metropolitan Police additionally maintains a Cybercrime Countermeasures Council which facilitates the coordination and cooperation between the police and internet companies in cybercrime-related cases (TMP, n.d. 'サイバー犯罪対策協議会').

Note: In contrast to many other countries around the world, Japan's National Police is considered by many analysts the most powerful intelligence agency in Japan.

5.6 Ministry of Economy, Trade, and Industry (経済産業省)

The Ministry of International Trade and Industry (MITI) was formed on 25 May 1949 and tasked with the revival of Japan's industrial base economy. Through the implementation of numerous industrial policies, e.g. micro-level policy interventions, liberalization of capital, opening up new markets, and close cooperation between the public and private sector, MITI essentially guided Japan's economy to become the second largest in the world within a mere 19 years (1968). The economic system that MITI (1949-2001) and METI (2001-present) created over seven decades also has significance implications for the cyber domain. First, METI's policy mandate essentially spans across Japan's entire economy – meaning because cybersecurity plays a major role in getting the defensive mission right, METI is involved in every industrial sector. Second, METI maintains strong relations with the private sector based on its "hand-on approach" principle – which outlines that it is imperative to gather first-hand information through dialogue with business managers and engineers in the field. And third, historically, METI has exercised functions similar to an intelligence agency by dispatching officials to embassies, consulates, international organizations, and even Japanese corporations abroad (Samuels 2019, p. 178-179).

Control System Security Center (CSSC)
(技術研究組合制御システムセキュリティセンター)
The Control System Security Center was established on 6 March 2012. It functions as a non-profit mutual assistance organization, and was approved by METI in accordance with the "Research and Development Partnership Act". According to the CSSC website, the Center's mission is to "ensure the security of control systems of important infrastructure" [ICS and SCADA systems], conduct R&D, implement international standards, certification, promotion and security verification, and human resource development (CSSC, n.d.). One of CSSC's most prominent feature is that it has developed small-scale mock plants to "simulate electric power system, gas system, building automation, automaker, sewage treatment, smart community and chemical process automation" (ISPC 2013b, p. 13). These plants are used for hands-on simulation exercises. As of this writing, CSSC has 34 members, including major Japanese corporations, universities, and national research institutes (CSSC, n.d.).

[25] On personnel numbers see: Sbbit, 2013

[26] Note: The Cyber Force Center is also a member of FIRST (a global Forum of Incident Response and Security Teams), See: First, n.d.

5.7 Ministry of Internal Affairs and Communications (MIC)
(総務省)

In the cyber domain, the MIC is essentially responsible for Japan's communications sector. Meaning, its mission is to create robust and reliable networks, improve the skills and awareness of internet users, conduct research and development on countermeasures, engage in public-private partnerships and international cooperation, as well as safeguard and oversee the proper usage of personal data. To fulfil its mission, MIC currently supports four prominent projects:

PRACTICE (Proactive Response Against Cyberattacks Through International Collaborative Exchange)
(August 2011-present)
According to Katsunari Yoshioka, Associate Professor at Yokohama University, PRACTICE "focuses on tracking online activities of malware infected hosts like botnets by correlation analysis between cyber attacks observed by world-wide distributed sensors deployed at international collaborators and dynamic behaviors of individual malware samples closely and continuously monitored in the Internet-connected sandboxes. Characteristic behavior of malware, such as domain name resolutions and network scanning, are extracted and compared to reveal the relationship between the observed network attacks and malware samples being monitored in the sandboxes. Our final goal is to make proactive response by understanding the underlying structure of the online threats, estimating their scale, and grasping their trends" (Yoshioka, 2013).

ACTIVE (Advanced Cyber Threats response InitiatiVE)
(November 2013-present)
ACTIVE primarily revolves around setting up honeypots in close cooperation with ISPs and antivirus vendors (ICT-ISAC, n.d.). The information gained is used to remove malware from infected machines (warning emails & updating malware signatures), as well as prevent future malware infections (blacklisting command & control servers, blocking and taking down malicious websites). According to Fujitsu, the initiative successfully reduced the number of infected PCs by blocking a total of 100 million communications between the period of February 2016 to May 2017 (Fujitsu, 2017).

CYDER (CYber Defense Exercise with Recurrence)
(September 2013-present)
CYDER is a hands-on cyber defense exercise for IT personnel in government organizations, local governments, independent administrative agencies, and critical infrastructure providers. Its curriculum is divided into three stages (NICT, n.d., p. 16). First, trainees take an online training to understand the latest cyberattack trends, countermeasures, and gain incident-handling knowledge. Second, the trainees are divided into teams to gain general experience in practically handling incidents. This includes performing incident detection, reporting, locating and isolating problems, analysis, and checking damage conditions. Third, the trainees engage in group work to clarify policies and operational problems observed in the previous stage, and then discuss and consider appropriate countermeasures. As of FY2018, a combined 7929 individuals have participated in CYDER (NICT 2019, p. 2).

NOTICE (National Operation Towards IoT Clean Environment) (February 2019-present)
NOTICE was implemented in February 2019 to secure the 2021 Tokyo Olympics and Paralympics. Essentially, it is a two-stage project consisting of (a) a nation-wide awareness campaign on securing IoT devices, followed by (b) allowing the MIC and the National Institute of Information and Communications Technology (NICT) to run dictionary attacks against the millions of IoT devices in Japan. The goal is to "identify vulnerable devices, such as those with weak password settings, and provide the information of the devices to the telecommunications carriers. Then, the telecommunications carrier will identify the users of the devices and alert users to the problem" (MIC, 2019).

5.8 Cyber Attack Analysis Council
(サイバー攻撃解析協議会)

On 11 July 2012, METI and MIC established the Cyber Attack Analysis Council (CAAC). The CAAC encompasses METI's Information Technology Promotion Agency, MIC's National Institute of Information and Communications Technology, the Telecom Information Sharing and Analysis Center Japan (Telecom-ISAC Japan), and JPCERT/CC. The Council's mission is to "grasp the development of cyberattacks and provide the results to the relevant ministries, agencies and critical infrastructure operators" (MIC, 2012).

Information Technology Promotion Agency
(情報処理推進機構)
Since its creation in 2004, IPA has been implementing various IT initiatives under METI (IPA, n.d., p. 2). Therefore, IPA is often seen as a METI-affiliated agency. IPA's mission is to monitor and analyze the latest trends in IT and cutting-edge technologies, provide guidelines (ex. ensuring security and reliability of IoT devices), as well as implement information security measures and nurture IT talents and professionals (IPA, n.d., p. 3). Two of its most notable cybersecurity initiatives are: (a) the Japan-Cyber Security Information sharing Partnership (J-CSIP), which was established in cooperation with METI on 25 October 2011 (IPA, 2020), and (b) the Japan Cyber Rescue Advice Team (J-CRAT), which was created in cooperation with METI on 16 July 2014 (IPA, 2019).

In the J-CSIP context, IPA serves as an exchange hub for cyber incident information between the participating organizations (all sign non-disclosure agreements). IPA anonymizes the information, adds its own analysis, and then obtains approval from the information providers to share the gathered information with – for example JPCERT/CC. Between April to December 2019, IPA shared incident information 169 times with 262 organizations. By contrast, in 2012, IPA shared incident information 160 times with only 39 organizations. (IPA, 2020). In case of a major incident, IPA will directly inform METI – which in turn will collaborate with NISC.
J-CRAT on the other hand, serves as an open support desk for attacked organizations to get speedy analysis and quick advice to initiate countermeasure protocols and foster damage control. In 2019, J-CRAT conducted 221 consultations, handled 80 rescue support cases, and managed 18 on-site support visits (IPA, 2019). Private individuals and researchers can also contact J-CRAT.

National Institute of Information and Communications Technology
(国立研究開発法人情報通信研究機構)
NICT was established in April 2004, by merging the Communications Research Laboratory (旧通信総合研究所) and the Telecommunications Advancement Organization (旧通信・放送機構) (NICT, n.d. 'History'). According to its own website, NICT's mission is to promote "the full spectrum of research and development in ICT from basic to applied research with an integrated perspective, and thus promotes the advancement of Japan as an intellectual nation that leads the international community." To fulfill its mission NICT cooperates closely with the academic and business community in Japan, and research institutes overseas. Organizationally, NICT encompasses several research centers and institutes, ranging from the Applied Electromagnetic Research Institute and the Center for information and neural networks to the Cybersecurity Research Institute and the National Cyber Observation Center (NICT, n.d. 'Organization').

Japan Computer Emergency Response Team Coordination Center
In 1991, the Japanese Engineering & Planning Group/IP (JEPG/IP) was established with the goal of conducting technological studies and reviews for the smoother operation and stable advancement of the Internet in Japan (JPNIC, 2018). Spurred by the lessons learned from the Morris worm in 1988, JEPG/IP decided to create a security working group and an incident point-of-contact in 1992. Four years later, JPCERT/CC was officially launched as a private organization with the funding support of METI's predecessor MITI (Slayton & Clarke, 2019, p. 13). In 1998, JPCERT/CC became Japan's first CSIRT by joining the Forum of Incident Response and Security Teams (FIRST), and subsequently established close relations with newly emerging CSIRTs across the Asia-Pacific. In 2003, JPCERT/CC was incorporated and registered as a limited liability intermediate company. JPCERT/CC's mission encompasses incident response and analysis, streamlining vendor and CSIRT coordination, publishing security alerts and advisories, as well as conducting education and training.

Telecom Information Sharing and Analysis Center Japan
(テレコム・アイザック推進会議)
Telecom-ISAC Japan was established as a non-profit organization in July 2002 by MIC and seven of Japan's major domestic ISPs. Currently, its members encompass 20 companies ranging from NEC and NTT to Fujitsu, Hitachi, and Softbank. T-ISAC's activities include: managing 12 information sharing Working Groups, holding cyberattack exercises, and operating the critical infrastructure observation system. In cooperation with the MIC, T-ISAC also operates the "ACTIVE" initiative – which seeks to prevent and remove malware infections through rapid information sharing from honeypots – and participates in "PRACTICE" – a trial international malware detection and response system aimed at predicting cyberattacks (Koji, n.d., p. 9 & 16).

5.9 Ministry of Justice (法務省)

The Ministry of Justice has a broad scope of different tasks within the cyber domain, ranging from combatting cybercrime and fighting cyber terrorism (in close cooperation with the NPA), to raising awareness on human rights online and working on justice reforms to punish new cyber offenses. The case of Masato Nakatsuji is particularly informative to grasp the ongoing efforts by the Ministry of Justice to adapt to the 21st century. The story started when 24-year old Masato decided to spread a malware dubbed "Harada" on the peer-to-peer file sharing platform Winny. The malware displayed images of popular anime series Clannad while wiping mp3 and movie files from a victim's computer (Jacob, 2008). In 2008, Masato was arrested, charged with copyright infraction for using the anime images without permission, and received a 3-year suspended sentence. Masato was not charged for writing and disseminating malware, because at the time Japan had no law against malware creation and distribution (Humphries, 2008). While on probation, Masato was arrested again in 2010 after infecting 20,000 to 50,000 computers with the Ikatako malware. The malware was disguised as a music file, disseminated through Winny, and replaced files on a victim's machine with squid images. This time however, Masato was charged with property destruction – because it was impossible to retrieve the original computer files – and sentenced to two and a half years in prison (Geere, 2010). On 17 June 2011, the Japanese parliament approved the revised Cybercrime Law which specifically penalizes malware

creation and distribution if (a) the malware is created, procured, or stored without a legitimate reason and (b) it is distributed to someone's computer without their consent (Tsuboi, n.d., p. 3-5). In 2012, the Japanese parliament finally also ratified the Council of Europe Convention on Cybercrime (Budapest Convention).[27]

Public Security Intelligence Agency (PSIA)
(公安調査庁)
PSIA is responsible for dealing with subversive groups within Japan that pose a risk to the public. Groups include *Aum Shinrikyo* (which carried out the Tokyo subway sarin gas attack in 1996 that killed 12 and injured 5,000), leftist extremists such as the Middle Core Faction (which ran a coordinated terror campaign against Japan National Railways in 1985), right wing groups, and the General Association of Korean residents (which maintains close ties to the North Korean regime). In one form or another, all of these "conflicts" have spilled into the cyber domain. To fulfill its mission, PSIA conducts domestic surveillance to collect and analyze relevant intelligence (counter-intelligence function), engages in public-private cooperation with critical infrastructure providers (protecting against domestic terrorist attacks), and in conjunction with METI promotes initiatives that "protect important information owned by private corporations and research institutes" (safeguarding against industrial espionage) (MoJ 2018, p. 14). In this context, PSIA also tackles cyber incidents, attacks, and related threats.

Note: As early as September 2013, PSIA has stood up a "Special Task Force for Intelligence" to safeguard the 2021 Tokyo Olympic and Paralympic Games, which also operates in cyberspace (MoJ 2018, p. 20).

5.10 Ministry of Foreign Affairs (外務省)

Japan's cyber security diplomacy revolves around three main pillars: (a) promoting the rule of law in cyberspace (UN GGE, Open-ended Working Group (OEWG), and Global Conference on Cyberspace (GCCS)), (b) developing confidence building measures (ASEAN regional forum and bilateral consultations), and (c) cooperating on capacity building (raising awareness, protecting critical infrastructure, combatting cybercrime, strengthening law enforcement and CSIRTs). On 12 July 2016, MOFA created a dedicated Cyber Security Policy Division whose mission it is to "lead international discussions on how to ensure a safe and secure cyberspace, strengthening coordination with other countries" (MOFA, 2016b).

Ambassador in charge of Cyber Policy
(サイバー政策担当大使)
In February 2012, the post of Ambassador in charge of Cyber Policy was created. The Ambassador's task is to coordinate Japan's multilateral meetings in the ASEAN Regional Forum (Cybercrime Dialogue and Inter-sessional meetings on ICT Security), the United Nations (UN GEE & OEWG), and GCCS. The Ambassador also leads the Japanese delegations in the bilateral consultations on cyber policy. Apart from the Japan-US Cyber Dialogue, Tokyo has engaged in cyber dialogues with the EU and 11 other countries (see: Table 1). As of this writing, the latest cyber dialogue was held in Tokyo with a delegation from the UK on January 31, 2020 (MOFA, 2020; See page 30).

Intelligence and Analysis Service (IAS)
(国際情報統括官組織)
MOFA's Intelligence and Analysis Service is divided into four divisions. According to Bush, "the first is responsible for coordination within the IAS; the second is charged with intelligence collection and functional issues; the third covers Asia and Oceania; and the fourth watches the rest of the world" (Bush 2013, p. 164). It is generally assumed that the IAS overwhelmingly relies on open source intelligence and information gained through MOFA's diplomatic corps overseas. In regards to the cyber domain, there does not seem to be any open source information available as to how the IAS actually operates.

[27] Japan signed the Budapest Convention in 2001

Table.1 Cyber Dialogues between Japan and other countries (as of 30 January 2020)

		United Kingdom	India	USA	European Union	Trilateral Japan, South Korea, China
1st Dialogue	Japan	2012, June 19-20 (Tokyo)	2012, Nov. 5 (Tokyo)	2013, May 9-10 (Tokyo)	2014, Oct. 6 (Tokyo)	2014, Oct. 21 (Beijing)
2nd Dialogue	Japan	2014, Dec. 15 (London)	2017, Aug. 17 (New Delhi)	2014, April 10 (D.C.)	2017, Jan. 25 (Brussels)	2015, Oct. 15 (Seoul)
3rd Dialogue	Japan	2016, Oct. 21 (Tokyo)	2019, Feb. 27 (Tokyo)	2015, July 22 (Tokyo)	2018, March 5 (Tokyo)	2017, Feb. 10 (Tokyo)
4th Dialogue	Japan	2018, March 16 (London)		2016, July 27 (D.C.)	2019, June 11 (Brussels)	2019, Nov. 18 (Beijing)
5th Dialogue	Japan	2020, January 31 (Tokyo)		2017, July 20-21 (Tokyo)		
6th Dialogue	Japan			2018, July 26 (D.C.)		
7th Dialogue	Japan			2019, Oct. 11 (Tokyo)		

		Israel	France	Estonia	Australia	Russia
1st Dialogue	Japan	2014, Nov. 17 (Tokyo)	2014, Dec. 12 (Paris)	2014, Dec. 17-18 (Tallinn)	2015, Feb. 13 (Canberra)	2015, March 24 (Tokyo)
2nd Dialogue	Japan	2016, June 21-22 (Tel-Aviv)	2016, Dec. ? (Tokyo)	2015, Dec. 7-8 (Tallinn)	2016, Aug. 2 (Tokyo)	2016, Nov. 11 (Moscow)
3rd Dialogue	Japan	2017, Nov. 29 (Tokyo)	2017, Jan. 27 (Paris)	2017, Jan. 26 (Tallinn)	2017, Dec. 11 (Tokyo)	2019, Nov. 20, (Tokyo)
4th Dialogue	Japan	2018, Nov. 12 (Tel-Aviv)	2018, June 12 (Tokyo)		2019, Feb. 22 (Canberra)	
5th Dialogue	Japan		2019, July 12 (Rennes)			

		Germany	Ukraine
1st Dialogue	Japan	2016, Sept. 9 (Tokyo)	2016, Dec. 21 (Kiev)
2nd Dialogue	Japan		2020, Jan. 23 (Tokyo)

Source: Japanese Ministry of Foreign Affairs: 日本のサイバー外交　二国間協議・対話等
(https://www.mofa.go.jp/mofaj/fp/nsp/page24_000687.html)

6 Conclusion

As this study has hopefully shown, Japan's national cybersecurity and defense posture is both highly fragmented horizontally and deeply centralized vertically. In theory, the current set-up should create the necessary pressures for government agencies and ministries to cooperate interdependently while innovating separately.[28] In practice, the lack of open source information available as to how far and deep ministries actually cooperate – bilaterally, through the NISC, and within the Cybersecurity Strategic HQ – makes it difficult to evaluate success or failure from the outside looking in (as, for instance, in the case of assessing the prevalence of intelligence silos).

By contrast, the individual innovation of government agencies and ministries is clearly visible through the creation of new units, councils, and avenues to engage the private sector and other non-governmental actors. As far as visible, there are little to no duplication efforts among ministries and agencies. Instead they seem to naturally seek cooperation in areas where they overlap and individually invent new research items and structures in line with their mission profile. In this regard, the Ministry of Foreign Affairs stands somewhat apart from all the rest. MOFA has not shown the same innovative spirit as the other ministries. Instead, MOFA's cyber security policy division, the cyber ambassador, and the IAS seem to follow the general trajectory of the international community – particularly on norms and rules for state behavior online – while taking tentative steps to lead capacity-building efforts in the ASEAN region. The criticism here is not so much that MOFA is sluggish, but that the ministry has so much more potential to develop its own policies in-house rather than primarily replicate and attach itself to Western approaches. If MOFA is willing and able to experiment with its own bold cyber policy ideas in the not so distant future, it has the potential to promulgate a distinct Japanese style of cyber diplomacy.

The Ministry of Defense is already on this trajectory, with barriers falling on the offensive end and an alignment with US operational thinking in cyberspace becoming a distinct possibility (ex. persistent engagement and defending forward). Depending on how far and wide Japanese law enforcement is willing and legally able to push the envelope in its fight against cybercrime, some of the capabilities procured by the MoD could also be utilized to disrupt cybercriminal infrastructure abroad – thus emulating Australia's interpretation of international law and principle of due diligence during the COVID-19 crisis.[29]

Overall, one can conclude that the Japanese government has learned very early on that standing stationary in cyberspace is not a viable option. Innovation and experimentation are key to progress, cooperation is key to strength, and preparing for the unexpected is key to evolving.

[28] METI's cooperative innovation approach stands apart from the other ministries.

[29] See: Australian Ministry of Defense 2020.

7 Abbreviations

2ch	2channel
ACTIVE	Advanced Cyber Threats response InitiatiVE
APPI	Act on Protection of Personal Information
ASDF	Air Self-Defense Force
ASEAN	Association of South East Asian Nations
C4	Command, Control, Communication, and Computers
C5	Command, Control, Communications, Computers, and Combat Systems
CAAC	Cyber Attack Analysis Council
NATO CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CCS	Central Command System
CDC	Cyber Defense Council
CDPWG	US-Japan Cyber Defense Policy Working Group
CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Response
CERT	Computer Emergency Response Team
CIRO	Cabinet Intelligence and Research Organization
CSES	Computer Security Evaluation Squadron
CSG	Communication Security Group
CSIRT	Computer Security Incident Response Team
CSSC	Control System Security Center
CYDER	CYber Defense Exercise with Recurrence
CYMAT	Cyber Incident Mobile Assistant Team
DDoS	Distributed Denial of Service
DFS	Directorate for Signals Intelligence
DHS	Department of Homeland Security
DIH	Defense Information Headquarters
DII	Defense Information Infrastructure
DoD	US Department of Defense
DOD-CIO	Department of Defense – Chief Information Officer
DoJ	US Department of Justice
EDD	Extended Deterrence Dialogue
FBI	Federal Bureau of Investigations
FIRST	Forum of Incident Response and Security Teams
FSA	Financial Services Agency
GCCS	Global Conference on Cyberspace
GDPR	General Data Protection Regulation
GSDF	Ground Self-Defense Force
GSOC	Government Security Operation Coordination Team
IAS	Intelligence and Analysis Service
IAWG	Japan-US Information Assurance Working Group
ICS	Industrial Control System
ICT	Information Communication Technology
IoT	Internet of Things
IPA	Information Technology Promotion Agency
ISP	Information Service Provider
ISPC	Information Security Policy Council
ISMPO	Information Security Measures Promotion Office
J-CRAT	Japan Cyber Rescue Advice Team
J-CSIP	Japan-Cyber Security Information sharing Partnership
JEPG/IP	Japanese Engineering & Planning Group/Internet Protocol
JMOD	Japanese Ministry of Defense
JPCERT/CC	Japan Computer Emergency Response Team/Coordination Center
JPS	Japanese Pension Service
METI	Ministry of Economy, Trade, and Industry
MHI	Mitsubishi Heavy Industries
MIC	Ministry of Internal Affairs and Communications
MITI	Ministry of International Trade and Industry (1949-2001)
MoD	Ministry of Defense
MOFA	Ministry of Foreign Affairs
MSDF	Maritime Self-Defense Force
MTDP	Mid-term Defense Program
NDPG	National Defense Program Guidelines
NICT	National Institute for Information and Communications Technology
NISC	National Center for Incident Readiness and Strategy for Cybersecurity
NOTICE	National Operation Towards IoT Clean Environment
NPA	National Police Agency
NSA/CSS	National Security Agency/Central Security Service
NSC	National Security Council
NSS	National Security Secretariat
NTT	Nippon Telegraph and Telephone
OECD	Organisation for Economic Co-operation and Development
OEWG	Open-ended Working Group
PII	Personal Identifiable Information
PRACTICE	Proactive Response Against Cyberattacks Through International Collaborative Exchange
PSIA	Public Security Intelligence Agency
R&D	Research and Development
RPB	Regional Police Bureau

SCADA	Supervisory Control and Data Acquisition
SDF	Self-Defense Force
SOC	Security Operations Center
SPU	System Protection Unit
TAA	Terror Action Association
T-ISAC	Telecom Information Sharing and Analysis Center
UN GEE	United Nations Group of Governmental Experts

8 Bibliography

ACSW. n.d. "Air Communications and Systems Wing - 部隊紹介." Japanese Ministry of Defense. https://www.mod.go.jp/asdf/acsw/#butai.

Adelstein, Jake. 2017. "How Japan's Cyberterrorist Lost Game of Cat and Mouse." The Daily Beast. https://www.thedailybeast.com/how-japans-cyberterrorist-lost-game-of-cat-and-mouse.

Aranguren, Juan Luis Lopez. 2016. "The Communicative Dimension and Security in Asia-Pacific: A Communicative-Viewing Proposal for Reform of the Japanese Intelligence Services." Revista UNISCI. https://www.ucm.es/data/cont/media/www/pag-83486/UNISCIDP41-2LOPEZARANG.pdf.

Australian Ministry of Defense. 2020. "On the offensive against COVID-19 cyber criminals." https://www.minister.defence.gov.au/minister/lreynolds/media-releases/offensive-against-covid-19-cyber-criminals

Barkin, Noah. 2018. "Exclusive: Five Eyes Intelligence Alliance Builds Coalition to Counter China." Reuters. https://www.reuters.com/article/us-china-fiveeyes/exclusive-five-eyes-intelligence-alliance-builds-coalition-to-counter-china-idUSKCN1MM0GH.

Barrette, Greg. 2016. "SOC Fundamentals for Your Threat Intelligence Program." Recorded Future. https://www.recordedfuture.com/security-operations-center-fundamentals/.

BBC. 2000. "Hackers Blast Japan over Nanking Massacre." BBC. http://news.bbc.co.uk/2/hi/asia-pacific/618520.stm.

BBC. 2015. "Death Threat Hacker Who Fooled Police Is Jailed." BBC. https://www.bbc.com/news/technology-31129817.

Blaster, Master. 2014. "Alleged Hacker Yusuke Katayama Publicly Confesses to Spree of Bizarre Crimes." SoraNews24. https://soranews24.com/2014/05/21/alledged-hacker-yusuke-katayama-publicly-confesses-to-spree-of-bizarre-crimes/.

Burke, Matthew M. 2018. "Japan Ground Self-Defense Force to Experience 'Biggest Restructuring' Ever." Stars and Stripes. https://www.stripes.com/news/japan-ground-self-defense-force-to-experience-biggest-restructuring-ever-1.518790.

Bush, Richard C. 2013. *The Perils of Proximity: China-Japan Security Relations*. Brookings.

CAS. n.d. "国家安全保障局." Cabinet Secretariat. https://www.cas.go.jp/jp/gaiyou/jimu/anzenhosyou.html.

CAS. 2010. "情報と情報保全." Cabinet Secretariat. https://www.kantei.go.jp/jp/singi/shin-ampobouei2010/dai7/siryou1.pdf.

CAS. 2017. "Ministry of Defense." Cabinet Secretariat. https://www.cas.go.jp/jp/gaiyou/jimu/jinjikyoku/2017_pdf/14_2017mod.pdf.

CIA. 1995. "Intelligence in the New Japan." Central Intelligence Agency. https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no3/html/v07i3a01p_0001.htm.

CIRO. 2018a. "採用案内 2017." Cabinet Intelligence and Research Office. https://www.cas.go.jp/jp/saiyou/pdf/panf_2017.pdf.

CIRO. 2018b. "採用案内 2018." Cabinet Intelligence and Research Office. https://www.cas.go.jp/jp/saiyou/pdf/panf_2018.pdf.

CIRO. 2019. "採用案内 2019." Cabinet Intelligence and Research Office. https://www.cas.go.jp/jp/saiyou/pdf/panf_2019.pdf.

CISA. n.d. "Cyber Storm: Security Cyber Space." Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/cyber-storm-securing-cyber-space.

Cotton, Tim. 2019. "Russia's Bitcoin Hacking Funds." Medium. https://blog.cotten.io/russias-bitcoin-hacking-funds-c0a87b33f1e2.

Council of Europe. n.d. "Details of Treaty No.185 - Convention on Cybercrime." Council of Europe. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

CSSC. n.d. "Backgrounds and Objectives." CSS-Center. http://www.css-center.or.jp/en/aboutus/purpose.html.

Cybersecurity Strategic Headquarters. 2017. "The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)." Japanese Government. https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf.

DIH. 2013. "DFS SIGINT-Enabled Cyber." The Intercept. https://theintercept.com/document/2018/05/19/dfs-briefing-feb-2013/.

DIH. 2019. "防衛省情報本部 職員採用パンフレット2020." Defense Intelligence Headquarters. https://www.mod.go.jp/dih/2020_joho_web.pdf.

Dooley, Ben. 2019. "Bitcoin Tycoon Who Oversaw Mt. Gox Implosion Gets Suspended

Sentence." The New York Times. https://www.nytimes.com/2019/03/15/business/bitcoin-mt-gox-mark-karpeles-sentence.html.

e-Gov. n.d. "組織・制度の概要案内 － 詳細情報: 防衛省." e-Gov.go.jp. https://search.e-gov.go.jp/servlet/Organization?class=1050&objcd=100170&dispgrp=0003.

EU Commission. n.d. "Adequacy Decisions: How the EU Determines If a Non-EU Country Has an Adequate Level of Data Protection." EU Commission. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

EU Commission. 2019. "European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows." EU Commission. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421.

FIRST. n.d. "FIRST Teams." First.org. https://www.first.org/members/teams/.

Freire, Carl. 2006. "Virus Spreads Data, Scandal over Winny - Antinny Has Hit Airlines, Police and the National Defense Agency." NBC News. http://www.nbcnews.com/id/13283771/ns/technology_and_science-security/t/virus-spreads-data-scandal-over-winny/#.XeD0n-hKhaQ.

FSA. 2015. "The Policy Approaches to Strengthen Cyber Security in the Financial Sector (Summary)." Financial Services Agency. https://www.fsa.go.jp/en/news/2015/20151105-1/01.pdf.

FSA. 2019. "Financial Sector Cybersecurity Report." Financial Services Agency. https://www.fsa.go.jp/en/news/2019/20191028/cyber_report.pdf.

Fujitsu. 2017. "Security Measures Indispensable to Realizing a Data-Driven Society." Fujitsu Journal. https://journal.jp.fujitsu.com/en/2017/11/20/02/.

G7. 2016. "G7 Principles and Actions on Cyber." G7. https://www.mofa.go.jp/files/000160279.pdf.

Gallagher, Ryan. 2018. "The Untold Story of Japan's Secret Spy Agency." The Intercept. https://theintercept.com/2018/05/19/japan-dfs-surveillance-agency/.

Geere, Duncan. 2010. "Japanese Virus Replaces Files with Pictures of Squid." Wired. https://www.wired.co.uk/article/japanese-virus.

Google. n.d. "サイバーテロ by Time, Location and Popularity on Google Trends." Google. https://trends.google.com/trends/explore?date=all&geo=JP&q=%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E3%83%86%E3%83%AD.

Gradijan, Dave. 2006. "Winny Virus Continues to Wreak Havoc Across Japan." CSO Online. https://www.csoonline.com/article/2121198/winny-virus-continues-to-wreak-havoc-across-japan.html.

Green, Michael J., and Koji Murata. n.d. "The 1978 Guidelines for the U.S.- Japan Defense Cooperation: Process and the Historical Impact." George Washington Univerisity: US-Japan Project. https://nsarchive2.gwu.edu//japan/GreenMurataWP.htm.

Haberman, Clyde. 1985. "Sabotage Cripples Japan Rail Lines." The New York Times. https://www.nytimes.com/1985/11/30/world/sabotage-cripples-japan-rail-lines.html.

Humphries, Matthew. 2008. "Japanese Student Finally Convicted for Spreading Harada Virus." Geek.com. https://www.geek.com/law/japanese-student-finally-convicted-for-spreading-harada-virus-575126/.

ICT-ISAC. n.d. "Action for Removal of Malware." ICT-ISAC. https://www.ict-isac.jp/active/en/active/removal.html.

IPA. n.d. "IPA - Better Life with IT." IPA. https://www.ipa.go.jp/files/000058630.pdf.

IPA. 2019. "サイバーレスキュー隊J-CRAT（ジェイ・クラート）." IPA. https://www.ipa.go.jp/security/J-CRAT/index.html.

IPA. 2020. "サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））." IPA. https://www.ipa.go.jp/security/J-CSIP/index.html.

ISPC. 2006. "The First National Strategy on Information Strategy - Toward the Realization of a Trsutworthy Society." Information Security Policy Council. https://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

ISPC. 2009. "The Second National Strategy on Information Security - Aiming for Strong 'Individual' and 'Society' in IT Age." IPSC. https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf.

ISPC. 2010. "Information Security Strategy for Protecting the Nation." ISPC. https://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf.

ISPC. June 10, 2013a. "Cybersecurity Strategy - Toward a World-Leading, Resilient and Vigirous Cyberspace." ISPC. https://www.nisc.go.jp/eng/pdf/cybersecuritystrategy-en.pdf.

ISPC. October 2, 2013b. "International Strategy on Cybersecurity Cooperation - j-Initiative for Cybersecurity." Information Security Policy Council. https://www.nisc.go.jp/eng/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf.

ISMPO. 2000. "重要インフラのサイバーテロ対策に係る特別行動計画." Information Security Measures Promotion Office. https://www.nisc.go.jp/active/sisaku/2000_1215/1215actionplan.html.

Jacob, Marc. 2008. "Sophos: First Virus Writer Arrester Arrested in Japan... for Breaching." Global Security Mag. https://www.globalsecuritymag.fr/Sophos-First-Virus-writer-arrester,20080124,1456.html.

Jameson, Sam. 1985. "Millions Stalled as Japanese Radicals Sabotage Government-Owned Rail Lines." Los Angeles Times. https://www.latimes.com/archives/la-xpm-1985-11-29-mn-4958-story.html.

Japan Times. 2011. "Absurd Arrest Rectified." Japan Times. https://www.japantimes.co.jp/opinion/2011/12/26/editorials/absurd-arrest-rectified/#.XmDwGqhKhaQ.

Japan Times. 2019. "In First, Japan to Develop Computer Virus to Defend against Cyberattacks." Japan Times. https://www.japantimes.co.jp/news/2019/04/30/national/first-japan-develop-computer-virus-defend-cyberattacks/#.XmDjcKhKhaQ.

Japan Times. 2020. "'Five Eyes' Intel Alliance Ties up with Japan on North Korea Threat." Japan Times. https://www.japantimes.co.jp/news/2020/01/27/national/five-eyes-intelligence-sharing-alliance-partners-japan-north-korea/.

Japanese Government. 2000. "The Basic Act on the Formation of an Advanced Information and Telecommunications Network Society." Japanese Government. http://www.japaneselawtranslation.go.jp/law/detail/?id=3339&vm=02&re=.

Japanese Government. 2014. "The Basic Act on Cybersecurity." Japanese Government. http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&vm=02&id=2760.

Japanese Government. 2015. "Cybersecurity Strategy." The Government of Japan. https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.

Japanese Government. 2016. "Basic Act on the Advancement of Public and Private Sector Data Utilization." Japanese Government. https://japan.kantei.go.jp/policy/it/data_basicact/data_basicact.html.

Japanese Government. 2018. "Cybersecurity Strategy." Japanese Government. https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.

Jarkoff, Scott. n.d. "Scott Jarkoff Resume - ジャーカフスコットの履歴書." Jark.me. https://jark.me/about/resume/.

JCG. n.d. "情報通信課." Japan Coast Guard. https://www.kaiho.mlit.go.jp/soshiki/soumu/jyouhoutsuushin.html.

JPNIC. 2018. "The Internet Timeline." JPNIC. https://www.nic.ad.jp/timeline/en/.

JPS. 2015. "日本年金機構の個人情報流出について." Japan Pension Service. https://www.nenkin.go.jp/oshirase/topics/2015/20150721.files/0000150601ndjlleouli.pdf.

JWing. 2019. "陸自システム防護隊、日米共同CTFを初実施." Jwing.net. http://www.jwing.net/news/16116.

Kantei. n.d. "Establishment of the IT Strategy Headquarters." Kantei. https://japan.kantei.go.jp/it/council/establishment_it.html.

Kantei. n.d. "Government Offices' Functions & Web Site Content." Kantei. http://japan.kantei.go.jp/link/link1.html.

Kantei. n.d. "IT Strategic Headquarters." Kantei. https://japan.kantei.go.jp/policy/it/enkaku_e.html.

Kantei. n.d. "Members of the IT Strategy Council and the IT Strategy Headquarters." Kantei. http://japan.kantei.go.jp/it/council/member.html.

Kantei. 2000. "IT Strategy Council." Kantei. http://japan.kantei.go.jp/it/council/council_it.html.

Kantei. 2019. "高度情報通信ネットワーク社会推進戦略本部名簿." Kantei. https://www.kantei.go.jp/jp/singi/it2/pdf/kousei.pdf.

Kaspersky IT Encyclopedia. n.d. "Dictionary Attack." Kaspersky IT Encyclopedia. https://encyclopedia.kaspersky.com/glossary/dictionary-attack/.

Kaspersky Lab. 2013. "The 'Icefog' APT: A Tale of Cloak and Three Daggers." Kaspersky Lab. https://media.kaspersky.com/en/icefog-apt-threat.pdf.

Kawaguchi, Hiroshi. 2015. "Cybersecurity Strategy in Japan." Japan Security Operation Center. https://cs.kyushu-u.ac.jp/wp-content/uploads/17-kawaguchi.pdf.

Kim, Yu. 2010. "Epic Cyber War (Full Story): Japan V.S Korea." iNEWB.com. https://web.archive.org/web/20100312112213/http://inewp.com/?p=1086.

Kubota, Yoko. 2011. "Japan Contractor Hacking Likely Got Military Data: Asahi." Reuters. https://www.reuters.com/article/us-mitsubishi-heavy-cyberattack/japan-contractor-hacking-likely-got-military-data-asahi-idUSTRE79M3XS20111024.

Kyodo News. 2019. "China Hackers Likely Attacked Japan Business Lobby in 2016: Experts." *Kyodo News*, January 13, 2019. https://english.kyodonews.net/news/2019/01/4354ae41b20d-china-hackers-likely-attacked-japan-business-lobby-in-2016-experts.html.

Leyden, John. 2012. "Japan Tasks Fujitsu with Creating Search-and-Destroy Cyber-Weapon." *The Register*, January 3, 2012. https://www.theregister.co.uk/2012/01/03/japan_cyber_weapon_research/.

LIff, Adam P. 2018. "Japan's National Security Council at Five." Brookings. https://www.brookings.edu/blog/order-from-chaos/2018/12/04/japans-national-security-council-at-five/.

Littleton, Matthew J. 1995. "Information Age Terrorism: Toward Cyberterror." Naval Postgraduate School. https://calhoun.nps.edu/bitstream/handle/10945/7469/95Dec_Littleton.pdf?sequence=1&isAllowed=y.

McMillan, Robert. 2014. "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster." Wired. https://www.wired.com/2014/03/bitcoin-exchange/.

MHI. 2011. "Bulletin Board Notice Re Media Reporting of Virus Infections." *Mitsubishi Heavy Industries*, September 21, 2011. https://www.mhi.com/notice/notice_110921.html.

MIC. 2012. "サイバー攻撃解析協議会の開催." Ministry of Internal Affairs and Communications. https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000021.html.

MIC. 2019. "The 'NOTICE' Project to Survey IoT Devices and to Alert Users." Ministry of Internal Affairs and Communications. https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/19020101.html.

MIC & NICT. 2019. "The 'NOTICE' Project to Survey IoT Devices and to Alert Users." National Institute of Information and Communications Technology. https://www.nict.go.jp/en/press/2019/02/01-1.html.

MoD. n.d. "About Ministry." Japanese Ministry of Defense. https://www.mod.go.jp/e/about/.

MoD. n.d. "CDPWG - 日米サイバー防衛政策ワーキンググループ（CDPWG）について." Japanese Ministry of Defense. https://www.mod.go.jp/j/approach/defense/cyber/cdpwg/index.html.

MoD. n.d. "Cyber Security - Capability Building Assistance: Vietnam." Japanese Ministry of Defense. https://www.mod.go.jp/e/d_act/exc/cap_b/vietnam/20171211.html.

MoD. n.d. "令和元年度実施施策に係る政策評価の事前分析表." Japanese Ministry of Defense. https://www.mod.go.jp/j/approach/hyouka/seisaku/31/pdf/31bunseki_04.pdf.

MoD. 2001. "平成１３年度政策評価書（中間段階の事業評価）－ 防衛情報通信基盤（ＤＩＩ）の整備." Japanese Ministry of Defense. https://www.mod.go.jp/j/approach/hyouka/seisaku/13/chukan/honbun/01.pdf.

MoD. 2002. "保全監査隊の編制に関する訓令." Japanese Ministry of Defense. http://www.clearing.mod.go.jp/kunrei_data/a_fd/2001/ax20020320_00023_000.pdf.

MoD. July 2013a. "サイバーディフェンス連携協議会 （ＣＤＣ） の設置・取組について." Japanese Ministry of Defense. https://www.mod.go.jp/j/approach/defense/cyber/cdc/pdf/cyber_defense_council.pdf.

MoD. October 3, 2013b. "日米サイバー防衛政策ワーキンググループ（ＣＤＰＷＧ）の概要." Japanese Ministry of Defense. https://www.mod.go.jp/j/approach/anpo/kyougi/2013/10/03_cdpwg_gaiyou.html.

MoD. 2010. "Section 3. Trends Concerning Cyber Warfare Capabilities." Japanese Ministry of Defense. https://www.mod.go.jp/e/publ/w_paper/pdf/2010/07Part1_Chapter1_Sec3.pdf.

MoD. 2014a. "Establishment of National Security Council." Japanese Ministry of Defense. https://www.mod.go.jp/e/publ/w_paper/pdf/2014/DOJ2014_2-2-1_web_1031.pdf.

MoD. 2014b. "Organization of the Ministry of Defense and the Self-Defense Forces." Japanese Ministry of Defense. https://www.mod.go.jp/e/publ/w_paper/pdf/2014/DOJ2014_2-2-2_web_1031.pdf.

MoD. April 27, 2015a. "The Guidelines for Japan-U.S. Defense Cooperation." Japanese Ministry of Defense. https://www.mod.go.jp/e/d_act/us/anpo/shishin_20150427e.html.

MoD. November 2015b. "MOD's Reorganization." Japan Defense Focus. https://www.mod.go.jp/e/jdf/sp/no70/sp_activities.html.

MoD. January 9, 2015c. "第１１回日米ＩＴフォーラムの開催について." Japanese Ministry of Defense. https://www.mod.go.jp/j/press/news/2015/01/09a.html.

MoD. March 11, 2016. "第１２回日米ＩＴフォーラムの開催について." Japanese Ministry of Defense. https://www.mod.go.jp/j/press/news/2016/03/11a.html.

MoD. December 18, 2018a. "National Defense Program Guidelines for FY 2019 and Beyond." MoD. https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218_e.pdf.

MoD. December 18, 2018b. "Medium Term Defense Program (FY 2019 - FY 2023)." Japanese Ministry of Defense. https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/chuki_seibi31-35_e.pdf.

MoD. 2018c. "Organizational Diagram of the Self-Defense Forces." Japanese Ministry of Defense. https://www.mod.go.jp/e/publ/w_paper/pdf/2018/DOJ2018_diagram_web.pdf.

MoD. 2018d. "Defense of Japan 2018." Japanese Ministry of Defense. https://www.mod.go.jp/e/publ/w_paper/pdf/2018/DOJ2018_Full_1130.pdf.

MoD. April 19, 2019a. "Joint Statement of the Security Consultative Committee." Japanese Ministry of Defense. https://www.mod.go.jp/e/d_act/us/201904_js.html.

MoD. 2019b. "Defense Programs and Budget of Japan - Overview of FY2019 Budget." Japanese Ministry of Defense. https://www.mod.go.jp/e/d_act/d_budget/pdf/190510b.pdf.

MoD. August 8, 2019c. "日米共同ＣＴＦ（Cyber Thunder）について." Japanese Ministry of Defense. https://www.mod.go.jp/gsdf/news/press/2019/pdf/20190808_01.pdf.

MoD. November 25, 2019d. "日米サイバー防衛政策ワーキンググループ（CDPWG）第７回会合について." Japanese Ministry of Defense. https://www.mod.go.jp/j/approach/anpo/kyougi/2013/10/03_cdpwg_gaiyou.html.

MoD. 2020. "Defense Programs and Budget of Japan(Draft) - Overview of JFY2020 Budget." Japanese Ministry of Defense. https://www.mod.go.jp/e/d_act/d_budget/pdf/200225b.pdf.

MOFA. 2013. "Joint Statement - Japan-U.S. Cyber Dialogue." Japanese Ministry of Foreign Affairs. https://www.mofa.go.jp/region/page22e_000001.html.

MOFA. 2015. "The Guidelines for Japan-U.S. Defense Cooperation." Japanese Ministry of Foreign Affairs. https://www.mofa.go.jp/files/000078188.pdf.

MOFA. October 14, 2016a. "First Meeting of G7 'Ise-Shima Cyber Group (ISCG).'" Japanese Ministry of Foreign Affairs. https://www.mofa.go.jp/fp/nsp/press3e_000073.html.

MOFA. July 12, 2016b. "Establishment of Cyber Security Policy Division, Foreign Policy Bureau." Japanese Ministry of Foreign Affairs. https://www.mofa.go.jp/press/release/press4e_001203.html.

MOFA. April 6, 2016c. "Japan's Security Policy - National Security Council (NSC)." MOFA. https://www.mofa.go.jp/fp/nsp/page1we_000080.html.

MOFA. 2018. "Cyberattacks by a Group Based in China Known as APT10." MOFA. https://www.mofa.go.jp/press/release/press4e_002281.html.

MOFA. 2019. "The 7th Japan-US Cyber Dialogue." Japanese Ministry of Foreign Affairs. https://www.mofa.go.jp/press/release/press4e_002646.html.

MOFA. 2020. "The 5th Japan-UK Bilateral Consultations on Cyberspace." MOFA. https://www.mofa.go.jp/press/release/press4e_002766.html.

MoJ. 2018. "MInistry of Justice Japan 2018." MoJ. http://www.moj.go.jp/content/001254973.pdf.

Moosa, Eugene. 1985. "Hundreds of Police Hunt for 300 Rail Saboteurs." Associated Press News. https://apnews.com/eb2de145e6e22fb474d0500aa353cf28.

Muncaster, Phil. 2012. "Chinese Hacktivists Launch Cyber Attack on Japan." The Register. https://www.theregister.co.uk/2012/09/21/japan_china_attack_sites_senkaku/.

Nakao, Koji. n.d. "General Security Strategy in Japan (MIC) Including PRACTICE Overview." Gisfi.org. http://www.gisfi.org/pdf/19th_meeting/Koji%20Nakao%20for%20India.pdf.

NATO. 2019a. "Centres of Excellence." NATO. https://www.nato.int/cps/en/natolive/topics_68372.htm.

———. 2019b. "NATO and Japan Intensify Dialogue on Cyber Defence." NATO. https://www.nato.int/cps/en/natohq/news_169493.htm?selectedLocale=ens.

NICT. n.d. "History." NICT. https://www.nict.go.jp/en/about/history.html.

———. n.d. "Organization." NICT. https://www.nict.go.jp/en/about/organization.html.

———. n.d. "実践的サイバー防御演習「CYDER」のここがスゴい！." NICT. https://www.soumu.go.jp/main_content/000603221.pdf.

———. 2019. "参考資料." National Institute of Information and Communications Technology. https://nct.nict.go.jp/file/national_cyber_training_center_20191101_reference.pdf.

Nikkei. 2013. "「サイバー防衛隊」準備室を設置 防衛省." Nikkei.com. https://www.nikkei.com/article/DGXNASFS1603T_W3A510C1PP8000/.

NISC. n.d. "Outline of the Second National Strategy on Information Security." NISC. https://www.nisc.go.jp/eng/pdf/SecondNationalStrategy.pdf.

NISC. n.d. "サイバーセキュリティ協議会." NISC. https://www.nisc.go.jp/conference/cs/kyogikai/index.html.

NISC. n.d. "警察におけるサイバー攻撃対策の推進体制." NISC. https://www.nisc.go.jp/conference/cs/ciip/dai03/pdf/03shiryou0206.pdf.

NISC. 2005. "情報セキュリティ政策会議の設置について." NICT. https://www.nisc.go.jp/conference/seisaku/pdf/kitei.pdf.

NISC. 2007. "Japanese Government's Efforts to Address Information Seurity Issues - Focusing on the Cabinet Secretariat Efforts." National Center for Incident Readiness and Strategy for Cybersecurity. https://www.nisc.go.jp/eng/pdf/overview_eng.pdf.

NISC. 2012. "情報セキュリティ緊急支援チーム（CYMAT）設置について." NISC. https://www.nisc.go.jp/press/pdf/cymat_press.pdf.

NISC. 2014. "防衛省のサイバーセキュリティへの取組." NISC. https://www.nisc.go.jp/conference/seisaku/ituse/dai2/pdf/siryou0200.pdf.

NISC. 2015. "サイバーセキュリティ戦略本部の運営について." NISC. https://www.nisc.go.jp/conference/cs/pdf/unei_kitei.pdf.

NISC. 2019. "セプター特性把握マップ." NISC. https://www.nisc.go.jp/active/infra/pdf/cc_ceptoar.pdf.

NISC. 2020. "サイバーセキュリティ協議会について." NISC. https://www.nisc.go.jp/conference/cs/kyogikai/pdf/kyogikai_gaiyou.pdf.

NPA. n.d. "サイバー攻撃に対する警察の取組状況." National Police Agency. https://www.npa.go.jp/archive/keibi/syouten/syouten285/pdf/01_6-9P.pdf.

NPA. 2018. "Police of Japan 2018." National Police Agency. https://www.npa.go.jp/english/Police_of_Japan/Police_of_Japan_2018_full_text.pdf.

NPA. 2019. "令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について." NPA. https://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_kami_cyber_jousei.pdf.

NPA. n.d. "サイバーテロ." National Police Agency. https://www.npa.go.jp/archive/keibi/syouten/syouten279/p04.html.

NPSC. n.d. "委員のプロフィール." National Public Safety Commission. https://www.npsc.go.jp/about/chairman/profile/index.html.

NPSC. n.d. "概要." National Public Safety Commission. https://www.npsc.go.jp/about/summary/index.html.

NSA. 2013. "Cyber Paper Japan DFS." The Intercept. https://theintercept.com/document/2018/05/19/cyber-paper-japan-dfs/.

Phneah, Ellyne. 2012. "Anonymous Hacks Japanese Govt Sites." ZDNet. https://www.zdnet.com/article/anonymous-hacks-japanese-govt-sites/.

Phys.org. 2012. "Japan Anonymous Pick up Litter to Protest Download Laws." Phys.org. https://phys.org/news/2012-07-japan-anonymous-litter-protest-download.html.

Ryall, Julian. 2020. "Japan Almost a 'sixth Eye' as Five Eyes Keep Closer Watch on Chinese Military, North Korea." South China Morning Post. https://www.scmp.com/news/asia/east-asia/article/3048079/japan-almost-sixth-eye-five-eyes-keep-closer-watch-chinese.

Samuels, Richard. 2019. *Special Duty - A History of the Japanese Intelligence Community*. Cornell University Press.

Sbbit. 2013. "警察庁、「サイバー攻撃分析センター」を設置　全国警察の司令塔として20名." sbbit.jp. https://www.sbbit.jp/article/cont1/26329.

Schoff, James L., and Sayuri Romei. 2019. "The New National Defense Program Guidelines: Aligning U.S. and Japanese Defense Strategies for the Third Post-Cold War Era." Sasakawa USA. https://spfusa.org/wp-content/uploads/2019/04/Japan%E2%80%99s-New-National-Defense-Program-Guidelines-Aligning-U.S.-and-Japanese-Defense-Strategies.pdf.

Sebag, Gaspard. 2020. "Russian Bitcoin Suspect Charged in France After Greek Extradition." Bloomberg. https://www.bloomberg.com/news/articles/2020-01-28/russian-cyber-suspect-charged-in-france-after-greek-extradition.

Security Next. 2013. "防衛省、サイバーディフェンス連携協議会を発足 － サイバー攻撃対策で官民連携." Security-next.com. http://www.security-next.com/041625.

SHAPE. 2019. "Exercise Cyber Coalition 2019 Concludes in Estonia." SHAPE. https://shape.nato.int/news-archive/2019/exercise-cyber-coalition-2019-concludes-in-estonia.

Sims, Calvin. 2000. "Japan Software Suppliers Linked to Sect." The New York Times. https://www.nytimes.com/2000/03/02/world/japan-software-suppliers-linked-to-sect.html.

Slayton, Rebecca, and Brian Clarke. 2020. "Trusting Infrastructure - The Emergence of Computer Security Incident Response, 1989–2005." First.org. https://www.first.org/newsroom/newsletters/trusting-infrastructure.pdf.

SSRC. 2012. "The Japanese Government Established the Cyber Incident Mobile Assistant Team --- CYMAT Deals with Recent Anonymous Cyber-Attacks." SHIELD Security Research Center. https://www.shield.ne.jp/ssrc/topics/SSRC-ER-12-022-en.html.

SSRC. 2013. "警察庁、サイバー攻撃分析センターを設置." SHIELD Security Research Center. https://www.shield.ne.jp/ssrc/topics/SSRC-ER-13-021-ja.html.

TMP. n.d. "サイバーテロ対策協議会." Tokyo Metropolitan Police. https://www.keishicho.metro.tokyo.jp/kurashi/cyber/katsudo/cyber/index.html.

TMP. n.d. "サイバー犯罪対策協議会." Tokyo Metropolitan Police. https://www.keishicho.metro.tokyo.jp/kurashi/cyber/katsudo/cyber60/index.html.

Tsuboi, Mayumi. n.d. "Legislation on Cybercrime in Japan." Japanese Ministry of Justice. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b9868.

Umeda, Sayuri. 2018. "Japan: Basic Act on Cybersecurity Amended." US Library of Congress. https://www.loc.gov/law/foreign-news/article/japan-basic-act-on-cybersecurity-amended/.

US DHS. 2016. "Cyber Storm V: After Action Report." US Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/CyberStormV_AfterActionReport_2016vFinal-%20508%20Compliant%20v2.pdf.

US DoJ. 2017. "Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox." US Department of Justice. https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged.

US DoJ. 2019. "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." US Department of Justice. https://www.justice.gov/storage/report.pdf.

US JCS. n.d. "J6 Command, Control, Communications, & Computers/Cyber." US Joint Chiefs of Staff. https://www.jcs.mil/Directorates/J6-C4-Cyber/.

Vosse, Wilhelm M. 2019. "Japan's Cyber Diplomacy." EU Cyber Direct. https://eucyberdirect.eu/wp-content/uploads/2019/10/vosse_rif_topublish.pdf.

Watts, Jonathan. 2000. "Hackers Shake up Japan." The Guardian. https://www.theguardian.com/world/2000/jan/29/jonathanwatts.

Wehrfritz, George. 2000. "From Sarin to Software." Newsweek. https://www.newsweek.com/sarin-software-156381.

Wired. 2004. "Copyright Arrest in Japan." Wired. https://www.wired.com/2004/05/copyright-arrest-in-japan/.

WizSec. 2017. "Breaking Open the MtGox Case, Part 1." WizSec. https://blog.wizsec.jp/2017/07/breaking-open-mtgox-1.html.

Yoshida, Reiji. 2006. "SDF Establishes Joint Office for Military Operations." Japan Times. https://www.japantimes.co.jp/news/2006/03/28/national/sdf-establishes-joint-office-for-military-operations.

Yoshida, Reiji. 2007. "Defense Agency given Ministry Status." Japan Times. https://www.japantimes.co.jp/news/2007/01/10/national/defense-agency-given-ministry-status/.

Yoshioka, Katsunari. 2013. "PRACTICE - Proactive Response Against Cyber-Attacks Through International Collaborative Exchange." ieice.org. https://www.ieice.org/ken/paper/20130325JB2Y/eng/.

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.