A one-sided Affair: Japan and the People's Republic of China in Cyberspace

Hotspot Analysis

CSS CYBER DEFENSE PROJECT

Hotspot Analysis

A one-sided Affair: Japan and the People's Republic of China in Cyberspace

Zürich, January 2020

Version 1

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

Author: Stefan Soesanto

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zürich

Disclaimer: The opinions presented in this study exclusively reflect the author's views.

Please cite as: Stefan Soesanto (2020): A one-sided Affair: Japan and the People's Republic of China in Cyberspace, January 2020, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

1 Introduction

This Hotspot analysis takes a deep dive into the cyber threat landscape between Japan and the People's Republic of China. In contrast to other threat landscape reports, this analysis primarily looks at relevant incidents that have – or had the potential - to spill into the political realm. Meaning, it does not touch upon traditional cybercrime, background noise activities, or minor cyber-related incidents.

Section two provides political background information on four issues deemed constants in Japan-PRC relations, and explains the historical evolution of cybersecurity and –defense policies in both countries. Section three presents a chronological overview of relevant cyber incidents, including infection vectors and attribution assessments. Section four and five identify the various teams connected to these incidents, and extends insights into their history and – if available - current state of play. Section six then outlines social, economic, technical, and international effects resulting from the overall cyber threat landscape. And section seven concludes the analysis with a look into the future.

2 Background

Since the birth of the People's Republic of China on October 1, 1949, diplomatic relations between Tokyo and Beijing have gone through multiple cycles of rapprochement and political tension. Despite, or because of, these ups and downs, four unbridgeable issues have become political constants over time and space that occasionally spill over into the cyber domain.

(1) **Historic animosity**: Between 1930 and 1945, Imperial Japan waged an aggressive colonization campaign against large parts of mainland China, which saw mass atrocities, such as the Nanjing massacre, and human experimentation for biological warfare purposes (ex. Unit 731). These war-wounds have never healed despite numerous friendship treaties between both countries, rapidly expanding trade relations, offers of reparation payments, and longstanding Japanese official development assistance to China.

The specific reasons are multiple, but to a large degree, historical animosity is still leveraged by Beijing to rally support around nationalistic sentiments and to deflect any form of criticism voiced by Tokyo. This includes issues such as China's rapidly increasing military spending and Beijing's enduring human rights violations - stretching back from the Tiananmen massacre in 1989 to today's 're-education' of millions of Uighur Muslims in Xinjiang province. In most instances it is even the other way around, with China consistently calling out Japan on its annual defense budget - despite Beijing currently spending four times more – and accusing Tokyo of re-militarization efforts by arguing that Japan is "deny[ing] its history of aggression, challeng[ing] the post-war order, and harm[ing] the feelings of the people of those victimized nations" (Deutsche Welle, 2013; Johnson, 2019).

In the cyber domain, historic animosity most notably manifests itself in the form of Chinese hacktivists DDoS'ing and defacing Japanese government websites, particularly around the 18th of September, which marks the beginning of the Japanese invasion of Manchuria in 1931.

(2) **The rise of China**: Between 1946 and 1992, Japan experienced an era of rapid economic growth, propelling it to become the world's second largest economy behind the United States. China in turn, opened itself up to foreign trade and investment in 1979, and overtook Japan in 2010/11 when measured in nominal GDP (McCurry & Kollewe, 2011). While estimates vary, some analysts suggest that the Republic will become the world's largest economy sometime between 2028 and 2050.

The rise of China has serious security implications for Japan, ranging from Beijing's increased military spending and modernization efforts, Chinese hegemonic assertions abroad, and a creeping restructuring of both the global economy and the international political system at large. It should thus come as no surprise that Tokyo views Beijing's Belt and Road initiative (BRI) as a vehicle for expanding China's economic stranglehold across the globe.

To counter Chinese ambitions, the Japanese government developed, and has recently begun to promote, its own concept of a 'Free and Open Indo-Pacific' (FOIP) as part of its official foreign policy (Miyake, 2019). So far however, FOIP has gained little traction internationally as it only exists on two jumbled power point presentations and a short YouTube video put together by the Japanese Ministry of Foreign Affairs (MOFA, 2019b).

In its 2019 White Paper, the Japanese Ministry of Defense placed - for the first time since 2007 - the section on China's defense policies second behind the United States. In all the 12 years prior, the defense policies on the Korean Peninsula occupied the second spot. Many analysts have interpreted this subtle change as a strategic shift in the MoD's threat prioritization vis-à-vis the People's Republic (Kelly, 2019). The White Paper also specifically identified the Belt and Road Initiative as a possible cover for the People's Liberation Army (PLA) to advance its activities abroad (MoD, 2019a, p. 20).

In regard to the cyber domain, the rise of China proceeds in lockstep with Chinese espionage campaigns against a variety of Japanese industrial sectors and government agencies.

(3) **Territorial dispute**: Consisting of five islets and three rocks in the East China Sea, the uninhabited Diaoyu/Senkaku Islands are currently administered by the Japanese government and claimed by both China and Taiwan.[1] The territorial dispute flares up occasionally when Chinese submarines, frigates, and fishing trawlers enter the contiguous zone around the islands, or Chinese jet fighters violate Japanese airspace above. On September 7, 2010, a Chinese fishing trawler eventually collided with a Japanese coast guard vessel in the disputed waters. After detaining the Chinese skipper, relations between Beijing and Tokyo took a nosedive for the worse, including large-scale protests in both countries, the cancellation of bilateral meetings on the ministerial level and above, and even the arrest of four Japanese citizens in China on the suspicion of illegally filming in a military area. On September 24, the Chinese skipper was returned, due to Japanese concerns over further damaging bilateral relations, and on October 9, all four Japanese citizens previously arrested were released from Chinese custody.

The Diaoyu/Senkaku island dispute in part overlaps with the unresolved historic animosity between both countries. Meaning, any major clash or event touching the islands also mobilizes Chinese nationalistic hacktivists into action.

(4) **Military alliance**: In the aftermath of World War II, Japan committed itself to a pacifist constitution, which under Article 9 proclaims that, "the Japanese people forever renounce war as a sovereign right of the nation and the threat or use of force as means of settling international disputes" (Japanese Constitution, 1946). The article continues to note that "in order to accomplish the aim of the preceding paragraph, land, sea, and air forces, as well as other war potential, will never be maintained. The right of belligerency of the state will not be recognized" (Japanese Constitution, 1946).

On September 8, 1951, Tokyo and Washington signed the 'Security Treaty between the United States and Japan,' which forms the bedrock of regional stability and US military power projection across the Indo-Pacific. Consecutive Japanese cabinets subsequently re-interpreted Article 9 to mean that the right of self-defense would still be permissible. As a result, Japan has build-up a self-defense naval, air, and ground force whose military budget is unofficially capped at 1% of GDP – a ceiling established by then Prime Minister Takeo Miki in 1976 (Wright, 2016, p. 3). According to the IISS' Military Balance 2019, Japan's annual defense budget is the eight highest in the world, currently standing at $47.3 billion USD (The Military Balance, 2019, p. 21).

As part of the US-Japan alliance agreement, Japan is also host to 23 US military bases and approximately 50,000 US soldiers. Among them, the 7th carrier fleet stationed at Yokosuka naval base, and the 18th Air Wing at Kadena AFB – the self- proclaimed "hub of airpower in the Pacific" (kadena.af.mil).

In terms of military activity, a look at the 2018 statistics published by the Japanese Ministry of Defense reveals that Japan's Air Self-Defense Force was "scrambled 638 times against Chinese aircraft, an increase of 138 times compared to the previous fiscal year" (MoD, 2019b, p. 1). In its 2018 Defense white paper, the Japanese MoD therefore noted that, "China's sea and air power is expanding its operational areas surrounding Japan, including the area around [the] Senkaku Islands" (MoD, 2018a, p. 3).

From a Chinese point of view, the US-Japan alliance is largely seen as a fulcrum to protect the geopolitical status quo and contain Beijing in East Asia and beyond. Chinese analysts however do diverge on ascertaining whether the US government is actively trying to push Tokyo to revise its pacifist constitution

[1] Note: Because Taiwan views itself as the only legitimate Chinese government, every historical territorial claim that Beijing puts forward, Taiwan emulates in its own way. This is true for the Diaoyu/Senkaku islands and the 9-dash line in the South China Sea.

over time, or whether Washington's influence is actually helping to push back against Japan's full-blown re-militarization desires (Glaser, 2015).

In cyberspace, Tokyo and Washington are both pushing for deeper cooperation and coordination. At the 2019 Japan-US Security Consultative Meeting, the allies affirmed that "international law applies in cyberspace and that a cyber attack could, in certain circumstances, constitute an armed attack for the purposes of Article V of the U.S.-Japan Security Treaty" (MOFA, 2019a, p. 1). To date, no cyberattack against Japan has breached this threshold.

2.1 Japanese cybersecurity & defense policy

On November 30, 1985, the roughly 300-member strong Japan Revolutionary Communist League – also called Chukaku-ha or Middle Core Faction (中核派) – simultaneously targeted 35 key rail communication and signal systems in and around Tokyo and Osaka. They slashed vital cables in gutters along tracks and set fires inside 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 "jammed police and rescue radio frequencies in an attempt to hamper and delay response by the authorities" (Littleton, 1995). The LA Times also 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." A de-facto pinpoint strategy that was not aimed at blowing up infrastructure, but severing critical control circuits to disconnect command and control systems and "causing disruption in cyberspace" (Littleton, 1995).[2]

It took another 15 years for the Japanese government to be eventually 'shocked' by two events to take cybersecurity and cyber defense increasingly seriously.

In reaction to Tokyo's decision to allow the go-ahead for a controversial conference in Osaka on January 23, 2000, titled 'The Verification of the Rape of Nanking: The Biggest Lie of the 20th Century,' Chinese nationalistic hacktivists mobilized on January 29 and bombarded Japanese government e-mail inboxes, redirected website queries to porn sites, and defaced several sites with anti-Japanese messages. Messages ranged from "Nippon [Japan] is rotten animal," to "Japanese - As all peoples know, it's a folk which has no concern to face the truth of history. They are the disgrace of Asia" (Watts, 2000). According to The Guardian and ScanNetSecurity, the hacktivists also wiped census data from the website of the government's statistical bureau, and tried to gain access to the Bank of Japan, the Foreign Ministry, the Ministry of Finance, the Ministry of Agriculture, Forestry, and Fisheries, the Labor Agency, the Defense Agency, and Japan's Management and Coordination Agency (BBC, 2000; ScanNetSecurity, 2000). The hacktivists signed off as the "Brazil p00 Hackerz" and "Billy in Hunan Province" (Watts, 2000; ScanNetSecurity, 2000)

On March 2, 2000, Japanese police investigators announced 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 over 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).

Combined with the Chinese hacktivist campaign one month prior, and the techno terrorism incident of 1985, the Japanese government decided to prioritize combatting the threat of "cyber terror" (サイバーテロ) front and center.

The Metropolitan police agency for example "set up a special squad of 50 police officers to investigate internet crime," and the government said it "will dispatch officials to the US to seek advice on measures to prevent cyber terrorism" (Watts 2000). On October 23, 2001, The Japanese Metropolitan Police also established the Council for Countermeasures

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

against Cyber Terrorism (サイバーテロ対策協議会) - which to this day encompasses an important role in Japanese law enforcement cooperation and coordination with key infrastructure providers.[3] The incidents also spurred the adoption of the special action plan to protect Japan's critical infrastructure from cyber terror, which includes measures such as reviewing critical infrastructure protection and establishing and strengthening public-private partnerships (ISMPO, 2000).

In reaction to the Chinese hacktivist onslaught, the Japanese Self-Defense Forces also decided to set-up military Computer Emergency Response Teams (CERTs) within the three service wings. The Air Force's Computer Security Evaluation Squadron (航空自衛隊システム監査隊) was create on May 8, 2000; the Ground Force's System Protection Technology Unity (陸上自衛隊システム防護隊) in 2001; And the Maritime Force's Communication Security Group (海上自衛隊保全監査隊) was founded in March 2002 (NISC 2004, p. 40).[4]

Over the years, the cyber terrorism narrative slowly crumbled as there was no clear definition on what the term cyber terrorism actually included and excluded. The Japanese police for example defined cyber terror as broadly as "an electronic attack on a critical system of critical infrastructure or a serious failure in a critical system of critical infrastructure" (MPD, n.d.). Already by 2004, Japan's Information Technology Promotion Agency concluded that "according to a strict definition of the term terrorism, there are no known cases of cyber terrorism to date" (IPA, 2004, p. 38).

In February 2006, the Information Security Policy Council (ISPC) released Japan's 'First National Strategy on Information Security.' The document particularly focused on raising cybersecurity awareness and creating a 'Japan Model' IT ecosystem - which was to be "regarded as a synonym for high quality, high reliability safety and security, or just simply to create 'a nation which should be revitalized by the value of trustworthiness'" (ISPC, 2006, p. 5). Overall, the document treated cybersecurity as a purely technical issue devoid of political and national security implications. Notably absent from the strategy were any mentions of advanced persistent threats (APT), state sponsored non-state actors, or even nationalistic hacktivists. Terrorism was mentioned only twice within the 33-page long document. And both times it was qualified as "crimes and terrorism" – following the trend that cyber terrorism was increasingly seen as a sub-threat of foreign government supported cybercrime.

In 2009, the ISPC published the 'Second National Strategy on Information Security.' The new document recognized for the first time the importance of international partnerships and the discussion of countermeasures in the context of national security and protecting critical information infrastructure (ISPC, 2009, p. 22). While cybercrime was prominently featured in the report, the threat of 'cyber terror' entirely disappeared.

In reaction to the July 2009 barrage of denial-of-service attacks against US and South Korean government, media, and financial websites, the ISPC pushed out the 'Information Security Strategy for Protecting the Nation' in May 2010 (Weaver, 2009; ISPC, 2010,). As Gady correctly highlights, "the document appears to lay out a distinct Japanese mindset of the time - seeing cyberattacks as analogous to unpredictable natural disasters rather than concrete actions of state and non-state adversaries" (Gady, 2017, p. 12-13).

In mid- to late-2011, multiple Japanese government servers eventually fell victim to targeted intrusions - including the Japanese House of Representatives, the House of Councilors, the Japanese Ministry of Foreign Affairs, the Ministry of Internal Affairs and Communications, multiple Japanese embassies across the globe, as well as Japan's largest defense contractor Mitsubishi Heavy Industries. The ISPC's 'Information Security 2012' report soberly assessed that "in 2011, threats of targeted attacks, cases of which were reported to have previously occurred overseas, emerged in Japanese government agencies. […] The risk of such possible sophisticated cyber attacks aimed at stealing important government information is expected to further escalate, and thus there is a strong demand for measures to improve and combat such a situation" (ISPC, 2012, p. 2-3).

In June 2013, the ISPC released Japan's first 'Cybersecurity Strategy.' The document emphasized that in the near future "there is potential for cyber attacks targeting vulnerabilities in the software of […] systems to directly result in obstruction of communications, transportation disorder, blackouts and other large social turmoil and possibly even deaths" (ISPC, 2013, p. 9). For the first time ever, the ISPC also highlighted the role of the Japanese Ministry of Defense in this new warfare domain. Given Japan's constitutional constraints on offensive operations, the document exclusively focused on the creation of a dedicated Cyber Defense unit within the Japanese Self-Defense Force, to support readiness and preparedness,

[3] The Council has been holding an annual conference since 2001 which brings together government officials and critical infrastructure operators, and serves as a coordinating venue to prepare for major events being held in Japan (ex. the Tokyo 2020 Olympic and Paralympic Games). On Dec. 6, 2018, 65 operators from 14 sectors – ranging from information and communications, finance, aviation, railway, power, gas, medical, water, logistics, chemical, credit, oil – participated in the conference (MPD, n.d.).

[4] For more information see CSS' upcoming "National Policy Snapshot: Japan."

improving surveillance capabilities, holding realistic exercises, training talented personnel, and carrying out advanced research and development. The strategy furthermore stressed the importance of the application of international law to cyberspace, cooperation with the United States in the context of the military alliance, as well as specifically providing technical and policy support to the 12 member states within the Association of Southeast Asian Nations (ASEAN) (ISPC, 2013, p. 49-51). Overall, Japan's first cyber strategy emphasized the creation of a resilient cyber nation, including close public-private partnerships and a multi-stakeholder approach to internet governance.[5]

In 2015, Washington and Tokyo eventually published the new 'Guidelines for Japan-US Defense Cooperation.'[6] Section 6 in the document outlines that the alliance partners will: "maintain a posture to monitor their respective networks and systems; share expertise and conduct educational exchanges; 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" (MoD, 2015). In the event of a serious cyber incident that affects the security of Japan, the guidelines note that the "two governments will consult closely and take appropriate cooperative actions to respond" (MoD, 2015).

In July 2018, the Japanese government published its third and latest Cybersecurity Strategy. Under point 4.3.2. the strategy emphasizes that "in order to protect Japan's national security interest from cyberattacks, it is important to secure Japan's resilience against cyberattacks and 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).

2.2 Chinese cybersecurity & defense policy

Parallel to Beijing opening itself up to the internet in the mid-1990s, Chinese military planners and domestic security services recognized the dangers of so-called 'informatization' – a ominous term that describes the comprehensive integration of information technology to impact all aspects of society and mechanisms of statehood – including domestic security and modern warfare (Griffiths, 2019, p. 35-43). While China did indeed implement sweeping internet regulations and filtering mechanisms prior to allowing commercial access to the internet in 1995 - whose elements Wired dubbed the 'Great Firewall of China' - the stranglehold was still lose enough for citizens to organize themselves online (Barme & Ye, 1997).

In 1999, Beijing's fears of 'informatization' eventually materialized when the spiritual Falun Gong movement – which encompassed an estimated 70 million practitioners in China at the time – organized large-scale protests in 30 cities, including 10,000 protesters amassing around Zhongnanhai - the headquarter of the Communist Party in Beijing - to demand legal recognition of the movement and freedom from state interference. According to Lewis, "the Internet was one of the primary tools used to organize the demonstrations" (Lewis, 2006, p. 1). What followed was a massive crackdown with hundreds of thousands Falun Gong practitioners arrested, and hundreds extrajudicially executed. Alongside this purge, the Chinese government also launched a propaganda campaign "the like of which had not been seen since the heights of the Cultural Revolution," including even DDoS attacks against websites overseas associated with the movement (Griffiths, p. 54; Denning, 2017).

In contrast to the initial hopes that the internet would foster democracy, solidarity, and allow for the free flow of information and ideas to and within China, Beijing has subsequently regulated, censored, filtered, and molded the Chinese internet to exercise political control over and through it. US President Clinton's mocking words when he declared in March 2000 that "China has been trying to crack down on the Internet. Good luck! That's sort of like trying to nail Jell-O to the wall," did not age well (NYT, 2000).

In November 2012, Xi Jinping was appointed General Secretary of the Communist Party and Chairman of the Central Military Commission. As one of his first acts in office he announced the creation of the so-called Central Leading Group for Cybersecurity and Informatization (中央网络安全和信息化领导小组). Over the years this high-level group chaired by Xi has become central to pulling together China's fragmented cyber-policy landscape and direct change from the top.

[5] Note: On February 10, 2015, the IPSC was absorbed into the Cyber Security Strategic Headquarters. See: NISC, 2015

[6] Note: The last time the Guidelines for Japan-US Defense Cooperation were overhauled was in 1997.

Overall Chairman Xi is currently aggressively pushing four interlocked concepts to reposition China in the world.

(1) **A harmonious internet** - Given China's broad concept of national security, which spans both domestic stability and countering threats from abroad, a harmonious internet seeks to guide public opinion, support good governance, and foster economic growth. To achieve these objectives, Beijing has been exercising ever-tighter control over the content posted online to stymie political mobilization and prevent any flow of information that might undermine the regime. In 2014, Xi established the Cyberspace Administration of China (CAC)(国家互联网信息办公室), which is subordinate to the Central Leading Group and tasked with "controlling online content, bolstering cybersecurity, and developing the digital economy" (Segal, 2018). While the CAC has been vital for the development of China's initial cyberspace governance framework, it also ran into numerous power struggles with other ministries unwilling to step aside – most notably the Ministry of Public Security, the Ministry of Propaganda, and the Ministry of Industry and Information Technology. In 2018, the Leading Group was upgraded to the Central Cyberspace Affairs Commission (中央网络安全和信息化委员会), allowing the CAC to "depend less on staff and resources loaned from relevant ministries and to exert greater authority over functional power centers across government." As a result, Creemers et al. expect the CAC to exercise "a stronger role in protecting China's critical information infrastructure and directing its technical censorship apparatus via the Great Firewall" (Creemers et al., 2018).

(2) **Cyber sovereignty** - To support and defend the harmonious internet from its critics abroad and at home, Beijing has endorsed the concept of state sovereignty in cyberspace. According to Xi, cyber sovereignty is "the right of individual countries to independently choose their own path on cyber regulation and internet public policies, and participate in international cyberspace governance on an equal footing" (FMPRC, 2015). As Adam Segal succinctly notes, "China envisions a world of national internets, with government control justified by the sovereign rights of states" (Segal, 2018).

While there are numerous Chinese laws and regulations that have increasingly expanded the legal basis for Chinese sovereignty in cyberspace, two laws are at its helm. In 2016, Beijing enacted the Cyber Security Law of the People's Republic of China (中华人民共和国网络安全法), which to date is "the most visible document in a wider Chinese effort to govern cyberspace and secure the country's digital infrastructure" (Triolo et al. 2017). According to Wagner, "the law requires network operators to cooperate with Chinese crime or security investigators and allow full access to data and unspecified 'technical support' to the authorities upon request. The law also imposes mandatory testing and certification of computer equipment for critical sector network operators" (Wagner, 2017). In terms of data localization, the law mandates that network operators in critical sectors store all data gathered or produced in mainland China. The law also bans "the export of any economic, technological, or scientific data that would pose a threat to national security or the public interest" (Wagner, 2017). The Cyber Security Law came into effect on June 1, 2017. Eight months later, Apple officially moved all of its Chinese iCloud operations to a local firm in southern China, and for the first time ever "began hosting its iCloud encryption keys in China, instead of the US" (Liao, 2018).

Enacted on July, 27, 2017, China's new National Intelligence Law (中华人民共和国国家情报法) "repeatedly obliges individuals, organizations, and institutions to assist Public Security and State Security officials in carrying out a wide array of 'intelligence' work" (Tanner, 2017). Article 2 starts by explaining that the law adheres to the "overall national security perspective," a term coined by Xi Jinping in 2014 which virtually puts every issue – whether military, political, economic, social, technological, cultural or otherwise – within the realm of intelligence collection. Article 7 then goes on to explain that "any organization or citizen shall support, assist, and cooperate with state intelligence work according to law." According to Tanner this is a calculated measure "to drive wedges of mistrust between U.S. or foreign citizens or firms, and their Chinese partners" (Tanner, 2017). It is also an expression that Beijing considers itself strong and economically important enough to "call for intelligence cooperation even from foreigners doing business in China" (Tanner, 2017).

(3) **Techno-Nationalism and military-civil fusion** In November 2012, Xi Jinping also set forward the political guideline of military-civilian fusion, which envisions a two-way technology transfer and a resulting interdependence between the military and the civil-industrial sector. Meaning, on the one hand, it encourages civilian participation in the development of military technology. On the other, it stipulates the application of military technology in the civilian realm. Military-civilian fusion walks in lockstep with the idea of techno-nationalism e.g. the notion of technological interdependence, a strong high-tech army, and dominance in the areas of AI, quantum computing, robotics, and the setting of international standards. To achieve this development trajectory as fast as possible, the 2019 Annual Report of the US Department of Defense to Congress notes that, "China uses a variety

of methods to acquire foreign military and dual-use technologies, including targeted foreign direct investment, cyber theft, and exploitation of private Chinese nationals' access to these technologies, as well as harnessing its intelligence services, computer intrusions, and other illicit approaches. In 2018, Chinese efforts to acquire sensitive, dual-use, or military-grade equipment from the United States included dynamic random-access memory, aviation technologies, and antisubmarine warfare technologies" (OSD, 2019, p. iii).

Falling into the same strategy of military-civilian fusion is also the rapid expansion of Chinese tech giants abroad and their ever-growing cooperation with the Chinese government domestically. Huawei and Tencent are probably the two most well-known examples, with the former accused of maintaining close links to the People's Liberation Army (PLA) and the Ministry of State Security (MSS), and the latter being an eager accomplice in implementing China's repressive policies at home, while partly owning popular computer games played by millions abroad – including Fortnite and PUBG (Singh, 2019; Cook, 2019).

Note: Some analysts suggest that the global expansion of Chinese high-tech companies and capital is synonymous to a digital Silkroad strategy and thus a supporting component to Beijing's Belt and Road initiative (CSIS, 2019).

(4) **Cybersecurity & defense** – Apart from the items already mentioned under the header of cyber sovereignty, China has "publicly identified cyberspace as a critical domain for national security and declared its intent to expedite the development of its cyber forces" (OSD, 2019, p. 64). According to the US Department of Defense, "PLA writings note the effectiveness of [information operation] and cyberwarfare in recent conflicts and advocate targeting an adversary's C2 and logistics networks to affect its ability to operate during the early stages of conflict. They credit cyberattacks on an enemy's C2 system with the potential to 'completely disrupt' these systems, paralyzing the victim and thus gaining battlefield superiority for the attacker. Accordingly, the PLA may seek to use its cyberwarfare capabilities to collect data for intelligence and cyberattack purposes; to constrain an adversary's actions by targeting network-based logistics, communications, and commercial activities; or to serve as a force multiplier when coupled with kinetic attacks during armed conflict" (OSD, 2019, p. 64).

In 2016, the PLA fused together disparate information warfare and cyber capabilities to create the Strategic Support Force (SSF)(中国人民解放军战略支援部队), which serves as "a theater command-level organization to centralize strategic space, cyber, electronic, and psychological warfare missions" (OSD, 2019, p. 48). The creation of the SSF is in line with Chinese thinking on 'cyberspace superiority' and "using offensive cyber operations to deter or degrade an adversary's ability to conduct military operations against China" (OSD, 2019, p. 57). The DoD further notes that "Chinese writings suggest cyber operations allow China to manage the escalation of a conflict because cyber attacks are a low-cost deterrent. The writings also suggest that cyber attacks demonstrate capabilities and resolve to an adversary. To support A2/AD, Chinese cyber attack operations aim to target critical military and civilian nodes to deter or disrupt adversary intervention, and to retain the option to scale these attacks to achieve desired conditions with minimal strategic cost" (OSD, 2019, p. 56).

As of this writing, – and according to open source - China has not conducted any offensive cyber operations against Japan that have touched the threshold for the use of force.

3 Threat landscape chronology

This section provides a chronological overview of relevant events between 2000 and 2019, pertaining to the interaction between Japan and the People's Republic of China in cyberspace. Gold marks events in which a technical and/or political attribution was made. Light blue marks events with no attribution assessment whatsoever, but whose targeting strongly overlaps with Chinese national interests. As far as open source information is available, there have been no reported cyber incidents in China that were attributed to Japan-based threat actors, nor any data breaches in China that might be considered to be in line with Japanese national security interests.

September regularly stands out historically as the month that sees very high activity from Chinese national hacktivists hitting Japanese targets. This activity relates to the anniversary of the Japanese invasion of Manchuria in September 18, 1931, and the establishment of the puppet state of Manchukuo. It is important to note that Chinese hacktivist do not mobilize every year with the same veracity. It ebbs and flows depending on other factors that are outside the purview of this paper. September 2011 for example was a very quiet month, possibly due to the ongoing Fukushima nuclear incident that captured headlines around the world. Meanwhile, September 2012 saw the largest onslaught of Chinese hacktivists to date due to the Japanese government officially purchasing the Diaoyu/Senkaku Islands on September 11, 2012.

Please also note that the month of September is an exception in terms of causality. It markedly stands apart from the more opportunistic driven Chinese hacktivist campaigns – such as when the Japanese Prime Minister visits the Yasukuni Shrine - or other Japan-related news that make their way onto Chinese social media and bulletin boards to inevitably serve as a reason to organize anti-Japanese campaigns.

The overwhelming majority of incidents listed below have little to no connection to historical dates or geopolitical events. To date, Chinese activity against Japan can overall be categorized as a persistent cyber espionage campaign in line with supporting China's long-term strategic interests.

Date **Incident announced** **(Incident occurred)**	**Events**
Jan. 29 2000 (Jan. 25-Jan. 30)	In reaction to Tokyo's decision to give the go-ahead to a controversial conference in Osaka, titled "The Verification of the Rape of Nanking: The Biggest Lie of the 20th Century," Chinese nationalistic hacktivists bombarded e-mail inboxes, redirected queries to porn sites, and defaced several Japanese websites with anti-Japanese messages. Messages included: "Nippon [Japan] is rotten animal," and "Japanese - As all peoples know, it's a folk which has no concern to face the truth of history. They are the disgrace of Asia." (Watts, 2000) According to The Guardian and ScanNetSecurity, the hacktivists wiped census data from the website of the government's statistical bureau, and tried to gain access to the Bank of Japan, the Foreign Ministry, the Ministry of Finance, the Ministry of Agriculture, Forestry, and Fisheries, the Labor Agency, the Defense Agency, and Japan's Management and Coordination Agency (BBC, 2000; ScanNetSecurity, 2000) In reaction to the onslaught, the "Metropolitan police agency set up a special squad of 50 police officers to investigate internet crime," and the government said it "will dispatch officials to the US to seek advice on measures to prevent cyber terrorism" (Watts 2000). The incident also spurred the adoption of a special action plan to protect Japan's critical infrastructure from cyber terrorism, including measures such as reviewing critical infrastructure protection, and establishing and strengthening public-private partnerships (ISMPO, 2000). The hacktivists signed off as the "Brazil p00 Hackerz" and "Billy in Hunan Province" (Watts, 2000; ScanNetSecurity, 2000)
March 2011 (March 2011-unknown)	According to CrowdStrike, **APT12/IXESHE** was targeting **Japanese organizations during the Fukushima nuclear disaster**, which was "most likely done to close intelligence gaps on the ground cleanup/mitigation operation" (Meyers, 2013).
July 10, 2011 (July 10-11, 2011)	A DDoS attack is launched against **Japan's National Policy Agency (NPA)**, temporarily making the website inaccessible. According to a statement released by the NPA, the attack was organized on a **major Chinese bulletin board**, in reaction to events surrounding the Diaoyu/Senkaku Island dispute (NPA, 2011).
Sept. 19, 2011 (August 2011)	Japanese defense contractor **Mitsubishi Heavy Industries (MHI)** is breached. In September Japanese media outlets report on the breach citing internal MHI documents. Japanese government officials are furious as this is the first time they hear of the MHI breach, because the company failed to report the incident to the authorities (McCurry, 2011). On September 21, Mitsubishi confirmed that it was breached but that no classified information was leaked (MHI, 2011). Overall, 83 computers in at least 11 locations were infected with eight different malware products. According to the New York Times, the "Tokyo headquarter, factories, and a

	research and development center were accessed in the breach" (Tabuchi, 2011). The BBC noted that "the viruses targeted a shipyard in Nagasaki, where destroyers are built, and a facility in Kobe that manufactures submarines and parts for nuclear power stations. [And] plant in Nagoya, where the company designs and builds guidance and propulsion systems for rockets and missiles" (BBC, 2011). MHI is a contractor for Raytheon and Lockheed and builds the F-15 fighter jet, Patriot missile defense batteries, as well as the AIM-7 Sparrow air-to-air missile in Japan. On October 24, Asahi reports that the attackers "likely netted military data on warplanes and information on nuclear power plants" (Kubota, 2011). Japanese defense contractor IHI Corporation and Kawasaki Heavy Industries also reported that they received malware-ridden emails for months, but their security systems filtered them out (Kubota, 2011).
Oct. 25, 2011 (July 2011)	According to the Asahi Shimbun, computers and servers used by the **Japanese House of Representatives** were infected when a Trojan was emailed to a Lower House member in July 2011. The attackers gained access to email communications and stole usernames and passwords. In early November, Deputy Chief Cabinet Secretary Isao Saito further explained that, "the upper house office has confirmed that seven suspicious emails, the same ones that were sent to the lower house, were found" (Phys.org, 2011) None of the **House of Councilor**'s email servers were compromised. (Phys.org, 2011). At the time, Sophos noted that although one exfiltration server was located in mainland China this was not sufficient evidence to leap to a Chinese operation (Cluley, 2011). In September 2013, Kaspersky released its report on **Icefog – a small Chinese APT group, possibly mercenaries for hire** - which focus on targets in South Korea and Japan. The report goes on to state that, "back in 2011, we analyzed malware samples that were used to attack several Japanese organizations. Among the attacked organizations were the Japanese **House of Representatives** and the **House of Councilors**" (Kaspersky Lab, 2013, p. 14).
Oct. 27, 2011 (unclear)	The Yomiuri Shimbun reports that "at least dozens of computers used at **Japanese diplomatic offices in nine countries** [Canada, China, France, Myanmar, The Netherlands, South Korea, and the US] have been infected with" an unspecified backdoor (Yomiuri Shimbun, 2011). The Japanese Foreign Ministry launched an investigation, "suspecting the infection was caused by so-called spear attacks targeting the ministry's confidential diplomatic information" (Yomiuri Shimbun, 2011). It is unclear whether the investigation has led to any results.
Oct. 28, 2011 (unclear)	According to then Minister of Land, Infrastructure, Transportation and Tourism, Takeshi Maeda, a server at **Japan's Geospatial Information Authority** (GSI) was illegally accessed. (Geospatialworld.net, 2011) The GSI noted that the affected server was used for "very long baseline interferometry, in which radio waves from stars are picked up through several antennas, and the difference in arrival time is used to measure distances" (Geospatialworld.net, 2011). No personal or confidential information was accessed, but scientific data may have been compromised. Some analysts speculate that the GSI server might have been targeted as a trusted hop-off point to compromise other government systems (Ryall, 2011).
January 6, 2012 (July 6, 2011-January 6, 2012)	The **Japan Aerospace Exploration Agency (JAXA)** discovers that "a computer terminal used by one of our employees was infected with a computer virus, and information stored in the computer as well as system information that is accessible by the employee have been leaking outside" (JAXA, 2012a). On March 27, the investigation concludes with the result that no classified data was stored on the affected system, and no sensitive data on the H-II Transfer vehicle (HTV) was leaked. According to JAXA, the infection vector was a malicious email send to an employee who "did not update the computer [Office automation] software" (JAXA, 2012b).
March 29, 2012 (June 2011-unclear)	Trend Micro publishes its report on **Luckycat**. It notes that "in addition to targeting Indian military research institutions, as previously revealed by Symantec, the same [cyber-espionage] campaign targeted **entities in Japan** as well as the Tibetan community. […] We were able to track elements of this campaign to **hackers based in China**" (Trend Micro, 2012, p. 1). While Trend Micro does not name any specific Japanese victims, it does state that "the Luckycat campaign […] has been linked to 90 attacks against targets in Japan and India as well as Tibetan activists. […] In sum the Luckycat campaign managed to compromise 233 computers" (Trend Micro, p. 1).
Sept. 18-19, 2012	The dispute over the Senkaku/Diaoyu islands intensifies as Tokyo decided to buy the islands on September 11 from the Japanese family who had owned them for the past 100+ years. The date of the purchase coincides with the anniversary of the Mukden Incident of September 18, 1931, which led to the Japanese invasion of Manchuria and establishment of the puppet state of Manchukuo On September 18 the **Honker Union** conducts DDoS attacks, doxing campaigns, and defacements against **19 Japanese websites**. According to the Japanese National Police Agency, 11 sites were hit with DDoS attacks, including the **Japanese Defense Ministry** and the **Ministry of Internal Affairs**. The **Japanese Supreme Court**, the **Tokyo Institute of Technology**. At least six other sites were defaced with the Chinese flag (NPA, 2012). At the Tokyo Institute of Technology, the hacktivists also leaked the names and telephone numbers of over 1000 staffers (Muncaster, 2012). Overall, the Honker Union shortlisted around 300 sites with over 4,000 individuals posting messages about planned attacks on the Chinese chat site YY. According to then Minister of Internal Affairs and Communication, Tatsuo Kawabata, the DDoS attacks were most intense on Sunday afternoon (September 16) with 95% of traffic originating from China (Kyodo News, 2012).

Nov. 30, 2012 (March 17, 2011-Nov. 21, 2012)	The **Japan Aerospace Exploration Agency** announces another breach (JAXA, 2012c). The leaked information possibly included specification and operation related information on numerous space launch vehicles. On February 19, 2013 JAXA publishes the results of its investigation. According to the press release a computer terminal was infected on March 17 with a spoofed email dated March 15. The release notes that, "access from the said terminal to an outside malicious website was detected between March 17, 2011 and November 21, 2012. The communication volume and contents were unknown, and we cannot deny the possibility that information has been leaked from the said terminal" (JAXA, 2013a).
January 1, 2013 (unknown)	Citing government sources, the Daily Yomiuri reports that the computer of an employee at the **Japanese Ministry of Agriculture, Forestry and Fisheries** had been infected last year. More than 3000 documents were exfiltrated, including 20 top-secret documents on the Trans-Pacific Partnership (TPP) free trade pact negotiations, documents on the Asia-Pacific Economic Cooperation Summit meeting in November 2011, and the Japan-US summit meeting in April 2012 (Phneah, 2013). The infected computer allegedly communicated with a server in South Korea.
Feb. 5,2013 (unknown)	The **Japanese Ministry of Foreign Affairs (MOFA)** announces that it was informed by the National Information Security Center (NISC) of a "suspicious communication from a computer within MOFA with an external server" (MOFA, 2013). The Ministry suspects that "approximately 20 documents were leaked from the computer" (MOFA, 2013).
Feb. 19, 2013	Mandiant releases its **APT 1** report.[7] By April 2014, Mandiant observes that APT 1 ceased almost all of its activities between February 13, 2013 to August 1, 2013 (Fung, 2014). Cylance also noticed "a fairly large lul in activity from March-August 2013," explaining that the "activity didn't cease entirely, but the volume of malware SPEAR was able to collect during this period was remarkably decreased" (Gross, 2016, p. 4).
April 23, 2013 (April 13-22, 2013)	The **Japan Aerospace Exploration Agency (JAXA)** is breached for the third time. On July 2, 2013, JAXA published the results of its investigation (JAXA, 2013b). According to the report one server - which stored the ID and passwords of four other servers - was compromised. Technical information related to the Japan Experimental Module "Kibo" (JEM) and the space station replenisher "Kounotori" (HTV) were exfiltrated. Personal email addresses were also leaked.
Sept. 25, 2013	Kaspersky releases its report on **Icefog**, which notes that the APT also targeted **Fuji TV** and the **Japan-China Economic Association** (Kaspersky Lab, 2013, p. 33).
Sept. 3, 2014	FireEye publishes a blogpost on **APT12/IXESHE** noting that the group "recently started a new campaign targeting organizations in Japan and Taiwan. APT12 is believed to be a cyber-espionage group thought to have **links to the Chinese People's Liberation Army**. APT12's targets are consistent with larger People's Republic of China (PRC) goals" (Moran & Oppenheim, 2014).
Sept. 10, 2014	FireEye publishes its report titled 'Operation Quantum Entanglement' which identifies two separates yet connected campaigns. The first is the Moafee group, which operates out of Guangdong province and targets "governments and militaries of countries with national interests in the South China Sea" (Haq et al. 2014, p. 17). The second is the **DragonOK** group operating out of **Jiangsu province**, "which targets **high-technology and manufacturing companies in both Japan and Taiwan**" (Haq et al. 2014, p. 4). The report explains that "DragonOK used similar malware to the Moafee group. Specifically, we observed DragonOK employing PoisonIvy, Nflog, Mongall, CT, and NewCT" (Haq et al. 2014, p. 19). The report goes on to note that, "we believe that these groups are from two distinct regions in China and possibly (1) are collaborating, (2) received the same training, (3) have a common toolkit supply chain, or some combination of these three" (Haq et al. 2014, p. 3).
November 12, 2014	Symantec reports that **CloudyOmega** actively exploited an Ichitaro zero-day in the wild (Japanese Office Suit Software) to target Japanese organizations. Symantec traces CloudyOmega's campaign back to at least 2011. According to the blogpost "the **public sector in Japan** is the most targeted sector hit by Operation CloudyOmega" (Symantec, 2014). Other Japanese sectors include**: the chemical sector, the financial sector, trading companies, conglomerates, and think tanks**.
April 14, 2015 (January-March 2015)	On April 14, Palo Alto Network's Unit 42 identifies a new **DragonOK** backdoor deployed against Japanese targets in at least five phishing campaigns. According to the blogpost "all five phishing campaigns targeted a **Japanese manufacturing firm** over the course of two months, but the final campaign also targeted a separate **Japanese high-tech organization**" (Miller-Osborn & Grunzweig, 2015).
June 1, 2015 (May 8-23, 2015)	The **Japanese Pension Service (JPS)** is breached. Since May 8, JPS received 124 malicious emails. Five staffers opened some of them and the infection spread to 31 computers. Between May 21-23 the personal information of 1.25 million Japanese citizens was exfiltrated. On June 1, the JPS publicly announced in a press conference that its network was breached (JPS, 2015). The total amount for remediation cost and recovery is calculated to be around $8 million USD (Kakumaru et al. 2016, slide 4). On May 20, 2018, Japanese law enforcement closes the criminal investigation without any results. On November 6, 2015, JP-CERT/CC notes that the attack against the "Japan Pension Service indeed drew nationwide attention, but **Emdivi** has victimized several other government and private organizations. This attack campaign, specifically targeting Japan, is also known as '**CloudyOmega**' named by Symantec, or '**Blue Termite**' by Kaspersky" (Kubo & Kubo, 2015). As of this writing, the exfiltrated documents of neither breach have been used for malicious purposes, which likely indicates that they are

[7] For the full report see: Mandiant, 2013

	used for operational purposes by a foreign government agency. Note: Around the same time in June the US Office of Personnel Management announced that it was breached and the personal information of 22.1 million US government employees was exfiltrated.
August 14, 2015	Raytheon submits its secret report on **Stalker Panda** to the US government. The report notes that the group has possible links to the **PLA** and has conducted "targeted attacks against **Japan**, Taiwan, Hong Kong, and the United States" […] centered on **political, media, and engineering sectors**" (Raytheon, 2015, p. 1).
August 20, 2015	Kaspersky releases its findings on **Blue Termite** – noting that the Chinese cyberespionage campaign "has been targeting **hundreds of organizations in Japan**" **since 2013** (Kaspersky Lab, 2015).
June 9-25, 2015 (unclear)	In the aftermath of the JPS breach, several Japanese organizations also report that they have been targeted/breached by **Blue Termite/CloudyOmega/EMDIVI**, including: The **Petroleum Association of Japan** (June 9), the **Tokyo Chamber of Commerce and Industry** (June 10), the **National Institute for Health Services** (June 13), the **Japan Energy Service Corporation** (June 17), **Waseda University** (June 22), and the **Japanese Ministry of Justice** (June 25) (Kakumaru et al. 2016, slide 5).
Feb. 24, 2016 (2010-X)	Cylance releases its report on Operation **Dust Storm** which became active around 2010. The report notes that "attack telemetry in 2015 indicates the Dust Storm group has migrated from more traditional government and defense-related intelligence targets to exclusively seek out organizations involved in **Japanese critical infrastructure and resources**. The group recently compromised a wide breadth of victims across the following industry verticals: **electricity generation, oil and natural gas, finance, transportation, and construction**" (Gross, 2016, p. 1). Cylance also highlights an attack by Dust Storm in early February 2015 targeted an **unnamed "investment arm of a major Japanese automaker**" (Gross, 2016, p. 4). And it also discovered two campaigns in July-October 2015 against an **unnamed Japanese subsidiary of a South Korean electric utility** and **an unnamed major Japanese oil and gas company** (Gross, 2016, p. 6).
April 28, 2016 (2006-X)	Symantec releases a blog post on **Tick/Bronze Butler** noting that "a longstanding cyberespionage campaign has been targeting mainly Japanese organizations with its own custom-developed malware. The group, known to Symantec as Tick, has maintained a low profile, appearing to be active for at least 10 years prior to discovery. […] Tick's most recent attacks have concentrated on the **technology, aquatic engineering, and broadcasting sectors in Japan**" (DiMaggio, 2016a). On Oct. 12, 2017, Secureworks releases its threat analysis on **Tick/Bronze Butler**. It notes that the group "**likely originates in the People's Republic of China**" and has run a long-standing campaign intended to "exfiltrate intellectual property and other confidential data from Japanese organizations" (Secureworks, 2017).
November 2016 (July 1, 2014-October 2016)	The **Japanese Business Foundation (Keidanren)** officially reports that its network has been breached. On July 1, 2014, the Keidanren's International Cooperation Bureau received an email with a malicious attachment that triggered the breach (most likely a backdoor). According to Asahi, the e-mail was sent from an organization that Keidanren officials often worked with, and which was involved in the bilateral relations with China. It was later uncovered that the computer system of that organization had also been hacked earlier. On July 3, a remote access tool was installed on the Keidanren system. Two months later the exfiltration of documents and emails began to a server based in China's Guangdong province (Sudo, 2019). It wasn't until early October 2016 that Keidanren officials were informed by the company overseeing its computer system that suspicious transmissions had been uncovered. According to Kyodo News, the "investigative team found a large amount of suspicious data communications between 10 external servers and 23 infected PCs" (Kyodo News, 2019). Keidanren eventually paid several hundreds of millions of yen to replace its computer system. It is not entirely clear from open source reporting whether APT10 was responsible or not.
Nov., 2016 (September 2016)	According to Kyodo News, the **Defense Information Infrastructure (DII)** - which is the name for the **joint network of Japan's Self-Defense Forces** – was targeted by a "sophisticated cyberattack" (Kyodo, 2016). The news report notes that "possibly a state actor, […] gained unauthorized access to computers at the National Defense Academy and the National Defense Medical College, using them as a gateway to enter the [Ground Self-Defense Force's] computer system" (Kyodo, 2016). According to Kyodo News, "the incident prompted the ministry and the SDF to temporarily ban internal internet use" (Kyodo 2016). To date, no open-source information is available as to what infected the DII, how far it penetrated into the network, nor whether any data was actually compromised or exfiltrated.
January 2017 (unclear)	FireEye reports in July 2017 that: **APT10** sent an email related to an annual budget for scientific research to a **Japanese government agency** to deliver the HAYMAKER and BUGJUICE malware. APT10 targeted a **Japanese manufacturer** with an email lure related to China's defense strategy and news events such as the assassination of Kim Jong-Nam. APT10 also targeted a Japanese company in the **media and entertainment industry** (APSM, 2017).
April 2017	BAE Systems and PwC UK release their report on **Operation Cloud Hopper/APT10**. According to the report, "in a separate operation, APT10 has been systematically targeting **Japanese organization**" using ChChes malware, which shares infrastructure with APT10 but exhibits operational differences – suggesting a "potential sub-

	division within the threat actor" (PwC & BAE Systems, 2017, p. 9). In July 2017, Trend Micro publishes a blog post on the **ChessMaster** campaign which targets "**Japanese academia, technology enterprises, media outfits**, **managed service providers**, and **government agencies**" (Sy et al. 2017). The post also explains overlaps between APT10, Blue Termite/EMDIVI, and ChessMaster.
July 2018 (unclear)	FireEye reports that it "detected and blocked what appears to be **APT10** (Menupass) activity targeting the **Japanese media sector**" (Matsuda & Muhammad, 2018). The group used malicious emails that installed the UPPERCUT backdoor (ANEL)
Dec. 21, 2018	In reaction to the US DoJ indictment of two Chinese hackers associated with the **Ministry of State Security/APT10**, the Japanese Ministry of Foreign Affairs releases a statement on APT10 (MOFA, 2018).
July 24, 2019 (2011-X)	German public broadcasters BR and NDR release their investigation into **Winnti**, noting that it is a **"presumably China-based" "digital mercenary"** group that is "attacking companies in **Japan**, France, the U.S. and Germany" (Tanriverdi et al. 2019). The report further notes that Winnti targeted Japan's biggest chemical company, **Shin Etsu Chemical**, in 2015, and penetrated the networks of **Sumitomo Electric** in the summer of 2016 (Tanriverdi et al. 2019).

4 Japanese teams targeting China

The Japanese MoD has a defensive framework in place for responding to cyberattacks against its own information systems, but the Japanese Self-Defense Forces do currently not have the legal authority to offensively engage adversaries outside the MoD's wire during peacetime (MoD, n.d.). That being said, the overhaul of the National Defense Guidelines in December 2018 has lain the groundwork for allowing the SDF to – in case of an armed attack against Japan - "block and eliminate the attack by leveraging capabilities in space, cyber and electromagnetic domains" (Cabinet Secretariat, 2018, p. 12). According to the guidelines, this also includes capabilities to disrupt an opponent's use of cyberspace amidst an attack against Japan (MoD 2018b, p. 20).

In 2019, the MoD outsourced the development of offensive cyber capabilities to one or several unnamed private Japanese companies – mirroring the MoD's cooperation with Fujitsu in 2012.[8] The conceptual idea 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 anyone's best guess.

The most likely route will be that the SDF's Cyber Defense Group (サイバー防衛隊) will become the MoD's tip of the spear.[9] The Group was established in May 2013 (Nikkei, 2013) and politically consolidated in June with the adoption of Japan's first Cybersecurity Strategy (ISPC, 2013, p. 42). Currently, the Cyber Defense Group serves as the milCERT for the SDF's joint network - called the Defense Information Infrastructure. Meaning, the Group's capabilities are similar to the CERT teams within the three SDF service wings.[10] In FY2019, the SDF's Cyber Defense Group is set to increase its staffing from 150 to 220 (MoD, 2018c, p. 6). For FY2020, the plan is to increase that number to 290 (MoD, 2019c, p. 6).[11] As of this writing, the SDF has not conducted any offensive cyber operations against Chinese targets.

There is little to no open-source information available as to what Japan's intelligence agencies are doing in cyberspace. According to a 2008 NSA memo published by The Intercept in 2018, the MoD's Directorate for Signal Intelligence (DFS)(電波部) is "still caught in a Cold War way of doing business," which makes it "very hard to engage with them in multinational forums or even to get them to collaborate across Japanese government lanes. Bilaterally (NSA-DFS) they are a good partner, but they are very reluctant to participate with mixed or larger groups" (The Intercept, 2017, p. 1). The small trove of NSA documents tackling the DFS shows that the directorate has been learning from the NSA since 2012 to set up its own "SIGINT-enabled cyber operations" to enhance and streamline DFS' data collection efforts (The Intercept, 2018). It is unknown whether the DFS, or any other Japanese intelligence agency – most notably the Cabinet Intelligence and Research Organization (CIRO), the MoD's C4 Systems Department (J6), or the Ministry of Justice's Public Security Intelligence Agency (PSIA) - have conducted any computer intrusions into Chinese systems.

As far as available open source information goes, there are also no known Japan-based non-state actors that have targeted Chinese companies or government agencies. Please note that, given the lack of in-depth research on Japanese non-state actors in cyberspace, this assessment is very shaky. Future historical research might reveal dynamics that we know little about today.

Disclaimer: Research inquiries send to the Chinese International Press Center (IPC) – to get in touch with the Chinese Ministry of Defense and the Ministries of Public and State Security – went unanswered despite several follow-up emails. Similarly, getting in touch with information security vendor Qihoo 360 - to gain insights into China's threat landscape - were sadly unsuccessful.

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

[9] Note: In the official English translation, the provisional name for the Cyber Defense Group was "Cyber Defense unit" (small u). Its official name now is the Cyber Defense Group.

[10] Staffing numbers for the three service wing CERTs: The GSDF System Protection Unit (Army)(FY2020: ~140 personnel), the MSDF Communication Security Group (Navy)(FY2020: ~100 personnel), and the ASDF Computer Security Evaluation Squadron (Air Force)(FY2020: ~130 personnel).

[11] The Cyber Defense Group is a joint unit and thus draws its members from the three service wings.

5 Chinese teams targeting Japan

The number of Chinese teams hitting Japanese assets can be roughly divided into four categories: Nationalistic hacktivist, the People's Liberation Army, The Ministry of State Security, and contractors/ mercenaries-for-hire. This section discusses the various actors, their characteristics, preferred targets and tooling as per open source information available.

Note: The section tries to differentiate between proprietary and widely available tooling. However, the line between these two categories is not as steadfast as the terminology suggests. Widely available tools are broadly defined all those pen-testing and red team tooling that is either legitimate (ex. Mimikatz), or whose malware products are extensively used by a number of different ATP threat actors/cybercriminals. On the other hand, proprietary tools are defined as custom designed malware products that are exclusively used by one particular threat actor or group of threat actors. The author recognizes that this categorization is not perfect, and that depending on one's visibility, some proprietary tools could be classified as being widely available.

Disclaimer: Security vendors do occasionally disagree on whether a certain group is responsible for a specific campaign or targeted infection. This paper recognizes that the art of technical attribution has its limitations and difficulties, and that not every security vendor will agree with every attribution assessment made. Similarly, this paper understands that it is generally inappropriate to attribute an attack to a group solely based on the malware deployed or infrastructure used. Please also note, that each major vendor has their own APT naming convention.[12]

5.1 Nationalistic Hacktivists

In the late 1990s, Chinese nationalistic hacktivists mobilized for the first time when riots broke out across Indonesia in 1998, and when the US accidentally bombed the Chinese embassy in Belgrade during the Kosovo conflict in 1999.

In the Indonesian case, Chinese netizens were outraged when news of targeted attacks against Chinese-Indonesians reached the international ethnic Chinese communities. The May 1998 riots were subsequently labelled as "anti-Chinese" and Chinese netizens set up discussion boards and social media groups to organize defacements of Indonesian government websites (Desombre & Byrnes, 2018). As Dsombre and Byrnes explained, "many of these boards evolved into the first Chinese hacking groups" (Desombre & Byrnes, 2018, p. 6).

One year later, the death of three Chinese reporters amidst the US bombing of the Chinese embassy in Belgrade, sparked numerous DDoS attacks against NATO email servers, defacements of US government websites, and a flood of malware-ridden emails targeting NATO and US government officials (Stout, 1999). Out of the ashes - of what Wired labeled the "first Internet war" - emerged the largest and most prominent Chinese hacktivist collective – the Honker Union of China – which although fragmented, remains active today.[13]

Honker Union (中国红客)

Tooling
Proprietary: Unknown Widely available: Various; HTran
Targets
Targets designated by geopolitical events. Predominately, Japanese ministerial and agency websites, and Japanese bulletin boards.

The Honker Union emerged during the late 1990s and primarily gravitated around the long-standing cnhonker.com forum. Over the years, many Union members ventured into the legitimate cybersecurity sector and provided insights into the group. In a 2013 interview with the South China Morning Post, former Union member Liu Qing for example explained that, "I am mature businessman now, but I am proud to have participated in a patriotic cyberwar back then" (Nan, 2013). According to Liu, he joined the Union after the Hainan Island Incident in April 2011, when an EP-3 US spy plane collided with a J-8 Chinese jet fighter in mid-air. The body of the Chinese pilot was never recovered and the US plane had to conduct an unauthorized emergency landing at the PLA's Lingshui air base. According to Liu, hundreds of Chinese websites suffered attacks believed to have originated from the US in the aftermath of the incident – leading Liu and others to discuss counterstrike plans. As Liu put it "we were so angry and decided to fight back" (Nan, 2013). For the Honker Union the counter-US campaign on May 1, 2001 was a landmark event. According to the SCMP, "the group attracted more than 80,000 members in the following months, making it the largest hacker organization to date in China's internet history" (Nan, 2013).

Soberly looking back however, one has to conclude that this episode of hacktivist mobilization was one of severe over-interpretation and misguided media reporting. Back in late-April 2001, Jericho and Sioda over at Attrition.org summarized it aptly when

[12] For additional APT aliases see: MISP, n.d.; MITRE Att&ck, n.d.; ThaiCERT, 2019

[13] The term "honker" literally translates into "red guest" in Chinese, e.g. "black hat."

they noted that: (a) Website defacements happen all the time, (b) the US hackers that defaced Chinese websites initially had no political agenda at all (Poisonbox and Pr0phet), and (c) after Wired reported about an ongoing US hacker campaign against China – without actually providing any tangible evidence –, the whole story developed its own dynamics. As Jericho and Sioda put it, “the collective dick-waving of a bunch of script-kidiots fueled by so-called journalists generating media hype” led to “the former trying to feed their egos and the latter to feed their hit counts” (Jericho & Sioda, 2001).

In 2010, the Honker Union prominently went to “war” against Iran, after the Iranian Cyber Army hijacked the DNS records of China’s most popular search engine Baidu to redirect its traffic to a website featuring the sentence "protesting the military intervention of foreign and Israeli sites in our internal affairs division and distribution of false news” (Danchev, 2010). It is still unclear why the Iranian Cyber Army targeted Baidu in the first place, nor whether they expected Chinese hacktivists to just simply stand by and watch. Naturally, it did not take long for several Iranian websites to be DDoS’d, defaced with Chinese flags, and plastered with messages such as "We are China’s hacker! Let the world hear the voice of China! The state is higher than the dignity of all!" (China Economic Review, 2010).

Today the Honker Union is largely “fragmented and divided between several different forums, with different levels of activity” (Edwards, 2018). This structure works rather well to strengthen Chinese hacktivism at large, as most platforms maintain a hierarchical structure that actively trains new members on the lower levels, and hones the skills of advanced actors at the top. Meaning the Union can mobilize quantity over quality without degrading its advanced operations.

Despite rumors to the contrary, it is unclear whether the Honker Union, or any of the other Chinese hacking communities, had or do currently maintain direct ties to the Chinese government, military, or the intelligence services. It is highly likely that the line between nationalistic hacktivism and working for the Chinese government is murky at best, non-existent at worst.

Note: HTran, also called the HUC Packet Transmit Tool, was written by Honker Union member lion and bkbll in 2003 (lion & bkbll, 2003). It is a “rudimentary connection bouncer, designed to redirect TCP traffic destined for one host to an alternate host” (Stewart, 2011). Its primary purpose is to “disguise either the true source or destination of Internet traffic in the course of hacking activity” (Stewart, 2011). HTran is widely used outside the Chinese hacktivism scene, including by Chinese threat actors such as APT1, APT12, and DragonOK (Bureau & Jennings, 2018).

LuckyCat

Tooling
Proprietary: Unknown Widely available: Sparksrv and Comfoo malware variants; Sojax malware;
Targets
Indian military research organizations; South Asian shipping companies (some in Malaysia); Japanese entities’ Tibetan community and activists

Contrary to the ‘loud’ activities by the Honker Union, the LuckyCat hackers are one prominent example of a ‘silent’ campaign executed by members of the Chinese hacking community.

Symantec was the first to publicly report on the LuckyCat campaign back in March 2012. According to the report, the group conducted a series of attacks against Indian military research and South Asian shipping organizations. The data stolen varied from case to case, but appeared to be simply geared at documents with suggestive names. Meaning, the hackers also inexplicably exfiltrated documents that were publicly available on the victim’s website. All in all, Symantec describes the attackers as “us[ing] very simple malware, which required little development time or skills, in conjunction with freely available Web hosting, to implement a highly effective attack” (Symantec, 2012a, p. 1).

Later in the same month, Trend Micro took a deeper dive into LuckyCat. In terms of targeting, Trend Micro highlighted that the campaign was linked to at least “90 attacks against targets in Japan and India as well as Tibetan activist” (Trend Micro, 2012, p. 1). Trend Micro also uncovered significant overlaps with other campaigns, including ShadowNet and DuoJeen. The former historically targeting Tibetan activists abroad, while the latter targets the Tibetan community within China (Trend Micro, 2012, p. 12-17).

In terms of attribution, Trend Micro “connect[ed] the email address used to register one of LuckyCat’s command-and-control servers to a hacker in the Chinese underground community. He used the nickname ‘dang0102,’ and published posts in the famous [Chinese] hacker forum, XFOCUS, as well as recruited others to join a research project on network attack and defense at the Information Security Institute of the Sichuan University” (Trend Micro, 2012, p. 2). Symantec’s findings concur with Trend Micro’s attribution assessment, noting that “45 different attacker IP addresses were observed. Out of those, 43 were within the same IP address range based in Sichuan province, China” (Symantec, 2012a, p. 2).

5.2 People's Liberation Army (PLA)

As early as 2002, the first reports emerged that a group operating out of Shanghai and linked to the People's Liberation Army was conducting computer exploitation against US government organizations. According to a 2008 Wikileaks cable, the US State Department's Bureau of Diplomatic Security explained that Byzantine Candor - also known as the Comment Group – hit the "U.S. Army, […] other DoD services, as well as [Department of State], Department of Energy, additional [US government] entities, and commercial systems and networks" (Wikileaks, 2008). In 2013, Mandiant published its groundbreaking APT1 report, which identified APT1 as the 2nd Bureau of the PLA's 3rd Department – also known as Unit 61398 - operating out of the Pudong New Area in Shanghai (Mandiant, 2013, p. 3 & 26). The Comment Group was APT1's first known campaign against a foreign government. On May 1, 2014, the US Department of Justice indicted five PLA officers – all members of Unit 61398 - for "computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries" (US DoJ, 2014). According to then U.S. Attorney General Eric Holder, the case represented "the first ever charges against a state actor for this type of hacking" (US DoJ, 2014).

Responding to these development Foreign Ministry Spokesperson Qin Gang, merely stated that "the Chinese government, the Chinese military and their relevant personnel have never engaged or participated in cyber theft of trade secrets" (Xinhua, 2014).

Two PLA-connected Chinese teams are known to have hit Japanese assets.

APT1/Comment Group

Tooling
Proprietary: PoisonIvy variants; SeaSalt Widely available: Various; Mimikatz
Targets
Primarily US focused: IT sector, aerospace, public administrations, satellites and telecommunications, scientific research and consulting, energy, transportation, construction and manufacturing, international organizations, engineering services, high-tech electronics, legal services, media and entertainment, navigation, chemicals, financial services, food and agriculture, metals and mining, healthcare, and education

APT1 gained notoriety when Mandiant released its report in 2013, aptly titled "APT1: Exposing One of China's Cyber Espionage Units." Mandiant connected APT1 to activity by the Comment Group in 2002 and observed the group compromising 141 companies spanning 20 industrial sectors since 2006. The majority of APT1 targets were located in the US (115), with only one unnamed target located in Japan (Mandiant, 2013, p. 22).

After the release of the Mandiant report, APT1 delayed its return to normal operations following the Chinese New Year holiday in February 2013. It eventually re-emerged six months later after shifting its operational infrastructure. With the Chinese government vehemently denying any connection to APT1, Mandiant's Laura Galante rightly noted that, because "APT1 is supporting this denial storyline the government is telling, [it] shows that they wanted to be seen as not actively doing this, or at least to cover up their involvement" (Fung, 2014). It is not exactly clear when APT1 ceased its activity after re-emerging in August.

Note: In 2018, McAfee uncovered code based on APT1's Seasalt malware – which the group last used in 2010 - in a new implant McAfee named OceanSalt. The curious part of the story is that the "source code used by APT1 never became public, nor did it wind up on the black market" (Barrett, 2018). McAfee therefore suggest two possible explanations. Either APT1 has returned, or another adversary is conducting a false-flag operation to suggest that APT1 has re-emerged (Samani & Sherstobitoff, 2018). Given the exposure of APT1 in 2013, it is highly likely that the group was split and its tooling disseminated to other PLA teams with better operational security.

APT12/IXESHE/DynCalc

Tooling
Proprietary: Various backdoors including RIPTIDE/Etumbot, THREEBYTE, HIGHTIDE, WATERSPROUD, IXESHE, and Aumlib. Widely available: Various; HTran
Targets
Japanese high-tech companies, media outlets, telecommunications sector, government organizations

In October 2012, APT12 famously breached the computers of 53 employees at the New York Times (Perlroth, 2013). According to then NYT chief information officer Marc Frons, "they could have wreaked havoc on our systems. […] But that was not what they were after" (Perlroth, 2013). As the NYT reported four month later, APT12 "appeared to be looking for […] the names of people who might have provided information to [NYT Shanghai bureau Chief] [David] Baboza," who published an investigative piece on October 25, 2012, titled the "Billions in hidden riches for family of Chinese leader" (Perlroth, 2013). Based on thousands of corporate documents, Barboza uncovered and published a piece investigating the relatives of Wen Jiabao – then China's Prime Minister –

who had accumulated a fortune through shady business dealings (Barboza, 2012).[14]

Notably, APT12 also targeted Japanese organizations during the Fukushima nuclear disaster in 2011, which, according to CrowdStrike, was "most likely done to close intelligence gaps on the ground cleanup/mitigation operation (Meyers, 2013).

FireEye posits that "APT12 is believed to be a cyber espionage group thought to have links to the Chinese People's Liberation Army. APT12's targets are consistent with larger People's Republic of China (PRC) goals. Intrusions and campaigns conducted by this group are in-line with PRC goals and self-interest in Taiwan" (FireEye, n.d.).

One particular characteristic of APT12 is that it closely monitors online media related to its tooling and operations. Meaning, it adapts very quickly to public exposure by using new tools, tactics, and procedures (Moran & Oppenheim, 2014). Additionally the group likes to hide its activities by using compromised machines within a target's internal network as command and control servers. It also uses the open-source proxy tool HTran to mask its true location (Sancho et al., 2012, p. 15).

5.3 Ministry of State Security (MSS)

It is not entirely clear when exactly China's main intelligence agency - the Ministry of State Security – made its entry into the field of cyber espionage. Three MSS connected APTs have stood out in recent years due to being doxed by the ominous group known as Intrusion Truth.

Starting in 2009, APT10 conducted numerous espionage campaigns against US defense industrial base companies, the technology and communications sector, as well as multiple companies around the world relevant to China's innovation and economic development goals (PwC & BAE Systems, 2017, p. 5). In 2017, PwC and BAE Systems uncovered the most notable APT10 operation to date, dubbed Cloud Hopper. The op primarily targeted managed IT services providers (MSPs), which allowed APT10 "unprecedented potential access to the intellectual property and sensitive data of those MSPs and their clients globally" (PwC & BAE Systems, 2017, p. 4). On August 15, 2018, Intrusion Truth revealed that APT10 was managed out the Tianjin bureau of the Chinese Ministry of State Security (Intrusion Truth, 2018). Five months later, the DoJ unsealed an indictment against two APT10 members for "conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft" (US DoJ, 2018).

Dubbed Operation Aurora by security vendor McAfee in January 2010, APT17 targeted at least 34 companies in the technology, financial and defense sectors starting in late-2009 (Goodin, 2010). Using a zero-day in Internet Explorer and "nearly a dozen pieces of malware and several levels of encryption to burrow deeply into the bowels of company networks," APT17 was "highly successful in obfuscating the attack and avoiding common detection methods" (Zetter, 2010). Dmitri Alperovitch, then vice president of threat research at McAfee, explained that "we have never ever, outside of the defense industry, seen commercial industrial companies come under that level of sophisticated attack" (Zetter, 2010). On July 24, 2019, Intrusion Truth offered proof that APT17 was run out of the Jinan bureau of the Chinese Ministry of State Security (Intrusion Truth, 2019a). Similar to Chinese threat actor group APT41, APT17 also exhibited hallmarks of financially motivated cybercriminal operations (Lyngaas, 2019b). According to Intrusion Truth, members of APT17 circulated a data for sale list amongst the Chinese hacking community which also included packages on Chinese citizens (Intrusion Truth, 2019b). As of this writing it is unclear whether the MSS has lost control over APT17, or Intrusion Truth has lain down a false flag to create friction between the MSS and APT17.

[14] Note: Prime Minister is the informal westernized title. The official Chinese description is 'Premier of the State Council of the People's Republic of China.'

Up until 2015, APT3 primarily targeted US and UK-based aerospace, defense, telecommunications, and transportation companies before shifting inward and honing in on Hong Kong-based political targets (Symantec, 2016). On May 9, 2017, Intrusion Truth identified APT3 (Boyusec) as a Chinese contractor working for the MSS (Intrusion Truth, 2017). Four months later the US Department of Justice unsealed an indictment against three Boyusec members for "computer hacking, theft of trade secrets, conspiracy and identity theft" (US DoJ, 2017). As of this writing, Boyusec has not resurfaced.

At least four MSS connected teams have struck targets in Japan.

APT10/MenuPass/Stone Panda

Tooling
Proprietary: PlugX/TinyX; REDLEAVES RAT; Sogu/Kaba, ChChes, Haymaker, Uppercut (ANEL), Snugride, Bugjuice backdoor Widely available: China Chopper, PsExec, gsecdump, Mimikatz, Powersploit, QuasarRAT
Targets
Worldwide; Broad spectrum of target industries

APT10 has been active since at least 2009 and has "historically targeted construction and engineering, aerospace, and telecom firms, and governments in the United States, Europe, and Japan" (FireEye, n.d.).

After PwC and BAE Systems' write-up on the Cloud Hopper campaign in 2017, several security vendors also reported other APT10 campaigns conducted in the same year. According to a SCMP article published in April 2018, FireEye identified two APT10 campaigns against Japanese targets between September and October 2017. Curiously the malware used also included taunting lines of text, including such gems as: "I'm here waiting for u," "POWERED BY APT632185, NORTH KOREA," and "According to the analysis report, some Japanese analysts have always been portrayed as a bit of a joke" (SCMP, 2018).

In February 2019, Insikt Group and Rapid7 reported and attributed with "high confidence" an APT10 campaign that took place between November 2017 and September 2018. According to the analysis, the targets included Visma – "a billion-dollar Norwegian [MSP] company with at least 850,000 customers globally" –, an international apparel company, and a US law firm with "strong experience in intellectual property law with clients in the pharmaceutical, technology, electronics, biomedical, and automotive sectors, among others" (Insikt Group & Rapid7, 2019, p. 1). However, several security researchers took issue with the attribution assessment. Benjamin Koehl, an analyst at Microsoft's Threat Intelligence Center tweeted that, "this activity is not APT10. It is all APT31 (or ZIRCONIUM) in our terms" (Koehl, 2019). Similarly, Kris McConkey, head of cyberthreat detection and response at PwC stated that "none of the stuff that we were tracking as APT10 overlaps with what Recorded Future and Rapid7 have reported" (Lyngaas, 2019a). Sean Lyngaas over at Cyberscoop summarized the issue neatly by highlighting that these attribution differences happen quite regularly and that the lack of a standard nomenclature to summarize patterns of unique characteristics is a problem for identifying new threat actors (Lyngaas, 2019a). As of this writing the attribution debate in this case has not been resolved.

ChChes: On January 26, 2017, the Japan Computer Emergency Response Team Coordination Center (JP-CERT) reported the discovery of a new malware/backdoor called ChChes, which was used in a campaign against Japanese organizations since around October 2016 (Nakamura, 2017). In February, Palo Alto Network's Unit 42 confirmed that the campaign targeted "Japanese academics working in several areas of science, along with Japanese pharmaceutical and a US-based subsidiary of a Japanese manufacturing organizations" (Miller-Osborn & Grunzweig, 2017). Palo Alto also additionally explained that "the ChCes samples […] were digitally signed using a certificate originally used by HackingTeam and later part of the data leaked when they [HackingTeam] were themselves hacked" (Miller-Osborn & Grunzweig, 2017).[15] In July 2017 researchers at Trend Micro connected ChChes to APT10 by noting that, "we first saw ChChes set its sights on an organization that's long been a target of APT 10/menuPass. […] ChChes also resembles another backdoor, Emdivi, which first made waves in 2014. […] In one instance, we detected PlugX and Emdivi on the same machine. This PlugX variant connected to an APT 10/menuPass-owned domain, but the packer is similar to that used by ChChes. While it's possible it was hit by two different campaigns, further analysis told a different story. Both were compiled on the same date, only several hours apart" (Sy et al., 2017). It is highly likely that ChChes is not a new APT group, but an APT10 sub-team.

[15] HackingTeam is an Italian, Milan-based company specializing in "offensive solutions for cyber investigations." HT was breached in July 2015 with more than 400GB of internal files dumped into the public domain.

Blue Termite/CloudyOmega/EMDIVI

Tooling
Proprietary: various Emdivi versions;, Uppercut (ANEL), Korplug, and ZXshell backdoors; self-build logon.exe (see: Tomonaga & Nakamura, 2015, slide. 25); usp10jpg; BeginX (remote shell tool) Widely available: Various; Mimikatz/Quarks; PowerShell (UAC bypass); Htran
Targets
Japan: Governmental organizations, manufacturing, financial, chemical, satellite, media, medical, food, and education organizations.

In August 2015, Kaspersky's GReAT team released a blogpost on a new threat actor dubbed Blue Termite, which was running a cyberespionage campaign against "hundreds of organizations in Japan" since at least 2012 (Kaspersky Lab, 2015). Among other characteristics, Blue Termite stood out due to their usage of a zero-day Flash exploit and "a sophisticated backdoor, which [was] customized for each victim." As the team noted, "this was the first campaign known to Kaspersky Lab that [was] strictly focused on Japanese targets" (Kaspersky Lab, 2015).

Speaking at Code Blue in October 2015, Shusei Tomonaga and Yuu Nakamaura over JP-CERT's analysis center, provided a detailed presentation on the Blue Termite campaign. Among other items, they explained that (a) the Emdivi malware used was repeatedly upgraded, (b) in some cases, the targeted organization's proxy server address was hard-coded, and that (c) each Emdivi version possibly only ran on specific computers (encryption of data by computer SID) (Tomonaga & Nakamura, 2015, slide 37). According to Trend Micro, Emdivi appeared first in 2014 and is the most used remote access tool leveraged against targets in Japan (Arai, 2015).

Symantec conducted its own investigation into Blue Termite's activity, which the company identified as Operation CloudyOmega in November 2014. In contrast to Kaspersky, Symantec started to look into CloudyOmega's activity because the group exploited a zero-day in the popular Japanese word processing software Ichitaro. Further investigation revealed that "the attack was in fact part of an ongoing cyberespionage campaign specifically targeting various Japanese organization. […] variants of Backdoor.Emdivi are persistently used as payload" (Symantec, 2014).

In terms of attribution, Kaspersky states that "the graphic user interface of the Command and Control server as well as some technical documents related to the malware used in the Blue Termite operation are written in Chinese" (Kaspersky Lab, 2015). Presenting at the 28th Annual First Conference in Seoul in June 2016, Kakumaru et al. observed that (1) 97% of IP addresses possibly used by Blue Termite/CloudyOmega, were assigned by an ISP in Shanghai; (2) The group also made a mistake in one of their attacks which exposed a one hour time difference between the attacker's local time and Japanese Standard Time; And (3) the phishing documents were written in a slightly different character font than the original Japanese fonts (Kakumaru et al. 2016, slide 17-23). Meanwhile, Symantec found tooling overlaps between CloudyOmega and the Chinese APT group Hidden Lynx and the creators of the LadyBoyle backdoor (backdoor.boda) (Symantec, 2014; Symantec 2013).

Winnti group/Winnti Umbrella

Tooling
Proprietary: Winnti backdoor; ZxShell Widely available: China Chopper; Metasploit; Cobaltstrike; PlugX; PoisonIvy
Targets
Gaming companies in Japan, China, Taiwan, South Korea, Vietnam, Europe, Russia, and the US; Pharmaceutical and telecommunication companies; Tibetan and Chinese journalists, Uyghur and Tibetan activists, China-focused foreign news organizations; The government of Thailand

On April 11, 2013, Kaspersky published its report on the original Winnti group, which stated that "this group has been active for several years and specializes in cyberattacks against the online video game industry" (Kaspersky GReAT, 2013). In 2015, Winnti branched out and started pivoting into other sectors, such as targeting large holdings in the telecommunication section and major pharmaceutical companies. In one instance it even signed a driver "with a stolen certificate of a division of a huge Japanese conglomerate" (Tarakanov, 2015).

Over the years, security vendors have connected Winnti infrastructure and tooling to other campaigns and groups, which has led MITRE's Att&ck database to note that, "some reporting suggests a number of other groups, including Axiom (APT13), APT17, and Ke3chang, are closely linked to Winnti Group" (MITRE Att&ck, n.d.). Other aliases and sub-teams include LEAD, Barium, Wicked Panda, GREF, and PassCV (Hegel, 2018, p. 4). Thus, nowadays, the name "Winnti" is primarily used to refer to a custom backdoor used by teams under the Winnti umbrella. On May 3, 2018, ProtectWise 401TRG "assesse[d] with high confidence that the Winnti umbrella is associated with the Chinese state intelligence apparatus, with at least some elements located in the Xicheng District in Beijing" (Hegel, 2018, p. 3).

In terms of behavior, Winnti stands out for simple operational security mistakes. As one source explained to German broadcaster BR, "these hackers don't care if they're found out or not. They care only about achieving their goals" (Tanriverdi et al., 2019). This characteristic stands in stark contrast to other

Chinese ATP teams which notably try to hide and cover up their involvements.

According to Zhang and Ortolani over at Lastline, “no new [Winnti] campaign has been publicly reported after the one targeting German Pharmaceutical companies in April 2019” (Zhang & Ortolani, 2019). On December 6, 2019, the German Federal Office for the Protection of the Constitution (BfV) released – for the first time ever - a 19-page technical report, warning the German private sector of the Winnti threat. According to the report, the group started targeting German companies back in 2016, and the BfV currently assumes that Winnti is conducting a wave of persistent attacks against the German economy (BfV 2019, p. 2).

5.4 Contractors

This sub-section lists three Chinese APT threat actors that have targeted Japan assets, but so far have not been directly linked to any of the aforementioned groups. They are most likely Chinese contractors working for the PLA or the MSS in one way or another.

Dust Storm

Tooling
Proprietary: Misdat backdoor (2010-2011); Mis-type hybrid backdoor (2012); S-type backdoor (2013-2014); ZLIB backdoor (2014-2015); Specially crafted HLP files; Several zero-days (CVE-2011-0611, CVE-2012-1889, CVE-2014-0322, and maybe CVE 2013-5990) Widely available: Poison Ivy, Gh0st RAT
Targets
Prior to 2015: Government and defense-related intelligence targets (incl. US defense companies and Uyghur mailing lists) Since 2015: Japanese critical infrastructure, including electricity generation, oil and natural gas, finance, transportation, and construction companies. Also, subdivisions of larger foreign organizations

In February 2016, Cylance released a report on a long-standing persistent threat it dubbed Operation Dust Storm - which has been active since at least 2010. While Cylance has not attributed any group or individuals to the Dust Storm campaign, it did highlight “a fairly large lull in activity from March -August 2013” (Gross, 2016, p. 4). This coincides with APT1’s downturn after Mandiant released its report on APT1 in February 2013. Other breadcrumbs that point toward a Chinese-based APT are the group’s past use of “public RATs like Poison Ivy and Gh0st Rat,” as well as their targeting of US defense companies and the Chinese Uyghur ethnic minority (Gross, 2016, p. 2-4).

In 2015, Dust Storm veered away from traditional government and defense-related intelligence targets and migrated to “seek out organizations involved in Japanese critical infrastructure and resources” (Gross, 2016, p. 1). By 2016 it almost entirely shifted to “specifically and exclusively target Japanese companies or Japanese subdivisions of larger foreign organizations” (Gross, 2016, p. 1). The group also “adopted and eventually customized several Android backdoors,” and “rapidly expanded their mobile operations in May 2015” (Gross, 2016, p. 6).

Sadly, Cylance also explained that “as the group became more and more focused on Japan, less and less of their tactics and malware appeared in reports or write-ups” (Gross, 2016, p. 6). As far as open source is concerned, no vendor has published any major report on Dust Storm since.

Note: Some APT reports view Dust Storm as an APT10 campaign. To this author it is unclear on what information this attribution assessment is based on. MITRE for example categorizes Dust Storm separate from APT10, while Thales’ Cyberthreat Handbook identifies Dust Storm as APT10’s first major campaign ever (Thales & Verint, p. 38).

Stalker Panda

Tooling
Proprietary: ? Widely available: Elirks, SharpServer, Blogspot RAT, XUni, PowerShell scripts
Targets
Primarily political, media, and engineering sectors in Japan, Taiwan, Hong Kong, and the US

Very few public reports have been published on the group known as Stalker Panda. The most important document is an analysis written by Raytheon in August 2015 and published by WikiLeaks as part of the CIA’s Vault 7 leak in March 2017.

According to Raytheon, “[Stalker Panda] appears to have close ties to the Chinese National University of Defense and Technology, which is possibly linked to the PLA. Stalker Panda has been observed conducting targeted attacks against Japan, Taiwan, Hong Kong, and the United States. The attacks appear to be centered on political, media, and engineering sectors. The group appears to have been active since around 2010 and they maintain and upgrade their tools regularly” (Raytheon, 2015, p. 1).

While CrowdStrike additionally notes, that Stalker Panda ”is linked to BlogSpotRAT activity targeting Japan in June 2017” (CrowdStrike, 2018, p. 26), Raytheon clearly highlights that “there is nothing interesting, unique, or sophisticated about the Blogspot RAT” (Raytheon, 2015, p. 1).

Maybe – and this is just speculation on the authors part – Stalker Panda is a team comprised of Chinese PLA students, rather than staffed by professional PLA operators.

Icefog/Dagger Panda

Tooling
Several variants of the Icefog backdoor (Fucobha), HLP files, HWP exploits, CVE-2012-1856 and CVE2012-0158
Targets
Primarily Japan and South Korea: government institutions, military contractors, maritime and shipbuilding groups, telecom operators, industrial and high-tech companies, and media outlets.

Icefog was a Chinese APT threat actor that was active between 2011 and 2014. According to Kaspersky it primarily focused on targets in Japan and South Korea, including “governmental institutions, military contractors, maritime and shipbuilding groups, telecom operators, industrial and high-tech companies and mass media” (Kaspersky Lab, 2013, p. 3). What made Icefog stand out at the time were its hit-and-run tactics. Meaning, the group avoided long-term persistence within a network. It knew what it wanted from a victim and abandoned the target as soon as they had what they came for. Some analyst therefore assume that Icefog were mercenaries for hire (Mimoso, 2013).

Minor convergence with APT1: Icefog liked to use HLP files to infect their targets. Those HLP files did not contain any exploits, but abused certain Windows features to drop malware. As Kaspersky’s GReAT team explains, “it’s interesting to know that Icefog is not the only crew to heavily use HLP ‘exploits’ as part of their toolkit. Well known, very effective APT like the Comment Crew/APT1 have included the HLP trick in their kits, along with other lesser known crews” (Kaspersky Lab, 2013, p. 10).

In June 2019, senior FireEye researcher, Chi-en (Ashley) Shen, showed that since 2014, several new and updated Icefog malware strains were shared among numerous threat actors - including Roaming Tiger, APT15, Temp Group A, and suspected APT9 – to hit targets in Europe, Russia, and Central Asia (Shen, 2019). Shen warned that, “shared malware is a pitfall for attribution, we should not do attribution only based on malware” (Shen, 2019). Overall, it seems that Icefog followed the same trajectory as Winnti. Once exclusively used by one Chinese APT, new versions of the malware are now “shared among many different APTs, each with its own agenda” (Cimpanu, 2019b).

5.5 Unsorted

This section lists the most prominent Chinese threat actors that have targeted Japanese entities, but have so far not been identified as being part of, or contractually connected to the PLA or the MSS. Minor Chinese APTs targeting Japan that are not included in this non-exhaustive list are APT16, EvilPost, and Axiom APT/APT17 (Hidden Lynx’s DeputyDog campaign).[16]

Tick/Bronze Butler/REDBALDKNIGHT

Tooling
Proprietary: Daserf, Datper, xxmm, Mimzen, SymonLoader, Gofarer and Homamdownloader Widely available: Mimikatz, gsecdump
Targets
Primarily Japan and South Korea: government agencies; companies in the biotechnology, electronics manufacturing, and industrial chemistry sector; media and broadcasting organizations

The Tick espionage group has been active since at least 2006, and most likely originates in the People’s Republic of China (DiMaggio, 2016a). While Trick primarily targets Japan and South Korea with its own custom developed malware (Daserf), it has also sporadically hit organizations in Russia, Singapore, and even China itself.

According to Secureworks, The group is “able to craft phishing emails in native Japanese and operating successfully within a Japanese language environment” (Secureworks, 2017). It has also demonstrated the ability to identify a significant zero-day vulnerability within a popular Japanese corporate tool and then use scan-and-exploit techniques to indiscriminately compromise Japanese internet-facing enterprise systems. […] It has remained undetected in several compromised networks for up to five years” (Secureworks, 2017).

Tick stands out from the APT crowd in many different ways. The group is “highly selective in its approach and only appears to deploy its full range of tools once it establishes that the compromised organization is an intended target” (DiMaggio, 2016a). It “frequently use[s] either privacy protection services or domain brokers to mask registration information. These tactics are used to make discovery and attribution more difficult” (DiMaggio, 2016a). It was also one of the few initial groups that leveraged steganography within their attacks. Trend Micro described one use case by explaining that, “a downloader will be installed on the victim’s machine and retrieve Daserf from a compromised site. Daserf will then connect to another compromised site and download an image file (i.e., .JPG, .GIF). The image is embedded in either the encrypted backdoor

[16] For more information on APT16 & EvilPost see: Kaspersky GReAT, 2016; On DeputyDog see: Christopher Ahlberg, 2014.

configurations or hacking tool. After their decryption, Daserf will connect to its C&C and await further commands" (Chen & Hsieh, 2017).

Curiously, in 2018, Palo Alto Network's Unit 42 also discovered that Tick weaponized secure USB drives in an older campaign to specifically target air-gapped computers running out-of-support Windows systems. While Unit 42 has no information on any active targets, it did note that "air-gapped systems are common practice in many countries for government, military, and defense contractors, as well as other industry verticals" (Hayashi & Harbison, 2018).

DragonOK

Tooling
Proprietary: FormerFirstRAT; Upheart RAT; custom Sysget malware variants (version 2 and 3); updated IsSpace version (Nflog variant) Widely available: PoisonIvy; Nflog; Mongall; CR, NewCT; TidePool; PowerShell; PlugX; HTran
Targets
Japan: Manufacturing, energy, and technology companies; Higher education institutions. Taiwan: Manufacturing and technology companies Also: Seeking out victims in Tibet and Russia.

In September 2014, FireEye identified "two distinct campaigns originating from different geographic regions in China using similar tools, techniques, and procedures (TTPs)" (Haq et al., 2014, p. 3). FireEye named the first group Moafee (after their command and control infrastructure), and the second group DragonOK (after an event name in one of their payload executables). Moafee operated out of the Guangdong province (HTran backend server location) and targeted governments and military organizations with national interests in the South China Sea. DragonOK meanwhile appeared to operate out of Jiangsu province (HTran backend server location) with a focused interest for technology and manufacturing companies located in Japan and Taiwan (Haq et al., 2014, p. 17-19).

In April 2015, Palo Alto Networks' Unit 42 identified a new DragonOK backdoor (called FormerFirstRAT) that was deployed against Japanese targets in at least five phishing campaigns. According to the blogpost "all five phishing campaigns targeted a Japanese manufacturing firm over the course of two months, but the final campaign also targeted a separate Japanese high-tech organization" (Miller-Osborn & Grunzweig, 2015).

In January 2017, Palo Alto Networks' Unit 42 observed a number of attacks by DragonOK against individuals and organizations in Japan and Taiwan, but also against targets in Tibet and Russia (Grunzweig, 2017). Unit 42 summarized its findings by highlighting that "the DragonOK group are quite active and continue updating their tools and tactics. Their toolset is being actively developed to make detection and analysis more difficult. Additionally, they appear to be using additional malware toolsets such as TidePool" (Grunzweig, 2017).

In June 2017, government servers in Cambodia were targeted by a new remote access Trojan dubbed KHRAT. In an article by The Phnom Penh Post, Phnom Penh-based cybersecurity researcher Niklas Femerstrand is quoted as saying that "the DragonOK campaign has previously targeted organizations in Taiwan, Japan, Tibet and Russia, and political organizations in Cambodia since at least January, 2017" (Sassoon & Taing). On October 27, 2017, Ryan Olsen, Director of Threat Intelligence at Palo Alto Networks, was interviewed on the cyberwire podcast on the specific topic of the KHRAT. According to Olsen, "[KHRAT] is a malware tool--that's a Remote Access Tool or a Remote Access Trojan, depending on your terminology--that we associate with a group that's called DragonOK" (Bittner, 2017).[17]

Budminer/Taidoor

Tooling
Proprietary: Dripion custom backdoor; Blugger downloader Widely available: Taidoor Trojan
Taidoor Trojan connected Targets
Since 2008 (Taidoor trojan): government agencies; media, financial, telecom and manufacturing sectors in Taiwan, Japan, US, South Korea (Doherty & Krysiuk, n.d.). Since 2011: (Taidoor Trojan): shifted to target think tanks (Symantec, 2012b) Since 2015 (Dripion backdoor): Taiwan, Brazil, US (DiMaggio, 2016b)

Open source information is sparse on the Budminer APT. The Symantec website only returns two search hits on the group, and neither MISP nor MITRE list Budminer among any of their APT groups.

Symantec stumbled upon Budminer in August 2015 when it received three file hashes that had "the functionality of a back door with information stealing capabilities." The malware also appeared to be "new, rarely detected, and not publicly available," leading Symantec to realize that it was custom-developed malware they termed Dripion. Meaning, there was a very high likelihood that Dripion was tied to a cyberespionage campaign.

The downloader was identified as Blugger, which is not publicly available and has only been seen used by China-based threat actors. As DiMaggio noted, "this is the first time we have seen Blugger used to deliver malware other than Taidoor" (DiMaggio, 2016b).

Taidoor meanwhile is a malware that has been used in many other cyberespionage campaigns since at

[17] Note: Although often linked to in most of the reporting on the KHRAT-DragonOK connection, the Palo Alto's write-up on KHAT of August 2017 (Hinchliffe & Miller-Osborn, 2017) does in fact not mention DragonOK at all.

least 2008. Further investigation uncovered that "one of the Blugger samples associated with Dripion connected with a root domain also used in Taidoor-related activity" against targets in Taiwan, Japan, South Korea, and the US (DiMaggio, 2016b). According to a 2019 report by Macnica Networks, Taidoor was extensively used against Japanese telecommunication companies (including telecommunication hardware manufacturers) between the end of 2017 and June 2018. The report speculates that the Taidoor attacks were aimed at obtaining personal customer and infrastructure information for future operations (Macnica Networks, 2019, p. 8).

Note: Given the sparse sourcing, it is not clear to this author when Budminer was first identified. None of Symantec's extensive write-ups on Taidoor ever mention the group, and none of the other major security vendors seem to have designated an APT based on the Dripion backdoor, Blugger use, and Taidoor connection. It is also unclear as to how extensive Budminer is connected to the overall Taidoor deployments against Japanese targets.

6 Effects

6.1 Social effects

Since the MHI breach in 2011, the Japanese government has made increasing efforts to change the cyber security culture in Japan. While the country is still struggling with non-transparent incident reporting and a perception that admitting to a breach is a sign of weakness and shame, there have been noticeable changes in attitude (Phneah, 2013).

In 2011, Japanese government officials were furious when they learned of the MHI breach through the media rather than the company reporting the incident immediately to the Ministry of Defense. Given that this was the first publicly known case of a Japanese defense contractor having been breached, one could – with a large stretch of imagination - argue that MHI was simply not familiar with the reporting mechanisms or did not deem the incident relevant enough to activate it. Then minister of defense Yasuo Ichikawa put it most diplomatically by stating that "the ministry has business ties with the company, so we will instruct it to review its information control systems" (McCurry, 2011). According to the New York Times, the MHI breach also fueled concerns in Washington on whether Tokyo is able to handle delicate information. As the Times explained, the MHI breach came "less than two weeks after a Japanese air traffic controller was questioned for posting American flight information on his blog" – including detailed flight plans for Air Force One and data on a US military reconnaissance drone (Tabuchi, 2011).

Despite MHI's assertions that no confidential information was exfiltrated, the Asahi Shimbun reported on October 24, that the attackers "likely netted military data on warplanes and information on nuclear power plants" (Reuters, 2011). To date it remains unclear whether sensitive defense information was leaked.

In contrast to the MHI's public relations fiasco, the breach of the Japanese Pension Service (JPS) in May 2015 was discernably different. Between May 8 and May 20, 2015, the JPS received 124 suspicious emails that infected five computers and spread to 26 others. In the period of May 21-23, the data of approximately 1.25 million enrolled citizens was exfiltrated. On May 28, the infections were discovered, and on June 1 the JPS apologized in a televised press conference for having been breached. According to the JPS statement, they immediately reported the incident to the police and requested an investigation, hired an anti-virus company to analyze and contain the malware, and blocked all JPS network connections to the internet (JPS, 2015, p. 2). In addition, JPS also set up a system to inform each customer individually on whether their data was affected, and set up a hotline for reporting any suspicious phishing activities related to customer pension information (JPS, 2015, p. 2). According to the Mainichi Shimbun, the Metropolitan Police Department (MPD)'s Public Security Bureau investigated the case but was stymied by the culprit’s use of Tor (Kanamori, 2018). Three years after the breach – on May 20, 2018 - Japanese law enforcement officially closed the criminal investigation without any results. To date none of the records exfiltrated from the JPS have been used for malicious purposes. In the aftermath of the JPS breach, the active sharing of indicators of compromise led numerous other companies and government agencies to report similar breaches in their networks.

Despite the JPS ‘success’ story, the norm still seems to be that after each incident, Japanese government officials first reassure the public that no confidential information was leaked, and then walk back their statements because the investigation either showed otherwise, or the affected agency/company has no idea what was actually lost. Similarly, it is quite disturbing to note that the more narrowly focused an attacker is on Japan, the less and less technical information becomes publicly available on the attacker. Meaning, communicating with the Japanese public and the global security community at large still seems to be a very low priority for Japanese security vendors, companies, and government agencies alike (Gross, 2016, p. 6).

Fitting into this gaping hole of public relations building was the appointed of Yoshitaka Sakurada to the post of deputy chief of the government’s cybersecurity strategy office. Sakurada inevitable achieved global fame in November 2018 when he admitted in the Japanese Parliament that he never used a computer in his professional life and “appear[ed] confused by the concept of a USB drive” (McCurry, 2018). As opposition lawmaker Masato Imai pointedly put it, “it’s unbelievable that someone who has not touched computers is responsible for cybersecurity policies” (McCurry, 2018).

The preparations for the Tokyo Olympics in 2020 have nonetheless discernably impacted the government’s motivation to pro-actively secure Japan in cyberspace. In fact, the Japanese government has taken the unusual step of allowing the Japanese National Institute for Information and Communications Technology (NICT) to run dictionary attacks against the country’s 200 million Internet of Things devices starting in February 2019.[18] While the overall purpose of this ‘campaign’ is to collect data for a survey on default and easy-to-guess device passwords, the government’s plan also includes measures to alert vulnerable customers and help them to secure their devices (Cimpanu, 2019a).

Apart from these broader security issues, there are still numerous attack vectors that remain unique to Japan. Kaoru Hayashi over at Palo Alto Network’s Unit 42, highlighted one curious case in his blog post on July 24, 2017, involving the Tick group. According to Hayashi, “many Japanese companies introduced a file encryption system for secure data exchange over email. The system encrypts documents with a user-specified password and often creates a self-extracting (SFX) file for ease of decrypting the file to recipients. When sending the SFX file with a password by email, senders usually rename the file extension from .exe to something else to avoid blocking or detecting the attachment by an email gateway or security product” (Hayashi, 2017). For an adversary that knows how Japanese enterprise users exchange these emails it is a very easy task to craft a spear phishing email that exploit this attack vector.

6.2 Economic effects

It is not clear what actual effects the cyber-related incidents attributed to Chinese threat actors had on the Japanese economy. While there are a few publicly available figures on remediation costs - such as the JPS breach standing at roughly $8 million USD - and on the quantity of exfiltrated sensitive documents, quantifying these damages in a reliable manner is not possible.

To a certain degree Japan’s unique threat landscape has been impacting the country’s economy each year around September 18 - the anniversary of the Mukden Incident that led to the Japanese invasion of Manchuria and the establishment of the puppet state of Manchukuo. While Chinese nationalist hacktivist have been mobilizing DDoS attacks and defacements against Japanese targets in September rather regularly over the past decade, activity has notably settled down over recent years. Despite this trend, the Japanese ISP provider Internet Initiative Japan rightfully warns that “some [Chinese] cyber attacks are linked to real-life historical events and carry a historical context, so it is necessary to pay attention to political and social situations such as historically significant dates and current international affairs” (Saito, 2016, p. 5).

[18] 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.)

6.3 Technological effects

The onslaught of Chinese attacks against Japanese infrastructure has in part forced the Abe government to outsource the MoD's development of offensive cyber capabilities to one or several unnamed private Japanese companies in 2019 (Tokyo-np, 2019). While there are certainly legal hurdles that will still have to be pushed aside, the Japanese government already tried to outsource the development of a 'seek and destroy' malware to Fujitsu back in 2012 (Leyden, 2012). Open sources are not entirely clear as to whether the Fujitsu malware failed to produce the expected results or why exactly the product was shelved in end. It is anyone's best guess how the 2019 plan will work out. According to the Japan Times, the delivery date for the offensive cyber capability is set for March 2020 (Japan Times, 2019).

In terms of the heaps of documents that were exfiltrated by Chinese APTs over the years from every industrial sector in Japan, it is unclear as to how or whether they benefitted companies and research institutions in China. Quantifying this impact would necessitate insights into what documents were stolen, how they were disseminated in China, and whether they were actual useful. No such assessment can be made in this report.

6.4 International effects

On December 21, 2018, the Japanese Ministry of Foreign Affairs joined the Five Eyes' collective public attribution effort on APT10. According to the statement by Press Secretary Takeshi Osuga, "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. […] Japan will continue to closely cooperate with the international community and make efforts in order to ensure a free, fair and secure cyberspace" (MOFA, 2018). It is important to note that, apart from the Five Eyes, Japan was the only country that released a written statement. The Netherlands, Finland, Sweden, and Demark merely tweeted their support, while the German government only comment on APT10 when a government spokesperson was specifically asked by a journalist at the Federal Press Conference on Dec 21.

Meanwhile, the Chinese Ministry of Foreign Affairs continues to argue that Beijing has nothing to do with APT10, noting on December 21 that, "the U.S. side making unwarranted criticisms of China in the name of so-called 'cyber stealing' is blaming others while oneself is to be blamed, and is self-deception. China absolutely cannot accept this" (Wen, 2018).

Given the concerns of industrial espionage at home and Beijing's global ambitions abroad, the Japanese Ministry of Telecommunications also effectively blocked Huawei and ZTE from competing in Japan's 5G infrastructure build-up by allocating the 5G spectrum to Japanese telecommunications companies upon the condition that they "take sufficient cybersecurity measures including responding to supply chain risk" (Nussey & Shida, 2019). Japan's ban essentially follows similar policies enacted in 2018 by the US, Australia, and New Zealand.

In the context of the US-Japan military alliance, US Secretary of State, Mike Pompeo stated on April 19, 2019 that, "the United States and Japan affirmed that international law applies in cyberspace and that a cyberattack could, in certain circumstances, constitute an armed attack under Article 5 of the U.S.-Japan Security Treaty. We stressed the need to work together to protect classified information, maintain technological superiority, and preserve our shared defense and economic advantages from theft and exploitation" (Pompeo, 2019). As of this writing it is unclear whether Tokyo has negotiated any special arrangements with Washington within the context of persistent engagement/defending forward.[19]

[19] For a description of persistent engagement see: US Cyber Command, 2018, p. 6

7 Future Outlook

Beijing has a clearly defined grand strategy in cyberspace, covering everything from ‘informatization’ and state-sovereignty to techno-nationalism and cyber-defense. Japan in contrast, has not yet articulated any grand ambitions to define its place in the world of tomorrow, nor how it will defend itself in and across cyberspace against an increasingly assertive China.

If the Japanese government is able and willing to significantly overhaul its defense policy and constitutional maneuverability – and maybe even attempt to walk in lock-step with the US strategy of persistent engagement – we might witness an intense competition between Tokyo and Beijing in cyberspace. If however the Japanese government is unable to turn around the current one-sided onslaught, then Tokyo might become a liability to US alliance cooperation, intelligence sharing, and possibly even power projection across the Indo-Pacific over time.

In the long run, it is highly likely that Tokyo will not to be able to merely hedge its alliance commitments through the modernization of its conventional military assets. Japan’s military absence in the cyber domain will be felt in Washington one way or the other.

For Beijing the primary challenge in the short term is to push hard against any signs that US Cyber Command is operationally applying persistent engagement in the Indo-Pacific. Meaning, Beijing has to walk a tight rope between, on the one hand, continuing its industrial- and military espionage against Japanese firms and government agencies. While on the other hand, staying clear of any activities that could even remotely undermine Japan’s democratic discourse, push Tokyo into militarizing cyber space, or heighten concerns in Washington to such a degree that it will force US Cyber Command to pay significant attention to the Indo-Pacific.

In the long run, Beijing’s will most likely seek to significantly undermine the trust relationship between Tokyo and Washington. Depending on the relative intelligence gains that Beijing can extract from Tokyo over time, China might run the Russian playbook on information warfare against Japan in the not so distant future.

8 Abbreviations

A2/AD	Anti-Access/Area Denial
AFB	Air Force Base
APT	Advanced Persistent Threat
ASEAN	Association of Southeast Asian Nations
BBC	British Broadcasting Corporation
BR	Bayerischer Rundfunk
BRI	Belt and Road Initiative
C2	Command and Control
CAC	Cyberspace Administration of China
CIA	Central Intelligence Agency
DDoS	Distributed Denial of Service
DoD	Department of Defense
DFS	Directorate for Signal Intelligence
FOIP	Free and Open Indo-Pacific
GDP	Gross Domestic Product
GSI	Geospatial Information Authority
HLP	Help file format
HTran	HUC Packet Transmitter
HTV	H-II Transfer Vehicle
IISS	International Institute for Strategic Studies
IP	Internet Protocol
ISPC	Information Security Policy Council
IT	Information Technology
JAXA	Japan Aerospace Exploration Agency
JEM	Japan Experimental Module
JP-CERT	Japan – Computer Emergency Response Team
JPS	Japanese Pension Service
MHI	Mitsubishi Heavy Industries
MISP	Malware Information Sharing Platform
MoD	Ministry of Defense
MOFA	Ministry of Foreign Affairs
MPD	Metropolitan Police Department
MSPs	Managed Service Providers
MSS	Ministry of State Security
NATO	North Atlantic Treaty Organization
NDR	Norddeutscher Rundfunk
NICT	Japanese National Institute for Information and Communications Technology
NISC	National Information Security Center
NPA	National Police Agency
NSA	National Security Agency
NYT	New York Times
PLA	People’s Liberation Army
PRC	People’s Republic of China
RAT	Remote Administration or Access Tool
RAT	Remote Access Tool / Remote Access Trojan
SCMP	South China Morning Post

SFX	Self-Extracting File
SSF	Strategic Support Force
TCP	Transmission Control Protocol
TPP	Tran-Pacific Partnership
TTPs	Tools, techniques, and procedures
USB	Universal Serial Bus

9 Bibliography

APSM. 2017. “Chinese Cyber-Espionage Group APT10 Targeted Japanese Govt & Manufacturer, Media/Ent Companies This Year.” *Asia Pacific Security Magazine*, July 20, 2017. https://www.asiapacificsecuritymagazine.com/chinese-cyber-espionage-group-apt10-targeted-japanese-govt-manufacturer-mediaent-companies-this-year/.

Arai, Yuu. 2015. “Flash Player のゼロデイ脆弱性「CVE-2015-5119」による標的型攻撃を国内で確認.” *Trend Micro*, July 14, 2015. https://blog.trendmicro.co.jp/archives/11944.

Barboza, David. 2012. “Billions in Hidden Riches for Family of Chinese Leader.” *The New York Times*, October 25, 2012. https://www.nytimes.com/2012/10/26/business/global/family-of-wen-jiabao-holds-a-hidden-fortune-in-china.html.

Barme, Geremie R., and Sang Ye. 1997. “The Great Firewall of China.” *Wired*, June 1, 1997. https://www.wired.com/1997/06/china-3/.

Barrett, Brian. 2018. “The Mysterious Return of Years-Old Chinese Malware.” *Wired*, October 18, 2018. https://www.wired.com/story/mysterious-return-of-years-old-chinese-malware-apt1/.

BBC. 2000. “Hackers blast Japan over Nanking massacre.” *BBC News*, January 25, 2000. http://news.bbc.co.uk/2/hi/asia-pacific/618520.stm

BBC. 2011. “Japan Defence Firm Mitsubishi Heavy in Cyber Attack.” *BBC News*, September 20, 2011. https://www.bbc.com/news/world-asia-pacific-14982906.

BfV. 2019. “BfV Cyber-Brief Nr. 01/2019 - Hinweis auf aktuelle Angriffskampagne.“ Bundesamt für Verfassungschutz, December 6, 2019. https://www.verfassungsschutz.de/download/broschuere-2019-12-bfv-cyber-brief-2019-01.pdf

Bittner, David. 2017. “Tracking a Trojan: Talking KHRAT with Ryan Olson - Research Saturday.” *The Cyberwire Podcast*, October 28, 2017. https://www.thecyberwire.com/podcasts/cw-podcasts-rs-2017-10-28.html.

Bureau, Henry, and Luke Jennings. 2018. “Breaking down the NCSC’s Top Five Hacking Tools.” *Countercept*, November 20, 2018. https://www.countercept.com/blog/breaking-down-the-ncscs-top-five-hacking-tools/.

Cabinet Secretariat. 2018. “National Defense Program Guidelines for FY 2019 and Beyond.” http://www.cas.go.jp/jp/siryou/pdf/2019boueikeikaku_e.pdf.

Chen, Joey, and Ming Yen Hsieh. 2017. “REDBALDKNIGHT/BRONZE BUTLER’s Daserf Backdoor Now Using Steganography.” *Trend Micro - Security Intelligence Blog*, November 7, 2017. https://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/.

China Economic Review. 2010. “Honker Union on China’s Hacking Supremacy.” *China Economic Review*, January 13, 2010. https://chinaeconomicreview.com/honker-union-on-chinas-hacking-supremacy/.

Christopher Ahlberg. 2014. “Hunting Hidden Lynx: How OSINT is Crucial for APT Analysis.” *Recorded Future*, May 1, 2014. https://www.recordedfuture.com/hidden-lynx-analysis/

Cimpanu, Catalin. 2019b. “Ancient ICEFOG APT Malware Spotted Again in New Wave of Attacks.” *ZDNet*, June 7, 2019b. https://www.zdnet.com/article/ancient-icefog-apt-malware-spotted-again-in-new-wave-of-attacks/.

Cimpanu, Catalin. 2019. “Japanese Government Plans to Hack into Citizens’ IoT Devices.” *ZDNet*, January 27, 2019. https://www.zdnet.com/article/japanese-government-plans-to-hack-into-citizens-iot-devices/.

Cluley, Graham. 2011. “Japanese Parliament Hit by Cyber-Attack.” *Naked Security*, October 25, 2011. https://nakedsecurity.sophos.com/2011/10/25/japanese-parliament-hit-by-cyber-attack/.

Cook, Sarah. 2019. “Worried About Huawei? Take a Closer Look at Tencent.” *The Diplomat*, March 26, 2019. https://thediplomat.com/2019/03/worried-about-huawei-take-a-closer-look-at-tencent/.

Creemers, Rogier, Paul Triolo, Samm Sacks, Xiaomeng Lu, and Graham Webster. 2018. “China’s Cyberspace Authorities Set to Gain Clout in Reorganization.” *New America*, March 26, 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/.

CrowdStrike. 2018. “2018 Global Threat Report - Blurring the Lines between Statecraft and Tradecraft.” CrowdStrike. https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf.

CSIS. 2019. “China’s Digital Silk Road.” CSIS. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190211_Chinas_Digital_Silk_Road.pdf.

Danchev, Dancho. 2010. “Baidu DNS Records Hijacked by Iranian Cyber Army.” *ZDNet*, January 12, 2010. https://www.zdnet.com/article/baidu-dns-records-hijacked-by-iranian-cyber-army/.

Denning, Dorothy. 2017. “How the Chinese Cyberthreat Has Evolved.” *The Conversation*, October 5, 2017. https://theconversation.com/how-the-chinese-cyberthreat-has-evolved-82469.

Desombre, Winnona, and Dan Byrnes. 2018. “Thieves and Geeks: Russian and Chinese Hacking Communities.” *Recorded Future*, October 10, 2018. https://go.recordedfuture.com/hubfs/reports/cta-2018-1010.pdf.

Deutsche Welle. 2013. “China Slams Japan’s New Defense Plan.” *Dw.Com*, December 21, 2013. https://www.dw.com/en/china-slams-japans-new-defense-plan/a-17315266-0.

DiMaggio, Jon. April 28, 2016a. “Tick Cyberespionage Group Zeros in on Japan.” *Symantec Security Response*, April 28, 2016a. https://www.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan.

DiMaggio, Jon. 2016b. “Taiwan Targeted with New Cyberespionage Back Door Trojan.” *Symantec Security Response*, March 29, 2016b. https://www.symantec.com/connect/blogs/taiwan-targeted-new-cyberespionage-back-door-trojan.

Doherty, Stephen, and Piotr Krysiuk. 2012. “Trojan.Tiadoor - Targeting Think Tanks.” Symantec Security Response. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/trojan_taidoor-targeting_think_tanks.pdf.

Edwards, Mitch. 2018. “Honker’s Union of China (HUC): Quantity and Quality.” *Medium.Com*, April 11, 2018. https://medium.com/@theCTIGuy/honkers-union-of-china-huc-quantity-and-quality-96ec0fd8ad86.

FireEye. n.d. “Advanced Persistent Threat Groups - Who’s Who of Cyber Threat Actors.” *FireEye*. https://www.fireeye.com/current-threats/apt-groups.html.

FMPRC. 2015. “Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference.” Ministry of Foreign Affairs of the People’s Republic of China, December 16, 2015. https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml

Fung, Brian. 2014. “The Mysterious Disappearance of China’s Elite Hacking Unit.” *The Washington Post*, April 10, 2014. https://www.washingtonpost.com/news/the-switch/wp/2014/04/10/the-mysterious-disappearance-of-chinas-elite-hacking-unit/.

Gady, Franz-Stefan. 2017. “Japan: The Reluctant Cyberpower.” IFRI - Center for Asia Studies. https://www.ifri.org/sites/default/files/atoms/files/gady_japan_reluctant_cyberpower_2017.pdf.

Geospatialworld.net. 2011. “Hackers Target Geospatial Information Authority Japan.” *Geospatialworld.Net*, 2011. https://www.geospatialworld.net/news/hackers-target-geospatial-information-authority-japan/amp/.

Glaser, Bonnie S. 2015. “Through Beijing’s Eyes: How China Sees the U.S.-Japan Alliance.” *The National Interest*, May 12, 2015. https://nationalinterest.org/feature/through-beijings-eyes-how-china-sees-the-us-japan-alliance-12864.

Goodin, Dan. 2010. “IE Zero-Day Used in Chinese Cyber Assault on 34 Firms.” *The Register*, January 14, 2010. https://www.theregister.co.uk/2010/01/14/cyber_assault_followup/.

Griffiths, James. 2019. *The Great Firewall of China: How to Build and Control an Alternative Veriosn of the Internet*. Zed Books Ltd.

Gross, Jon. 2016. “Operation Dust Storm.” Cylance. https://www.cylance.com/content/dam/cylance/pdfs/reports/Op_Dust_Storm_Report.pdf.

Grunzweig, Josh. 2017. “DragonOK Updates Toolset and Targets Multiple Geographic Regions.” *Palo Alto Networks - Unit 42*, January 5, 2017. https://unit42.paloaltonetworks.com/unit42-dragonok-updates-toolset-targets-multiple-geographic-regions/.

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

Haq, Thoufique, Ned Moran, Sai Vashisht, and Mike Scott. 2014. “Operation Quantum Entanglement.” FireEye. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf.

Hayashi, Kaoru. 2017. “‘Tick’ Group Continues Attacks.” *Palo Alto Networks - Unit 42*, July 24, 2017. https://unit42.paloaltonetworks.com/unit42-tick-group-continues-attacks/.

Hayashi, Kaoru, and Mike Harbison. 2018. “Tick Group Weaponized Secure USB Drives to Target Air-Gapped Critical Systems.” *Palo Alto Networks - Unit 42*, June 22, 2018. https://unit42.paloaltonetworks.com/unit42-tick-group-weaponized-secure-usb-drives-target-air-gapped-critical-systems/.

Hegel, Tom. 2018. “Burning Umbrella: An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers.” ProtectWise

401TRG. https://github.com/401trg/detections/raw/master/pdfs/20180503_Burning_Umbrella.pdf.

Hinchliffe, Alex, and Jen Miller-Osborn. 2017. “Updated KHRAT Malware Used in Cambodia Attacks.” *Palo Alto Networks - Unit 42*, August 31, 2017. https://unit42.paloaltonetworks.com/unit42-updated-khrat-malware-used-in-cambodia-attacks/.

Insikt Group, and Rapid7. 2019. “APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign.” Recorded Future. https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf.

Intrusion Truth. July 24, 2019a. “APT17 Is Run by the Jinan Bureau of the Chinese Ministry of State Security.” *Intrusiontruth.Wordpress.Com*, July 24, 2019a. https://intrusiontruth.wordpress.com/2019/07/24/apt17-is-run-by-the-jinan-bureau-of-the-chinese-ministry-of-state-security/.

Intrusion Truth. July 25, 2019b. “Encore! APT17 Hacked Chinese Targets and Offered the Data for Sale.” *Intrusiontruth.Wordpress.Com*, July 25, 2019b. https://intrusiontruth.wordpress.com/2019/07/25/encore-apt17-hacked-chinese-targets-and-offered-the-data-for-sale.

Intrusion Truth. 2017. “APT3 Is Boyusec, a Chinese Intelligence Contractor.” *Intrusiontruth.Wordpress.Com*, May 9, 2017. https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/#more-115.

Intrusion Truth. 2018. “APT10 Was Managed by the Tianjin Bureau of the Chinese Ministry of State Security.” *Intrusiontruth.Wordpress.Com*, August 15, 2018. https://intrusiontruth.wordpress.com/2018/08/15/apt10-was-managed-by-the-tianjin-bureau-of-the-chinese-ministry-of-state-security/.

IPA. 2004. “電力重要インフラ防護演習に関する調査 報告書.” Information Technology Promotion Agency, August 8, 2004. https://www.ipa.go.jp/security/fy15/reports/infra/documents/infra_2004.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.” Cabinet Secretariat, Information Security Measures Promotion Office, December 15, 2000. https://www.nisc.go.jp/active/sisaku/2000_1215/pdf/txt3.pdf

ISPC. 2006. “The First National Strategy on Information Security - Toward the Realization of a Trustworthy 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.” Information Security Policy Council. https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf.

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

ISPC. 2012. “Information Security 2012.” Information Security Policy Council. https://www.nisc.go.jp/eng/pdf/is2012_eng.pdf.

ISPC. 2013. “Cybersecurity Strategy - Towards a World-Leading, Resilient and Vigorous Cyberspace.” Information Security Policy Council. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Japan%20Cybersecurity%20Strategy%202013.pdf.

Japan Times. 2019. “In first, Japan to develop computer virus to defend against cyberattacks.” The Japan Times, April 30, 2019. https://www.japantimes.co.jp/news/2019/04/30/national/first-japan-develop-computer-virus-defend-cyberattacks/

Japanese Constitution. 1946. “The Constitution of Japan.” Prime Minister of Japan and His Cabinet. https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html.

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

JAXA. 2012a. “Computer Virus Infection at JAXA.” *Japan Aerospace Exploration Agency*, January 13, 2012a. https://global.jaxa.jp/press/2012/01/20120113_security_e.html.

JAXA. 2012b. “Computer Virus Infection Investigation Results.” *Japan Aerospace Exploration Agency*, March 27, 2012b. https://global.jaxa.jp/press/2012/03/20120327_security_e.html.

JAXA. 2012c. “Computer Virus Infection and Possible Information Leak at JAXA.” *Japan Aerospace Exploration Agency*, November 30, 2012c. https://global.jaxa.jp/press/2012/11/20121130_security_e.html.

JAXA. 2013a. “Investigation Result of JAXA Computer Virus Infection Incident.” *Japan Aerospace Exploration Agency*, February 19, 2013a. https://global.jaxa.jp/press/2013/02/20130219_security_e.html.

JAXA. 2013b. “JAXA のサーバーに対する外部からの不正アクセスに関する調査結果について.” *Japan Aerospace Exploration Agency*, July 2, 2013b.

http://www.jaxa.jp/press/2013/07/20130702_security_j.html.

Jericho & Sioda. 2001. “Cyberwar with China: Self-fulfilling Prophecy.” *Attrition.org*, April 29, 2001. http://www.attrition.org/security/commentary/cn-us-war.html

Johnson, Jesse. 2019. “China Defense White Paper Singles out Japan over Security Shift and Blasts U.S. for Undermining Global Stability.” *The Japan Times*, July 24, 2019. https://www.japantimes.co.jp/news/2019/07/24/asia-pacific/china-blasts-u-s-undermining-global-stability-defense-white-paper/#.XXDYQOgzZaQ.

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.

Kadena.af.mil. n.d. “Kadena Air Base.” Kadena.af.mil. https://www.kadena.af.mil/.

Kakumaru, Takahiro, Hiroki Iwai, and Kenzo Masamoto. 2016. “Chasing the Operation after the Infection of Thecontinuing Cyber Attacks -Emdivi -.” 28th Annual FIRST Conference. http://docplayer.net/40775875-Chasing-the-operation-after-the-infection-of-the-continuing-cyber-attacks-emdivi.html.

Kanamori, Takayuki. 2018. “MPD Closes Japan Pension Service Personal Info Hack Case without a Suspect.” *Mainichi Shimbun*, May 21, 2018. https://mainichi.jp/english/articles/20180521/p2a/00m/0na/012000c.

Kaspersky GReAT. 2013. “Winnti. More than Just a Game.” *Securelist*, April 11, 2013. https://securelist.com/winnti-more-than-just-a-game/37029/.

Kaspersky GReAT. 2016. “CVE-2015-2545: Overview of Current Threats.” *Securelist*, May 25, 2016. https://securelist.com/cve-2015-2545-overview-of-current-threats/74828/.

Kaspersky IT Encyclopedia. n.d. “Dictionary Attack.” *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.

Kaspersky Lab. 2015. “Blue Termite: A Sophisticated Cyber Espionage Campaign Is After High-Profile Japanese Targets.” *Kaspersky Policy Blog*, August 20, 2015. https://www.kaspersky.com/about/press-releases/2015_blue-termite-a-sophisticated-cyber-espionage-campaign-is-after-high-profile-japanese-targets.

Kelly, Tim. 2019. “Japan lists China as bigger threat than nuclear-armed North Korea.” Reuters, September 27, 2019. https://www.reuters.com/article/us-japan-defence/japan-promotes-china-as-bigger-threat-than-nuclear-armed-north-korea-idUSKBN1WC051

Koehl, Benjamin. 2019. “This Activity Is Not APT10. It Is All APT31 (or ZIRCONIUM) in Our Terms.” *Twitter*, February 6, 2019. https://twitter.com/bkMSFT/status/1093109336740642816.

Kubo, Keishi, and Shiori Kubo. 2015. “Emdivi and the Rise of Targeted Attacks in Japan.” *JPCERT/CC Eyes*, November 6, 2015. https://blogs.jpcert.or.jp/en/2015/11/emdivi-and-the-rise-of-targeted-attacks-in-japan.html.

Kubota, Yoko. 2011. “Japan Contractor Hacking Likely Got Military Data: Asahi.” *Reuters*, October 24, 2011. https://www.reuters.com/article/us-mitsubishi-heavy-cyberattack/japan-contractor-hacking-likely-got-military-data-asahi-idUSTRE79M3XS20111024.

Kyodo News. 2012. “Chinese Cyber Attacks Hit Japan over Islands Dispute.” *The Globe and Mail*, September 19, 2012. https://www.theglobeandmail.com/news/world/chinese-cyber-attacks-hit-japan-over-islands-dispute/article4553048/.

Kyodo News. 2016. “Defense Ministry, SDF networks hacked; state actor suspected.” *Kyodo News*, November 28, 2016. https://www.japantimes.co.jp/news/2016/11/28/national/politics-diplomacy/defense-ministry-hit-cyberattack-info-may-accessed/#.Xd-n4ehKhaQ

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.

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

Lewis, James A. 2006. “The Architecture of Control: Internet Surveillance in China.” CSIS. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0706_cn_surveillance_and_information_technology.pdf.

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/.

Liao, Shannon. 2018. “Apple Officially Moves Its Chinese ICloud Operations and Encryption Keys to China.” *The Verge*, February 28, 2018. https://www.theverge.com/2018/2/28/17055088/apple-chinese-icloud-accounts-government-privacy-speed.

Lion, and bkbll. 2003. “HTran.Cpp - HUC Packet Transmit Tool.” *Cnhonker.Com*, 2003.

https://github.com/HiwinCN/HTran/blob/master/Windows_Version/HTran.cpp.

Littleton, Matthew J. 1995. “Information Age Terrorism: Toward Cyberterror.” Naval Postgraduate School, December 1995. https://fas.org/irp/threat/cyber/docs/npgs/ch4.htm#b_japan

Lyngaas, Sean. 2019b. “Meet APT41, the Chinese Hackers Moonlighting for Personal Gain.” *Cyberscoop*, August 7, 2019b. https://www.cyberscoop.com/apt41-fireeye-china/.

Lyngaas, Sean. 2019a. “Right Country, Wrong Group? Researchers Say It Wasn’t APT10 That Hacked Norwegian Software Firm,” February 12, 2019a. https://www.cyberscoop.com/apt10-apt31-recorded-future-rapid7-china/.

Macnica Networks. 2019. “標的型攻撃の実態と対策アプローチ.” Macnica Networks. https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf.

Mandiant. 2013. “APT1 - Exposing One of China’s Cyber Espionage Units.” Mandiant. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

Matsuda, Ayako, and Irshad Muhammad. 2018. “APT10 Targeting Japanese Corporations Using Updated TTPs.” *FireEye Threat Research*, September 13, 2018. https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html.

McCurry, Justin. 2011. “Japan Anxious over Defence Data as China Denies Hacking Weapons Maker.” *The Guardian*, September 20, 2011. https://www.theguardian.com/world/2011/sep/20/china-denies-hacking-attack-japan.

———. 2018. “System Error: Japan Cybersecurity Minister Admits He Has Never Used a Computer.” *The Guardian*, November 15, 2018. https://www.theguardian.com/world/2018/nov/15/japan-cyber-security-ministernever-used-computer-yoshitaka-sakurada.

McCurry, Justin, and Julia Kollewe. 2011. “China Overtakes Japan as World’s Second-Largest Economy.” *The Guardian*, February 14, 2011. https://www.theguardian.com/business/2011/feb/14/china-second-largest-economy.

MPD. n.d. “サイバーテロ対策協議会.” Metropolitan Police Department. https://www.keishicho.metro.tokyo.jp/smph/kurashi/cyber/katsudo/cyber/index.html

Meyers, Adam. 2013. “Whois Numbered Panda.” *CrowdStrike*, March 29, 2013. https://www.crowdstrike.com/blog/whois-numbered-panda/.

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.

Miller-Osborn, Jen, and Josh Grunzweig. 2015. “Unit 42 Identifies New DragonOK Backdoor Malware Deployed Against Japanese Targets.” *Palo Alto Networks - Unit 42*, April 14, 2015. https://unit42.paloaltonetworks.com/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/.

———. 2017. “MenuPass Returns with New Malware and New Attacks against Japanese Academics and Organizations.” *Palo Alto Networks - Unit 42*, February 17, 2017. https://unit42.paloaltonetworks.com/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/.

Mimoso, Michael. 2013. “Icefog Espionage Campaign Is ‘Hit and Run’ Targeted Operation.” *Threatpost*, September 25, 2013. https://threatpost.com/icefog-espionage-campaign-is-hit-and-run-targeted-operation/102417/3/.

MISP. n.d. “MISP Galaxy Clusters.” *MISP*. https://www.misp-project.org/galaxy.html#_threat_actor.

MITRE. n.d. “Groups.” *MITRE ATT&CK*. https://attack.mitre.org/groups/.

MITRE Att&ck. n.d. “Winnti Group.” *MITRE Att&ck*. https://attack.mitre.org/groups/G0044/.

Miyake, Kuni. 2019. “What Does the ‘Indo-Pacific Strategy’ Mean?” *The Japan Times*, March 11, 2019. https://www.japantimes.co.jp/opinion/2019/03/11/commentary/japan-commentary/indo-pacific-strategy-mean/#.XXDZPegzZaR.

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

MoD. 2018a. “Defense of Japan 2018.” Japanese Ministry of Defense. https://www.mod.go.jp/e/publ/w_paper/pdf/2018/DOJ2018_Digest_1204.pdf.

MoD. 2018b. “National Defense Program Guidelines for FY 2019 and beyond.” Japanese Ministry of Defense, December 18, 2018. https://www.mod.go.jp/j/approach/agenda/guideline//2019/pdf/20181218_e.pdf

MoD, 2018c. “Defense Programs and Budget of Japan: Overview of FY2019 Budget Request.” Japanese Ministry of Defense, August 2018. https://www.mod.go.jp/e/d_budget/pdf/310118.pdf

MoD. 2019a. “Defense of Japan 2019.” Japanese Ministry of Defense https://www.mod.go.jp/e/publ/w_paper/2019.html

MoD. 2019b. “Statistics on Scrambles through Fiscal Year 2018.” Japanese Ministry of Defense - Joint Staff Japan.

https://www.mod.go.jp/js/Press/press2019/press_pdf/p20190412_06.pdf.

MoD, 2019c. “Defense Programs and Budget of Japan: Overview of FY2020 Budget Request.” Japanese Ministry of Defense, August 2019. https://www.mod.go.jp/e/d_budget/pdf/191112c.pdf

MoD. n.d. “Regarding Response to a Cyber Attack.” *Japanese Ministry of Defense*. https://www.mod.go.jp/e/p_affair/answers/cyber/index.html.

MOFA. 2019a. “Joint Statement of the Security Consultative Committee.” Japanese Ministry of Foreign Affairs. https://www.mofa.go.jp/files/000470738.pdf.

MOFA. 2019b. “Free and Open Indo-Pacific.” Japanese Ministry of Foreign Affairs. https://www.mofa.go.jp/policy/page25e_000278.html.

MOFA. 2013. “Leakage of Information from the MOFA Network to the Internet.” Japanese Ministry of Foreign Affairs. https://www.mofa.go.jp/announce/announce/2013/2/0205_03.html.

MOFA. 2018. “Cyberattacks by a Group Based in China Known as APT10 - Statement by Press Secretary Takeshi Osuga.” *Japanese Ministry of Foreign Affairs*, December 21, 2018. https://www.mofa.go.jp/press/release/press4e_002281.html.

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

Moran, Ned, and Mike Oppenheim. 2014. “Darwin’s Favorite APT Group.” *FireEye*, September 3, 2014. https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html.

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

Nakamura, Yu. 2017. “ChChes – Malware That Communicates with C&C Servers Using Cookie Headers.” *JPCERT/CC Eyes*, February 15, 2017. https://blogs.jpcert.or.jp/en/2017/02/chches-malware--93d6.html.

Nan, Wun. 2013. “From Hackers to Entrepreneurs: The Sino-US Cyberwar Veterans Going Straight.” *South China Morning Post*, August 21, 2013. https://www.scmp.com/news/china/article/1298200/hackers-entrepreneurs-sino-us-cyberwar-veterans-going-straight.

Nikkei. 2013. “サイバー防衛隊」準備室を設置　防衛省.” *Nihon Keizai Shimbun*, June 16, 2013 https://www.nikkei.com/article/DGXNASFS1603T_W3A510C1PP8000/

NISC. 2004. “第1次提言 - 情報セキュリティ問題に取り組む政府の機能・役割の見直しに向けて.” NISC, November 16, 2004. https://www.nisc.go.jp/conference/kihon/teigen/pdf/1teigen_hontai.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, February 10, 2015. https://www.nisc.go.jp/conference/cs/pdf/unei_kitei.pdf

NPA. 2011. “平成23年7月の警察庁に対するサイバー攻撃への対応について.” Japanese National Police Agency. http://www.npa.go.jp/keibi/biki3/230826kouhou.pdf.

NPA. 2012. “尖閣諸島問題等と関連したとみられるサイバー攻撃事案について.” Japanese National Police Agency. http://www.npa.go.jp/keibi/biki3/20120919kouhou.pdf.

Nussey, Sam, and Yoshiyasu Shida. 2019. “Japan Telcos’ 5G Go-Ahead Cements Curbs on Chinese Vendors.” *Reuters*, April 10, 2019. https://www.reuters.com/article/us-japan-telecoms-5g/japan-telcos-5g-go-ahead-cements-curbs-on-chinese-vendors-idUSKCN1RM0ML.

NYT. 2000. “Clinton's Words on China: Trade Is the Smart Thing.” *The New York Times*, March 9, 2000. https://www.nytimes.com/2000/03/09/world/clinton-s-words-on-china-trade-is-the-smart-thing.html

OSD. 2019. “Annual Report to Congress - Military and Security Developments Involving the People’s Republic of China 2019.” US Department of Defense. https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pd.

Perlroth, Nicole. 2013. “Hackers in China Attacked The Times for Last 4 Months.” *The New York Times*, January 30, 2013. https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html.

Phneah, Ellyne. 2013. “Japan Ministry Information Reportedly Stolen in Cyberattack.” *ZDNet*, January 3, 2013. https://www.zdnet.com/article/japan-ministry-information-reportedly-stolen-in-cyberattack/.

Phys.org. 2011. “New Cyber Attack on Japan Parliament.” *Phys.Org*, November 2, 2011. https://phys.org/news/2011-11-cyber-japan-parliament.html.

Pompeo, Michael R. 2019. “Remarks With Acting Secretary of Defense Patrick Shanahan, Japanese Foreign Minister Taro Kono, and Japanese Defense Minister Takeshi Iwaya at a Joint Press Availability for the U.S.-Japan 2+2 Ministerial.” *US Department of State*, April 19, 2019. https://www.state.gov/remarks-with-acting-secretary-of-defense-patrick-shanahan-japanese-foreign-minister-taro-kono-and-japanese-defense-minister-takeshi-iwaya-at-a-joint-press-availability-for-the-u-s-japan-22-ministe/.

PwC, and BAE Systems. 2017. “Operation Cloud Hopper.” PwC UK. https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf.

Raytheon. 2015. “20150814-256-CSIR-15005 Stalker Panda.” Raytheon Blackbird Technologies. https://wikileaks.org/vault7/document/2015-08-20150814-256-CSIR-15005-Stalker-Panda/2015-08-20150814-256-CSIR-15005-Stalker-Panda.pdf.

Reuters. 2011. “UPDATE 1-Japan Contractor Hacking Likely Got Military Data -Paper.” *Reuters*, October 24, 2011. https://www.reuters.com/article/mitsubishi-heavy-cyberattack/update-1-japan-contractor-hacking-likely-got-military-data-paper-idUSL3E7LN0DS20111024.

Ryall, Julian. 2011. “Latest Japan Hack Prompts Concerns It Is Sustained Attack.” *The Telegraph*, October 28, 2011. https://www.telegraph.co.uk/technology/news/8855639/Latest-Japan-hack-prompts-concerns-it-is-sustained-attack.html.

Saito, Mamoru. 2016. “Infrastructure Security.” *Internet Infrastructure Review* 33. https://www.iij.ad.jp/en/dev/iir/pdf/iir_vol33_infra_EN.pdf.

Samani, Raj, and Ryan Sherstobitoff. 2018. “‘Operation Oceansalt’ Delivers Wave After Wave.” *McAfee Labs*, October 17, 2018. https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-oceansalt-delivers-wave-after-wave/.

Sancho, David, Jessa dela Torre, Matsukawa Bakuei, Nart Villeneuve, and Robert McArdle. 2012. “IXESHE - An APT Campaign.” Trend Micro. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf.

Sassoon, Alessandro Marazzi, and Rinith Taing. 2017. “Kingdom Targeted by New Malware.” *The Phnom Penh Post*, September 5, 2017. https://www.phnompenhpost.com/national/kingdom-targeted-new-malware.

ScanNetSecurity. “各省庁への不正アクセス、その後も相次ぐ（運輸省、郵政省、経済企画庁、他）.” *ScanNetSecurity*, February 1. https://scan.netsecurity.ne.jp/article/2000/02/01/5.html

SCMP. 2018. “China Hacker Accused of Attacking Japanese Defence Firms.” *SCMP*, April 23, 2018. https://www.scmp.com/news/china/diplomacy-defence/article/2142863/china-hackers-accused-attacking-japanese-defence-firms.

Secureworks. 2017. “BRONZE BUTLER Targets Japanese Enterprises.” *Secureworks - Counter Threat Unit - Threat Intelligence*, October 12, 2017. https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses.

Segal, Adam. n.d. “When China Rules the Web.” *Foreign Affairs*, no. September/October 2018. https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web.

Shen, Chi-en. 2019. “Into the Fog - The Return of ICEFOG APT.” FireEye. https://speakerdeck.com/ashley920/into-the-fog-the-return-of-icefog-apt.

Sims, Calvin. 2000. “Japan Software Suppliers Linked to Sect.” *The New York Times*, March 2, 2000. https://www.nytimes.com/2000/03/02/world/japan-software-suppliers-linked-to-sect.html

Singh, Kanishka. 2019. “U.S. Intelligence Says Huawei Funded by Chinese State Security: Report.” *Reuters*, April 20, 2019. https://www.reuters.com/article/us-usa-trade-china-huawei/u-s-intelligence-says-huawei-funded-by-chinese-state-security-report-idUSKCN1RW03D.

Stewart, Joe. 2011. “HTran and the Advanced Persistent Threat.” *Secureworks Threat Analysis*, August 3, 2011. https://www.secureworks.com/research/htran.

Stout, David. 1999. “CRISIS IN THE BALKANS; China Protests Crash White House Web Site.” *The New York Times*, May 12, 1999. https://www.nytimes.com/1999/05/12/world/crisis-in-the-balkans-china-protests-crash-white-house-web-site.html.

Sudo, Tatsuya. 2019. “Chinese Hackers May Have Struck Keidanren System in 2016.” *The Asahi Shimbun*, January 13, 2019. http://www.asahi.com/ajw/articles/AJ201901130021.html.

Sy, Benson, CH Lei, and Kawabata Kohei. 2017. “ChessMaster Makes Its Move: A Look into the Campaign’s Cyberespionage Arsenal.” *Trend Micro - Security Intelligence Blog*, July 27, 2017. https://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-cyber-espionage-campaign/.

Symantec. 2012a. “The Luckycat Hackers.” *Symantec Security Response*, March, 2012. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_luckycat_hackers.pdf.

Symantec. 2012b. “Trojan.Taidoor Takes Aim at Policy Think Tanks.” *Symantec Security Response*, March 27, 2012b. https://www.symantec.com/connect/blogs/trojantaidoor-takes-aim-policy-think-tanks.

Symantec. 2013. “Hidden Lynx – Professional Hackers for Hire.” *Symantec Security Response*, September 17, 2013. https://www.symantec.com/connect/blogs/hidden-lynx-professional-hackers-hire.

Symantec. 2014. “Operation CloudyOmega: Ichitaro Zero-Day and Ongoing Cyberespionage

Campaign Targeting Japan.” *Symantec Security Response*, November 12, 2014. https://www.symantec.com/connect/blogs/operation-cloudyomega-ichitaro-zero-day-and-ongoing-cyberespionage-campaign-targeting-japan.

Symantec. 2016. “Buckeye Cyberespionage Group Shifts Gaze from US to Hong Kong.” *Symantec Security Response*, September 6, 2016. https://attack.mitre.org/groups/G0022/.

Tabuchi, Hiroko. 2011. “U.S. Expresses Concern About New Cyberattacks in Japan.” *The New York Times*, September 21, 2011. https://www.nytimes.com/2011/09/22/world/asia/us-expresses-concern-over-cyberattacks-in-japan.html.

Tanner, Murray Scot. 2017. “Beijing’s New National Intelligence Law: From Defense to Offense.” *Lawfare*, July 20, 2017. https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

Tanriverdi, Hakan, Maximilian Zierer, Rebecca Ciesielski, Svea Eckert, and Jan Lukas Strozyk. 2019. “Winnti: Attacking the Heart of the German Industry.” *Joint Investigation by Bayerischer Rundfunk and Norddeutscher Rundfunk*, July 24, 2019. http://web.br.de/interaktiv/winnti/english/.

Tarakanov, Dmitry. 2015. “Games Are over: Winnti Is Now Targeting Pharmaceutical Companies.” *Securelist*, June 22, 2015. https://securelist.com/games-are-over/70991/.

ThaiCERT. 2019. “Threat Group Cards: A Threat Actor Encyclopedia.” ThaiCERT. https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf.

Thales & Verint. 2019. “The Cyberthreat Handbook.” https://www.thalesgroup.com/en/group/journalist/press-release/cyberthreat-handbook-thales-and-verint-release-their-whos-who.

The Intercept. 2017. “What Are the Japanese Like as SIGINTers.” *The Intercept*, April 24, 2017. https://theintercept.com/document/2017/04/24/what-are-the-japanese-like-as-siginters/.

The Intercept. 2018. “DFS Briefing Feb 2013.” The Intercept. https://theintercept.com/document/2018/05/19/dfs-briefing-feb-2013/.

The Military Balance. n.d. “The Military Balance 2019: Chapter Two - Comparative Defence Statistics.” IISS. https://www.tandfonline.com/doi/pdf/10.1080/04597222.2019.1561026.

Tokyo-np. 2019. サイバー反撃ウイルス保有へ有事に備え防衛省、作成方針. *Tokyo-np.co.jp*, April 30, 2019. https://www.tokyo-np.co.jp/article/politics/list/201904/CK2019043002000106.html

Tomonaga, Shusei, and Yu Nakamura. 2015. “Revealing the Attack Operations Targeting Japan.” JPCERT. https://www.jpcert.or.jp/present/2015/20151028_codeblue_apt-en.pdf.

Trend Micro. 2012. “Inside an APT Campaign with Multiple Targets in India and Japan.” Trend Micro. https://documents.trendmicro.com/assets/wp/wp_luckycat_redux.pdf.

Triolo, Paul, Samm Sacks, Graham Webster, and Rogier Creemers. 2017. “China’s Cybersecurity Law One Year On.” *New America*, November 30, 2017. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/.

US Cyber Command. 2018. “Achieve and Maintain Cyberspace Superiority - Command Vision for US Cyber Command.” https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

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

US DoJ. 2017. “U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage.” *US Department of Justice - Office of Public Affairs*, November 27, 2017. https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations.

US DoJ. 2018. “Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information.” *US Department of Justice - Office of Public Affairs*, December 20, 2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

Wagner, Jack. 2017. “China’s Cybersecurity Law: What You Need to Know.” *The Diplomat*, June 1, 2017. https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.

Watts, Jonathan. 2000. “Hackers shake up Japan.” *The Guardian*, January 29, 2000. https://www.theguardian.com/world/2000/jan/29/jonathanwatts

Weaver, Matthew. 2009. “Cyber Attackers Target South Korea and US.” *The Guardian*, July 8, 2009.

https://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack.

Wehrfritz, George. 2000. “From Sarin to Software.” *Newsweek*, March 12, 2000.

https://www.newsweek.com/sarin-software-156381

Wen, Philip. 2018. “China Denies ‘slanderous’ Economic Espionage Charges from U.S., Allies.” *Reuters*, December 21, 2018. https://www.reuters.com/article/us-china-cyber-usa-ministry/china-denies-slanderous-economic-espionage-charges-from-u-s-allies-idUSKCN1OK03Y.

Wikileaks. 2008. “Diplomatic Security Daily.” *Wikileaks*, October 30, 2008. https://wikileaks.org/plusd/cables/08STATE116943_a.html.

Wright, John C. 2016. “The Persistent Power of 1 Percent.” Sasakawa USA. https://spfusa.org/wp-content/uploads/2016/09/1-percent-final.pdf.

Xinhua. 2014. “China Suspends Cyber Activities with US in Indictment Protest.” *China Daily*, May 20, 2014. http://www.chinadaily.com.cn/china/2014-05/20/content_17519284.htm.

Yomiuri Shimbun. 2011. “Diplomatic Computers Hit / ‘Backdoor’ Virus Found at Japanese Missions in 9 Countries.” *The Yomiuri Shimbun*, October 27, 2011. https://web.archive.org/web/20111227100555/http://www.yomiuri.co.jp/dy/national/T111026005025.htm.

Zhang, Jason & Stefano Ortolani. 2019. “HELO Winnti: Attack or Scan.” Lastline, September 30, 2019. https://www.lastline.com/labsblog/helo-winnti-attack-scan/

Zetter, Kim. 2010. “Google Hack Attack Was Ultra Sophisticated.” *Wired*, January 14, 2010. https://www.wired.com/2010/01/operation-aurora/.

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.