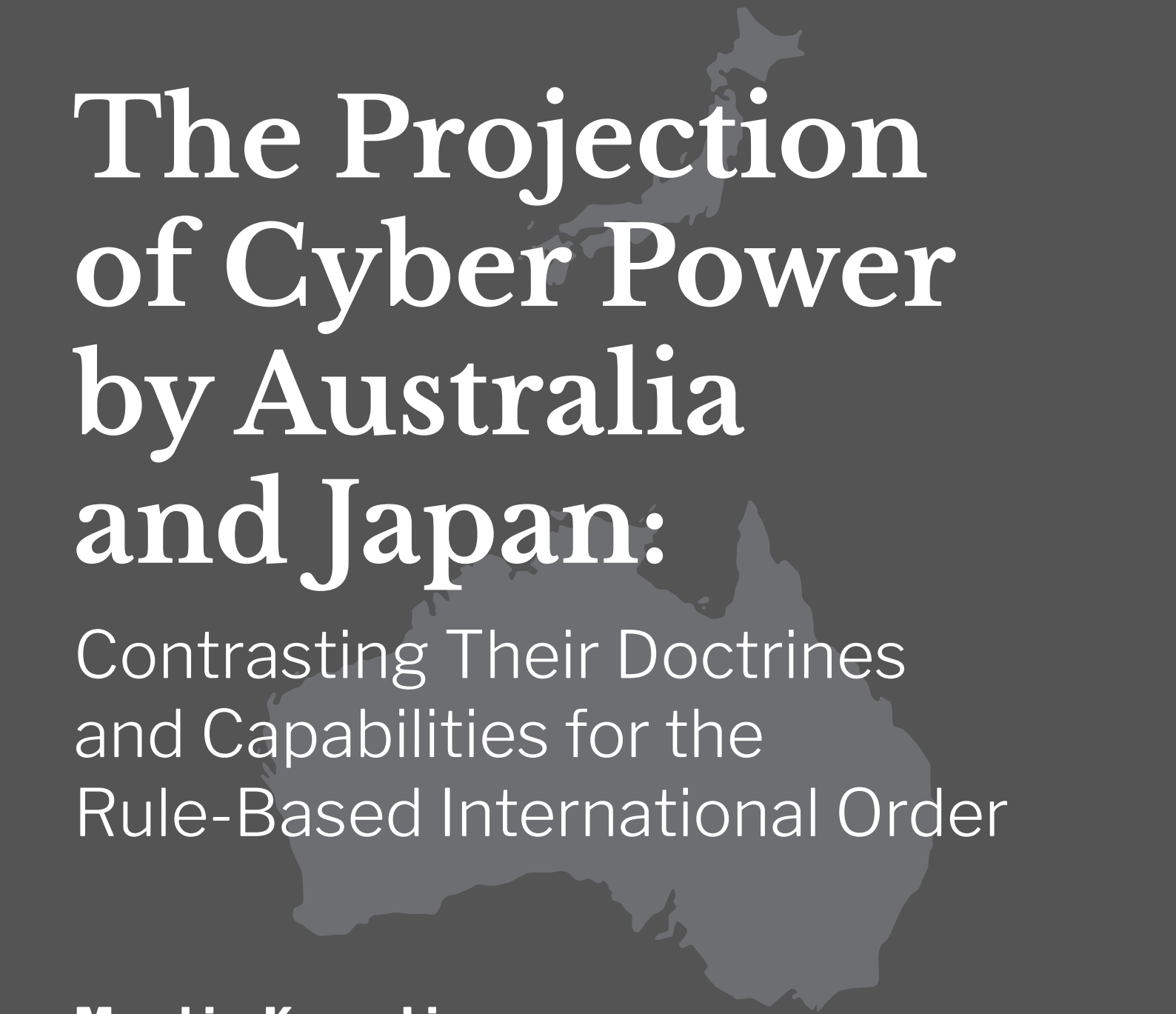

The Projection of Cyber Power by Australia and Japan:

Contrasting Their Doctrines and Capabilities for the Rule-Based International Order

Masahiro Kurosaki

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

Acknowledgements

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This study was produced by an external consultant, contracted to produce studies for the Security and Technology Programme's Cyber Stability workstream, which is funded by the Governments of France, Germany, the Netherlands, Norway, and Switzerland, and by Microsoft. Gratitude is extended to Fergus Hanson and Giacomo Persi Paoli for offering their thoughts on this paper.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

About the Author

MASAHIRO KUROSAKI is Associate Professor of International Law in the Department of International Relations of the National Defense Academy of Japan (NDA) and Director of the Study of Law, Security, and Military Operations at the NDA Center for Global Security.

TABLE OF CONTENTS

On the Research Paper Series

The number of States possessing the capability to conduct international cyber operations against or through foreign information and communications technology (ICT) infrastructure is on the rise. These cyber operations can signal a mounting large-scale threat to the security of a State, could be understood as a violation of sovereignty, and may lead to an escalation.

To facilitate transparency, advance trust among States, and thus promote stability in international cyberspace, the UNIDIR Security and Technology Programme commissioned a series of research papers outlining national capabilities to conduct international cyber operations and the relevant national doctrines regulating the conduct of such operations. In the resulting papers, nine scholars and practitioners provide an overview of the capabilities and doctrines of 15 States across different regions: Australia, Brazil, Canada, China, France, Germany, India, the Islamic Republic of Iran, Israel, Japan, the Republic of Korea, the Russian Federation, Saudi Arabia, the United Kingdom of Great Britain and Northern Ireland, and the United States of America.

To read more about the research paper series, please refer to the "International Cyber Operations: National Doctrines and Capabilities" paper, available at www.unidir.org/cyberdoctrines.

Andraz Kastelic

Lead Cyber Stability Researcher,
Security and Technology Programme, UNIDIR

Introduction

Over the past decade, major power competition has intensified in the Indo-Pacific, revolving around the Korean Peninsula and the East and South China Seas. Under such tense circumstances, Australia and Japan are now both at the forefront of initiatives to enhance security, stability, and prosperity for their shared vision of a rule-based "Free and Open Indo-Pacific".[1] They undertake this within the Quadrilateral Security Dialogue (Quad), a strategic partnership framework involving the United States and India.[2] This shift in national security focus has been accompanied by a marked increase in reliance on cyberspace to achieve their security goals in the region.

In the age of digital transformation, with growing access to the Internet and information and communications technology (ICT) infrastructure, cyberspace has become the main theatre for States to expand their influence in competition for leadership in the Indo-Pacific and around the globe. Yet, as the recent stagnation in the attempts by the United Nations to advance cyber norms of responsible State behaviour illustrates, it remains only halfway towards "a free, open, and secure" digital domain. This has led States and non-State actors to use it "increasingly as a platform for irresponsible behavior", such as "significant disruptive, destructive, or otherwise destabilizing cyber activity".[3] The Indo-Pacific region is thus a potential flashpoint for cyber conflict, and all the more so because the COVID-19 crisis has accelerated such heightened geopolitical rivalry, extending into cyberspace.[4]

Against this backdrop, how are Australia and Japan poised to tackle those security threats with their cyber statecraft? What kinds of challenge do they encounter in maintaining their shared vision of rule-based order? To address these questions, the present paper offers an analysis of how and under what guidance Australia and Japan now seek to build and

1 The Free and Open Indo-Pacific is an updated vision of regional order, first advocated in 2016 by Japanese Prime Minister Shinzo Abe at the Opening Session of the Sixth Tokyo International Conference on African Development (TICAD VI), to combine the Asian and African continents and the Pacific and Indian Oceans. It redefined the geostrategic contours of the Asia-Pacific in a bid to adapt to the changing security environment. The new vision was symbolized by the change in name by the United States of its Pacific Command (PACOM) to Indo-Pacific Command (INDOPACOM) in May 2018. See Japanese Ministry of Foreign Affairs (2020); United States Department of State (2019); Mattis (2018); Australian Department of Foreign Affairs and Trade (2017a, 3–4, 25–27).

2 See, e.g., Japanese Ministry of Foreign Affairs (2019); Australian Department of Defence (2020).

3 Australia et al. (2019).

4 See Australian Department of Foreign Affairs and Trade and Australian Cyber Security Centre (2020).

employ their offensive cyber capabilities – the capabilities to disrupt, degrade, or deny a targeted computer system or network[5] – to project their power outward across the region. In doing so, it offers the following observations. First, Australia has been advancing its offensive cyber capabilities with an eye on a full spectrum of situations covering "grey-zone" activities prevalent in the Indo-Pacific. These capabilities are housed in its major intelligence agency and are intended to discourage offshore malicious actors from targeting its network in violation of cyber norms. Second, in contrast to Australia and due to constitutional constraints, Japan has limited its external cyber capabilities to response by its armed forces to situations of armed attack from other States. Third, notwithstanding the importance of a collective approach to filling gaps in cyber capabilities and readiness between Australia and Japan, there is growing divergence between like-minded States over the applicability of some rules of international law to cyberspace – notably the principles of sovereignty and due diligence. This could have an adverse effect on their willingness to take concerted and effective cyber measures to deter and respond to the expanding grey-zone activities, which need to be overcome to strengthen the rule-based order in the region.

5 As there is no established definition of "offensive cyber capabilities", the present paper follows the understanding by the Australian Government, which defines them as capabilities "that disrupt, deny or degrade the computers or computer networks of adversaries". Australian Department of Foreign Affairs and Trade (2017b, 54). According to the United Kingdom, they "involve deliberate intrusions into opponents' systems or networks, with the intention of causing damage, disruption or destruction". British Government (2016, 51).

The omnidirectional cyber power of Australia

ADAPTATION TO GREY-ZONE CHALLENGES

Australia has reoriented its security strategy to assume a more active and assertive role in defence of a rule-based Indo-Pacific.[6] The 2020 Defence Strategic Update enunciates that "Australia must be an active and assertive advocate for stability, security and sovereignty in our immediate region".[7] It also underlines the vital importance of building up Australia's self-reliant deterrent power and reducing its dependencies on alliance partners.[8] Given that "sharper prioritisation is required" due to its security environment being more complex, this new security strategy demands adjustments and expansion of Australia's force structure and capability.[9] These are to focus on the responses not only to high-intensity conflict, but also to "grey-zone" challenges "below the threshold of armed conflict".[10] The Update's predecessor, the 2016 White Defence Paper, made no mention of these.[11]

As part of this effort, Australia has recently highlighted its offensive cyber capabilities within the framework of the Five Eyes intelligence alliance.[12] It has given the highest priority to bolstering them for the response to diversifying threats targeting its national interests. This is particularly important against the background in which "[e]xpanding cyber capabilities and willingness by some countries and non-state actors to use cyber capabilities maliciously are further complicating Australia's environment", and where online services and infrastructure "will be key targets in grey-zone activities and as a precursor to conventional conflict".[13] The intended use is thus directed at the responses not only to offshore cyber criminals, but also to a range of grey-zone activities.[14] The latter have expanded in the Indo-Pacific, involving "military and non-military forms of assertiveness and coercion aimed at achieving strategic goals without provoking conflict", such as "active interference, disinformation campaigns and economic coercion".[15] In this sense, Australian offensive cyber strategy could be seen as

6 Reynolds (2020).
7 Australian Department of Defence (2020a, 25).
8 Australian Department of Defence (2020a, 27, 40).
9 Australian Department of Defence (2020a, 30).
10 Australian Department of Defence (2020a, 15, 25, 30). See also Reynolds (2020).
11 Australian Department of Defence (2016).
12 See generally Gold (2020).
13 Australian Department of Defence (2020a, 13–14). See also Australian Department of Defence (2020a, 27).
14 See also Australian Department of Defence (2020b, 12).
15 Australian Department of Defence (2020a, 5). See also Australian Department of Defence (2020a, 13).

taking a similar line to the "defend forward" and "persistent engagement" strategies of the United States Department of Defense, which aim "to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict".[16]

Further, it is noteworthy that these offensive cyber capabilities are assigned to the Australian Signals Directorate (ASD) with the complementary support of the Australian Defence Force (ADF).[17] The ASD is under the responsibility of the Minister for Defence and is "Australia's lead operational cyber security agency".[18] In cases where the ASD is engaged in offensive cyber operations in support of ADF operations, those operations are planned and executed by the ASD and the ADF's Joint Operations Command under the direction of the Chief of Joint Operations.[19]

Australia has made it clear that "[a]cknowledging this offensive capability… adds to our credibility as we promote norms of good behaviour on the international stage".[20] Compliance and transparency are key to the rule-based international order that Australia strongly espouses. Hence, in the course of its operations, the ASD is subject to stringent oversight primarily by the Inspector-General of Intelligence and Security. In addition, it must act pursuant to domestic law, notably the 1995 Commonwealth Criminal Code Act and the 2001 Intelligence Services Act.[21] Moreover, applicable existing international law on cyberspace includes the United Nations Charter in its entirety, the 2001 Council of Europe Convention on Cybercrime (Budapest Convention), the law on the use of force (*jus ad bellum*), the principle of non-intervention, international humanitarian law (*jus in bello*), international human rights law, and the law on State responsibility.[22] It should also be borne in mind that other norms articulated in a series of reports of the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security have been led and endorsed by Australia and, as such, play a significant role in guiding the cyber activities of the ASD and other Australian agencies.[23] At the level of military doctrines, the ASD's offensive cyber operations are governed by the ADF's Rules of Engagement informed by, and consistent with, relevant rules of domestic and international law when conducted in support of ADF military operations.[24] In armed conflict, they are "within a well-established system of command and control, within applicable legal frameworks, and subject to orders, directives and procedures" with the support of trained legal officers available to commanders.[25]

16 United States Department of Defense (2018, 1).
17 See Australian Department of Defence (2020b, 28).
18 Australian Government (2020, 21). See also Australian Government (2020, 34): "[T]he Australian Government's eminent authority responsible for three critical missions, namely the collection of signals intelligence, offensive cyber actions and the strengthening of Australia's cyber security".
19 See Australian Department of Foreign Affairs and Trade (2017b, 55).
20 Turnbull (2016).
21 *Criminal Code Act 1995; Intelligence Services Act 2001.* See also Australian Security Intelligence Organisation (n.d.).
22 See, e.g., Australian Department of Foreign Affairs and Trade (2017b, 36, 90–1); Australian Department of Foreign Affairs and Trade (2021).
23 For a non-exhaustive list of Australia's implementation of the 11 norms in the 2015 Group of Governmental Experts report, see Australian Department of Foreign Affairs and Trade (2017b, 47–50, 54). On the reports see generally United Nations Office for Disarmament Affairs (n.d.).
24 See Australian Department of Foreign Affairs and Trade (2017b, 55).
25 Australian Department of Foreign Affairs and Trade (2021, 4).

THE EVOLVING CYBER CAPABILITIES OF THE AUSTRALIAN SIGNALS DIRECTORATE

The ASD's offensive cyber operations cover "a broad range of activities designed to disrupt, degrade or deny" those adversaries and criminals operating online that pose a threat to Australia and its citizens.[26] The ASD's offensive cyber operations were first disclosed in 2016 by Prime Minister Malcolm Turnbull.[27] They were then partially revealed through Australian military operations against the Islamic State group (Daesh) in the Middle East.[28] The ASD's Director-General made clear that it helped the ADF and coalition partners "disrupt Daesh's ability to communicate, launch attacks and spread propaganda", saying "[i]t was the first time that an offensive cyber operation had been conducted so closely synchronised with the movements of military personnel in theatre".[29] In 2017, the Australian Government further directed the ASD "to use its offensive cyber capabilities to disrupt, degrade, deny and deter organised offshore cybercriminals".[30] Since then, ASD's offensive cyber operations have "struck back at the foreign criminals …, successfully disabling their infrastructure and blocking their access to stolen information".[31]

Obviously, it is indispensable for the ASD "to keep pace with the latest technology trends and invest in cutting-edge capabilities" in order to succeed in countering a vast number of anonymous, malicious cyber activities hidden in large volumes of data facilitated by the dark web and encryption technologies.[32]

To that end, Australia has built a set of sophisticated capabilities, such as one to attribute malicious cyber activities "in a timely manner to several levels of granularity – ranging from the broad category of adversary through to specific states and individuals".[33] The Australian Government is now enhancing its ability to conduct defensive and offensive cyber operations. This includes increasing the number of cyber operatives; investing $118 million to expand ASD's data science capabilities and $15 billion to improve network security and resilience over the next decade; integrating intelligence, surveillance, and reconnaissance (ISR) programmes; bolstering signals and information-sharing capabilities; and improving joint command, control, communications, and computers (C4) systems.[34]

With such huge investments in their enhancement, Australia's outward-facing cyber capabilities have thus been adapted towards omnidirectional orientation in a way to accommodate "major shifts in the strategic landscape, including security and stability across the Indo-Pacific".[35] Yet whatever these capabilities might evolve into in the future, one thing is clear: "maintaining the trust of the Australian Government and the Australian public, by demonstrating that ASD operates legally and with propriety, is of the utmost importance to ASD" all the more as "its foreign signals intelligence capabilities are uniquely intrusive, and its offensive cyber operations even more so".[36] Australia's statement on cyber weapons review should also be read in this context.[37]

---

26 Burgess (2019).
27 Turnbull (2016).
28 See Australian Signals Directorate (2019, 30). See also Australian Department of Defence (2016, 45).
29 Burgess (2019).
30 Australian Department of Foreign Affairs and Trade (2017b, 34).
31 Australian Government (2020, 14).
32 Australian Signals Directorate (n.d., 4).
33 Australian Department of Foreign Affairs and Trade (2017b, 54). In Australia's view, "States are entitled, in their sole discretion, and based on their own judgement, to attribute unlawful cyber activities to another State" with reasonable "conclusions based on the facts before them". Australian Department of Foreign Affairs and Trade (2021, 5).
34 Australian Government (2020, 23); Reynolds (2020).
35 Australian Signals Directorate (2019, 14).
36 Australian Signals Directorate (2019, 17).
37 Australian Department of Foreign Affairs and Trade (2021, 4): "A cyber capability could, in certain circumstances, constitute a 'weapon, or a means or method of warfare' within the meaning of Article 36 [of the 1977 Additional Protocol I to the 1949 Geneva Conventions] and require a review in accordance with Article 36 obligations."

The armed attack-oriented cyber power of Japan

AN EXCLUSIVELY DEFENCE-ORIENTED POLICY

Japan has maintained its own "exclusively defence-oriented policy" grounded in "the spirit of the Constitution".[38] It is simultaneously dependent on the offensive capabilities of the United States in accordance with the 1960 Japan–United States Security Treaty.[39] The alliance between Japan and the United States has thus underpinned the Japanese national security strategy as the cornerstone of peace and security of "not only Japan but also the Indo-Pacific region and the international community".[40]

The Japanese Constitution permits Japan to possess only minimum self-defence capability to the extent that it does not constitute a "war potential" against other States.[41] The parameters of this constitutional principle of minimum necessary force are subject to Japan's security environment and other circumstances prevailing at the time and, as such, are to be "discussed and decided through annual budget and other deliberations by the Diet on behalf of the people".[42] Under this framework, Japan had long refrained from possessing an offensive and expeditionary capability that would enable it to project its military power to target the territory of other States. It has even officially avoided using the qualifier "offensive" for its capability in order to avoid creating a misleading image inconsistent with the exclusively defence-oriented policy and the constitutional principle of minimum necessary force.

Yet the recent changes in its security environment have prompted Japan to introduce a more proactive defence strategy with virtually offensive capability, albeit in a manner consistent with the existing constitutional constraints. Since its approval of the National Defense Program Guidelines and Medium Term Defense Program in December 2018, Japan has underlined the vital importance of achieving superiority in the new operational domains of cyber, electromagnetic spectrum, and outer space. This signals an intent "to

38 Japan's "exclusively defence-oriented policy" is generally defined as "the posture of a passive defense strategy in accordance with the spirit of the Constitution". See Japanese Ministry of Defense (2020a, 202).

39 Article III of the Japan–United States Security Treaty reads: "The Parties, individually and in cooperation with each other, by means of continuous and effective self-help and mutual aid will maintain and develop, subject to their constitutional provisions, their capacities to resist armed attack."

40 Japanese Ministry of Defense (2020a, 480).

41 Article 9(2) of the Japanese Constitution lays down that "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."

42 Japanese Ministry of Defense (2020a, 200). Certain offensive military capabilities, the sole purpose of which is mass destruction of adversaries (e.g. intercontinental ballistic missiles (ICBM), long-range strategic bombers, or attack aircraft carriers) are already considered to go beyond the constitutional parameters of minimum necessary force.

deter and counter qualitatively and quantitatively superior military threats" posed by major powers surrounding Japan.[43] In its view, these domains are key for Japan's "Multi-Domain Defense Force" to "execute cross-domain operations, which organically fuse capabilities in all domains to generate synergy and amplify the overall strength" of its deterrent power.[44] With this in mind, the Japanese Government has decided to build, for the first time, its own "capability to disrupt, during attack against Japan, [the] opponent's use of cyberspace for the attack" while carefully avoiding officially labelling it as an "offensive cyber capability".[45]

The National Defense Program Guidelines set the limits on this capability in accordance with the existing policy framework in order for Japan not to become "a military power that poses [a] threat to other countries".[46] Further, Japan shares with Australia an awareness of a security environment in which grey-zone activities are prevalent in the Indo-Pacific region. [47] However, it currently confines the use of this capability to self-defence against armed attack on Japan and its allied and partner States.[48] The government defines an armed attack as "an organized, premeditated use of force against a state" by another State or quasi-State organization and, in its view, even a cyber-only attack could constitute an armed attack if the attack creates extremely serious damage comparable to a physical attack of significant consequence.[49] All of this suggest that Japan's current offensive cyber capability is not directed at any situations below the threshold of armed attack, including malicious cyber operations by non-State actors.

It should also be borne in mind that the use of Japan's cyber self-defence capability could further entail military support from the United States by virtue of the latter's joint defence obligation under Article V of the Japan–United States Security Treaty.[50] This obligation is conditioned on any kinetic effects caused by the cyber armed attack in question extending to "the territories under the administration of Japan".[51] In this way, the use of Japan's capability to disrupt an opponent's use of cyberspace is considered as a use of military force and, as such, shall be consistent with international law and constitutional law governing self-defence.[52]

AMBIGUOUS LEGAL PARAMETERS FOR PEACETIME EXTERNAL CYBER OPERATIONS

Meanwhile, it remains uncertain whether Japan's outward projection of cyber power (rather than physical force) could potentially, at least at the theoretical level, be justified against grey-zone activities in situations below the threshold of armed attack. The Japanese Government only underlines that "we will take whole-of-government measures, ... leveraging all effective means in response to any threat to our national security in cyberspace in collaboration with our ally and coalition partner States, even in cases where it is impossible to determine such a threat as an armed attack on our nation".[53] In Japan, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) takes the initiative in coordination and cooperation between the Japanese public and private sectors to secure cybersspace.[54] Yet Japan's peacetime national cyber

43 Japanese Cabinet (2018, 10).
44 Japanese Cabinet (2018, 10).
45 Japanese Cabinet (2018, 20).
46 Japanese Cabinet (2018, 7).
47 Japanese Cabinet (2018, 3).
48 See, e.g., Tsuchimichi (2020c).
49 A State-sponsored potent cyberattack on the critical infrastructure, such as transportation infrastructure, was one cited possible example for the qualification of an armed attack. Iwaya (2019b, author translation).
50 Iwaya (2019c). Article V of the treaty reads: "Each Party recognizes that an armed attack against either Party in the territories under the administration of Japan would be dangerous to its own peace and safety and declares that it would act to meet the common danger in accordance with its constitutional provisions and processes. Any such armed attack and all measures taken as a result thereof shall be immediately reported to the Security Council of the United Nations in accordance with the provisions of Article 51 of the Charter. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security." See also *The Guidelines for Japan–U.S. Defence Cooperation* (2015, 21–22).
51 Article V of the Japan–US Security Treaty.
52 Tsuchimichi (2020a); Tsuchimichi (2020c). As an aside, the Japanese Constitution only allows the use of force in self-defence and does not recognize an authorization from the United Nations Security Council under Chapter VII of the United Nations Charter as an independent legal basis for the use of force.
53 Abe (2019d, author translation).
54 National Center of Incident Readiness and Strategy for Cybersecurity (n.d.).

capabilities are primarily devoted to defensive operations by the Japan Self-Defense Forces (JSDF), notably, "persistent monitoring of command and communications systems and networks" and their "damage limitation and recovery" on an around-the-clock basis.[55] Judging from this, Japan does not currently seem to be poised to use its cyber capabilities against other States and non-State actors during peacetime, even if they launch malicious cyber activities against its national interests. That said, the Japanese Government has yet to make clear whether this is simply because the external use of its cyber capability *per se* is legally prohibited except in situations of self-defence against armed attack. That is related to the fact that it is unclear how far the international and domestic legal constraints on Japan's extraterritorial cyber operations extend.

On this point, it should be highlighted that Japan is careful about the issue of applicability of the principle of sovereignty to its extraterritorial activity in cyberspace.[56] The issue concerns whether and to what extent the principle is applied as a standalone rule in a manner to prohibit cross-border cyber operations outside the scope of intervention or use of force. It is now hotly debated, primarily in the context of State-sponsored information operations and activities, regardless of whether the purpose is national defence (espionage) or law enforcement (criminal investigation). Recently, the Japanese Government presented its view that "there exist certain forms of violation of sovereignty which may not necessarily constitute unlawful intervention prohibited under the principle of non-intervention", but it left the issue of what forms that violation can take in the cyber context to "State practices and future discussions".[57] At any rate, it should be noted that Japan also recognizes basic rules on State responsibility, including those on countermeasures and necessity, as applying to cyberspace.[58] This leads to the conclusion that, even if future Japanese offensive cyber operations were to violate the sovereignty of other States, they would be justifiable by virtue of the very rules of countermeasures or necessity as a ground for precluding international wrongfulness, insofar as they meet certain requirements.[59]

Turning to the domestic legal constraints in peacetime situations, among the most relevant are the Constitution and the 1999 Act on Prohibition of Unauthorized Computer Access. The former ensures the protection of the secrecy of communication and the latter proscribes unauthorized computer access.[60] Yet these statutory rules say nothing on their extraterritorial applicability to Japan's external cyber operations.[61] It thus seems debatable even at the level of domestic law whether Japan may project its cyber power outward without it constituting a prohibited use of force.[62] This brings us to the next question – if legally permitted, to what extent is Japan currently prepared to put in place necessary arrangements to deploy such capabilities?

---

55 Japanese Cabinet (2018, 20).

56 Japan seems to remain careful about the applicability of the sovereignty principle primarily to see the progress of the issue on trans-border access to data for criminal justice purposes – which, in Japan, is governed by Article 218(2) of the Code of Criminal Procedure – complicated by the "loss of location" problem engendered by cloud computing and encryption technologies. See, e.g., Eda (2011). The issue has long been a focal point of the work of the Council of Europe Cybercrime Convention Committee representing the State Parties to the Budapest Convention. See, e.g., Council of Europe Cybercrime Convention Committee (2013, 9); Council of Europe Cybercrime Convention Committee (2016, 15–17).

57 Japanese Ministry of Foreign Affairs (2021, 3).

58 Japanese Ministry of Foreign Affairs (2021, 4–5); Akahori (2020).

59 The requirements are set out in Articles 22, 25, 49–54 of the Articles on the Responsibility of States for Internationally Wrongful Acts prepared by the United Nations International Law Commission. See United Nations (2007, 27, 30). Yet not all of these rules are necessarily considered by States to reflect customary international law. To take a prominent example, France and the United Kingdom reject a notification requirement for lawful countermeasures in the cyber context. See French Ministry of the Armed Forces (2019, 8); Wright (2018).

60 Article 21(2) of the Constitution of Japan provides: "No censorship shall be maintained, nor shall the secrecy of any means of communication be violated." The Act on Prohibition of Unauthorized Computer Access stipulates that "[n]o person shall engage in an act of unauthorized computer access" (Article 3) as defined in Article 2(4) and punishes the act "by imprisonment with work for not more than three years or a fine of not more than 1 million yen" (Article 11). The Penal Code also criminalizes electromagnetic records that give unauthorized commands in its Articles 168-2 and 168-3 – the so-called "crime of the creation of computer viruses" – as part of the implementation of the Budapest Convention. The crime is extraterritorially applicable to offences committed by Japanese nationals outside the territorial jurisdiction of Japan (Article 4*bis*) in accordance with Article 22(1)(d) of the Budapest Convention. Nevertheless, the Japanese Government has said that the creation of computer viruses by a State could be justifiable even in peacetime, insofar as it is in accordance with laws and regulations or is in pursuit of lawful business (Article 35). See Tsuchimichi (2020b).

61 A remarkable ruling from the German Constitutional Court recently found that the Federal Intelligence Service is bound by the fundamental rights of the Basic Law when conducting its telecommunications surveillance of non-German citizens in other countries. This may have significant ramifications for future development on the issue. See German Federal Constitutional Court (2020).

62 In this respect, one might pay attention to Article 4(18) of the Act for the Establishment of the Ministry of Defense, which authorizes the JSDF to conduct surveys and research with a view to performing their duties. Based on the provision, the JSDF has conducted a broad range of overseas activities, such as the one aimed at ensuring freedom of navigation of the Japanese-flagged vessels in the high seas in the name of information gathering.

THE NASCENT CYBER CAPABILITIES OF THE JAPAN SELF-DEFENSE FORCES

The Japanese Government has expressed its resolve to respond decisively to any cyberthreat to Japan's security with all possible effective means and capabilities on a whole-of-government basis under the initiative of the Cabinet Secretariat and the NISC.[63] As discussed above, however, the response is currently limited to the JSDF, which is responsible for use of the capability to disrupt malicious cyber operations by foreign adversaries in situations of armed attack.[64] The possession of any other offensive cyber capabilities by the government is not envisaged at present.

The JSDF is now on track for a cyber evolution. In its Defense Programs and Budget 2021, the Japanese Government presented a plan to reorganize the JSDF's C4 Systems Command (C4SC), which operates and maintains the Defense Information Infrastructure (DII) and Central Command System (CCS), into a new command – tentatively named the "Cyber Command" – to be composed of approximately 540 personnel by the end of 2021. With a budget of 35.7 billion yen (approximately $325 million) in fiscal year 2021, the new command is intended to unify cyber defence functions currently distributed across the Ground, Maritime and Air Self-Defense Forces and thereby achieve more effective and efficient performance of their duties.[65]

While it declines to specify how this capability has evolved for security reasons, the Japanese Government admits that the JSDF has gained certain skills and techniques by building and developing its own cyber ranges, including malware creation and analysis and operational exercises.[66] As part of this effort, the JSDF seeks to utilize new and emerging and disruptive technologies, such as artificial intelligence (AI) and the fifth generation technology standard for cellular networks (5G), particularly for the purpose of appropriately gauging an indication of cyberattack for a split-second response.[67] The government has further announced that the JSDF plans to increase its cyber personnel to more than 1000 by around 2023.[68]

There is a growing need in Japan for offensive cyber strike capabilities to intercept and thwart an armed attack that is in progress within the territory of an adversary.[69] Yet Japan has just embarked on an offensive drive in its own cybersecurity efforts intended for an armed attack situation, and its cyber capabilities are still at a nascent stage. Most importantly, unlike Australia's capabilities, Japan's have never been employed in actual operations as Japan has never exercised its right to self-defence against armed attack. To be sure, Japan's overall cyber power may need to be assessed in combination with that of the United States since its duty to defend Japan means that its most advanced cyber capabilities could make up for Japan's shortcomings and readiness. But that duty applies only in situations of armed attack on the territories under the administration of Japan. In other situations of threat, the JSDF's cyber capabilities are not currently envisaged to be employed extraterritorially nor is the United States obliged to support Japan by cyber means. Given that its cyber deterrence posture is thus critically inadequate against malicious grey-zone activities, Japan needs to improve the posture promptly through putting in place a transparent framework that lays out firm responsive measures to those threats within the parameters of international law and the Constitution. This is all the more so because, as Japan itself has declared jointly with like-minded States, "[t]here must be consequences for bad behavior in cyberspace".[70]

63 Abe (2019b).
64 Japanese Ministry of Defence (n.d.).
65 Japanese Ministry of Defense (2020b, 9).
66 Suzuki (2020); Tsuchimichi (2020b). This seems to fall within the 2021 budget allocation for research and development on new cyber technologies (JPY 2.1bn). See Japanese Ministry of Defense (2020b, 9, 28, 46).
67 Kono (2020); Iwaya (2019a).
68 Abe (2019c).
69 It culminated in the revived debate over whether Japan should acquire weapons capable of striking missile launch sites in enemy territory. This move led to a proposal approved in August 2020 by the country's ruling Liberal Democratic Party for Japan to acquire "capabilities to halt ballistic missile attacks, etc. within the territory of adversaries". Liberal Democratic Party Political Survey Committee. 2020 (author translation).
70 Australia et al. (2019).

Challenges to collective responses to the grey zone

There is a significant gap between the offensive cyber capabilities and readiness of Australia and Japan. In such circumstances, to ensure the maintenance of the rule-based order and to more effectively deter and counter cyberthreats, a collective and multilateral approach to filling the gap involving highly cyber-capable States is indispensable. To pick up one strand of this approach, it is worthwhile noting that New Zealand recently expressed its intent, backing Estonia, to give active consideration to the issue of collective countermeasures in the "collective interest in the observance of international law" in view of "the potential asymmetry between malicious and victim states".[71]

This type of countermeasure, if permissible, would become most effective when an agreement is reached between victim States and assisting States as to what rules of international law are violated in cyberspace. Yet what makes it hard is the growing divergence among like-minded States on the basic rules of international law governing cross-border cyber operations that fall below the use of force and intervention. The most notable focal points are the general principles of sovereignty and due diligence.

The principle of sovereignty under general international law "represents the most significant red line between lawful and internationally wrongful conduct".[72] If applicable, it would thus come as a direct prohibition on those cyber operations that fall below the use of force and intervention, and the breach of the prohibition gives rise to an internationally wrongful act as a precondition for taking lawful countermeasures. As discussed above, however, the applicability of the principle is currently highly controversial among States leading up to the debate on the "sovereignty-as-principle" approach versus the "sovereignty-as-rule" approach. To date, the United Kingdom and, with some ambivalence, the United States have

71 New Zealand Foreign Affairs & Trade (2020). France rejected this Estonia's proposition. See French Ministry of the Armed Forces (2019, 8).
72 Schmitt and Vihul (2017, 213).

showed their hesitancy to recognize the principle as a legally binding prohibition in cyberspace.[73] This implies that the *sui generis* character of cyberspace, as opposed to the physical realm, leans toward the exclusion of general international law grounded in the principle of territoriality.[74] Interestingly, Australia, New Zealand, the United Kingdom, and the United States are all members of the Five Eyes, which has played a leading role in like-minded efforts to advance responsible State behaviour in cyberspace. Their positions may sometimes reflect an attitude of the alliance, but at least at the moment, Australia seems to carefully avoid taking a position on the issue, going no further than taking note of it.[75] Yet, as Finland has pointed out, "[a]greeing that a hostile cyber operation below the threshold of prohibited intervention cannot amount to an internationally wrongful act would leave such operations unregulated and deprive the target State of an important opportunity to claim its rights", including countermeasures to induce compliance with the rule of international law that the target State believes is violated.[76] Japan's "sovereignty-as-rule" approach is definitely in line with the Finnish statement.[77]

The same goes with the due diligence principle. It would require all States not to knowingly allow the use of their territory or cyber infrastructure under their jurisdiction for malicious cyber operations by both non-State actors and foreign States contrary to the rights of other States. Japan maintains the stance that "States have a due diligence obligation regarding cyber operations under international law", including the obligation of a territorial State "to exercise its capacity to influence the state-supported person or group of persons so as to prevent them from implementing such cyber operations".[78] However, some States, in varying degrees, remain wary about recognizing the legally binding status of the due diligence principle in cyberspace beyond a voluntary non-binding norm of responsible State behaviour.[79]

---

73 In the case of the United Kingdom, the controversy was sparked by a 2018 speech by Attorney General Jeremy Wright, in which he said: "Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law." Wright (2018).
On the United States, see Ney (2020): "The [Department of Defense Office of the General Counsel] view, which we have applied in legal reviews of military cyber operations to date, shares similarities with the view expressed by the U.K. Government in 2018." At the same time, however, it must be noted that the US Department of State takes a nuanced approach that does not necessarily exclude the possibility of the "sovereignty-as-rule" approach: "In certain circumstances, one State's non-consensual cyber operation in another State's territory could violate international law, even if it falls below the threshold of a use of force. This is a challenging area of the law that raises difficult questions. The very design of the Internet may lead to some encroachment on other sovereign jurisdictions. Precisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully, and it is one that ultimately will be resolved through the practice and opinio juris of States." Egan (2016).

74 While confirming that "the standalone rule of territorial sovereignty also applies in the cyber context", New Zealand underlines the unterritorial nature of cyberspace, stating that "the application of the rule of territorial sovereignty in cyberspace must take into account some critical features that distinguish cyberspace from the physical realm", notably "i) cyberspace contains a virtual element which has no clear territorial link; ii) cyber activity may involve cyber infrastructure operating simultaneously in multiple territories and diffuse jurisdictions; and iii) the lack of physical distance in cyberspace". New Zealand Foreign Affairs & Trade (2020). Such a *sui generis* character also seems to be shared, to a certain degree, by Australia, which contrasts cyberspace with "the physical realm". See Australian Department of Foreign Affairs and Trade (2021). In contrast, Japan enunciates that "[t]he term 'cyberspace' does not imply the existence of a space which does not belong to real space". Japanese Ministry of Foreign Affairs (2021, 2).

75 See, e.g., Australian Department of Foreign Affairs and Trade (2017b, 90): "Australia recognises that activities conducted in cyberspace raise new challenges for the application of international law, including issues of sovereignty, attribution and jurisdiction, given that different actors engage in a range of cyber activities which may cross multiple national borders."

76 Finnish Ministry of Foreign Affairs (2020, 3).

77 Japanese Ministry of Foreign Affairs (2021, 2): "The Government of Japan also hopes that the deepening of a shared understanding – particularly regarding which activities in cyberspace constitute a violation of international law and which tools are available under international law for States whose legal interests have been infringed by cyber operations – will deter malicious activities in cyberspace."

78 Japanese Ministry of Foreign Affairs (2021, 5–6). In addition, Japan is now very active in promoting the establishment of the rule in cyberspace, supporting an Oxford University research project on cyber due diligence. See Oxford Institute for Ethics, Law and Armed Conflict (n.d.).

79 In fact, the 2015 Group of Governmental Experts report merely declares that States "should" consider due regard for sovereignty. Australia, for its part, supports a territorial State's due diligence obligation to ensure ICT infrastructure located within its territory is not used to harm other States, as a result of "the right to exercise sovereignty over objects and activities within its territory". Yet it is not clear if cyberspace, including cloud data, is entirely under the territorial control of a State that underlies the exercise of its sovereignty. See Australian Department of Foreign Affairs and Trade (2021, 5). The most negative view would be the Argentine view: "under international law, there is no obligation of due diligence when it comes to cybersecurity". See Argentine Republic (2020). See also Schondorf (2020).

Given the shared awareness that malicious grey-zone activities are on the rise in the Indo-Pacific, the disagreement among like-minded States on the applicability of such basic rules of international law governing those activities could lead to the destabilization of the shared regional and global order.[80] As Australia is well aware, "in the absence of well-developed understandings about how to behave, there is a risk that unexplained cyber incidents could escalate … into conflict between states". [81] It is therefore imperative to "[f]oster recognition through diplomatic outreach and defence engagement that military offensive cyber capabilities are subject to the same limitations and obligations as any other military capability".[82] With that aim, for starters at the regional level, like-minded States should prioritize reaching an agreement on how those rules of international law are applicable to offensive cyber operations below the threshold of the use of force and intervention.[83]

80 Australia is well aware of this point. See Australian Department of Defence (2020a, 12): "The rules, norms and institutions that help maintain peace and security and guide global cooperation are under strain. Pressures on governance in the global commons, and in domains such as space and cyberspace, will open up potential sources of friction. The thresholds for activities that could trigger a military response are unclear in space and cyberspace as they lack the more clearly defined boundaries of national borders and geography."

81 Turnbull (2016).

82 Australian Department of Foreign Affairs and Trade (2017b, 53, 101).

83 See also Rasser (2021), who recommends that Australia's leaders consider focusing "in the near term on pursuing multilateral engagement for setting norms that promote a free and open cyberspace; crafting multilateral responses to nefarious cyber activity in accordance with international law; and spearheading a shared monitoring and cyber-intrusion remediation capability".

Conclusion

Overall, Australia and Japan have both developed offensive cyber capabilities designed to deter and counter malicious cyber operations by foreign adversaries. Yet the above analysis reveals considerable gaps between the two countries in their orientation, readiness, and proficiency.

In an effort to put the full spectrum of security threats in the Indo-Pacific within its range, Australia, as a Five Eyes member, has adapted its offensive cyber capabilities to respond to malicious grey-zone activities posed by foreign State and non-State adversaries. In contrast, Japan has limited its cyber capabilities to self-defence against armed attack by other States due to its constitutional constraints. Unlike Australia, the outward projection of Japan's cyber power does not currently cover situations below the threshold of armed attack, including transnational cyber operations by non-State actors.

Further, to be more effective and readily available, the projection set-up of Australia's evolving offensive cyber capabilities is unified under the lead intelligence agency, which has experience of actual deployments as represented by participation in military operations by the United States-led coalition against the Islamic State group. In contrast, Japan's military cyber capabilities are still under construction to meet the intended objectives and have never been in actual use, although they are potentially compensated for by the cyber power of the United States in certain armed attack situations through the bilateral treaty mechanism.

Taken together, it is imperative in the short term to cover the shortfall caused by Japan's inadequate cyber deterrence posture by creating a collective cyber response mechanism. Notably, this should target malicious grey-zone activities in order to maintain the rule-based international order in the Indo-Pacific, which is currently under tension. One possible strategy is to push forward the controversial issue of collective cyber countermeasures taken by highly cyber-capable States to induce compliance with international law by the offending State. Yet taking this measure requires an agreement by assisting and victim States on what rules of international law are violated. Hence, Australia and Japan, together with like-minded States in the region, need to solve the issue in advance on the applicability of rules governing malicious grey-zone activities, notably on the principles of sovereignty and due diligence.

References

Abe, Shinzo (Japanese Prime Minister). 2019a. Reply. 第198回国会衆議院会議録第24号: 13 [Minutes of the 198th Japanese House of Representatives Meeting No. 24: 13]. 16 May 2019. As of 20 October 2021: https://kokkai.ndl.go.jp/#/detail?minId=119805254X02420190516&spkNum=45&single.

— — —. 2019b. Reply. 第198回国会衆議院会議録第24号: 14 [Minutes of the 198th Japanese House of Representatives Meeting No. 24: 14]. 16 May 2019. As of 20 October 2021: https://kokkai.ndl.go.jp/#/detail?minId=119805254X02420190516&spkNum=48&single.

— — —. 2019c. Reply. 第198回国会衆議院会議録第24号: 5 [Minutes of the 198th Japanese House of Representatives Meeting No. 24: 5]. 7 June 2019. As of 20 October 2021: https://kokkai.ndl.go.jp/#/detail?minId=119815254X02420190607&spkNum=21&single.

— — —. 2019d. Reply. 第198回国会参議院会議録第24号: 13 [Minutes of the 198th Japanese House of Councillors Meeting No. 24: 13]. 7 June 2019. As of 20 October 2021: https://kokkai.ndl.go.jp/#/detail?minId=119815254X02420190607&spkNum=41&current=-1.

Act on Prohibition of Unauthorized Computer Access. Japanese Act No. 128 of 1999 (Amendment No. 28 of 2013). As of 20 October 2021: https://www.npa.go.jp/cyber/english/legislation/uca_Tentative.pdf.

Akahori, Takeshi (Japanese Ambassador for Cyber Policy). 2020. *Statement on the occasion of the virtual informal meeting of the OEWG on ICTs*. 2020. Permanent Mission of Japan to the United Nations. 29 September 2020. As of 20 October 2021: https://www.un.emb-japan.go.jp/itpr_en/akahori092920.html.

Argentine Republic. 2020. *The Statement by the Argentine Republic at the 4th meeting of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security – Second Substantive Session*. 10–14 February 2020. As of 20 October 2021: https://media.un.org/en/asset/k18/k18w6jq6eg.

Australia et al. 2019. *Joint Statement on Advancing Responsible State Behavior in Cyberspace*. United States Department of State. 23 September 2019. As of 20 October 2021: https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace.

Australian Department of Defence. 2016. *2016 Defence White Paper*. As of 20 October 2021: https://www1.defence.gov.au/sites/default/files/2021-08/2016-Defence-White-Paper.pdf.

— — —. 2020a. *2020 Defence Strategic Update*. As of 20 October 2021: https://www1.defence.gov.au/sites/default/files/2020-11/2020_Defence_Strategic_Update.pdf.

— — —. 2020b. *2020 Force Structure Plan*. As of 20 October 2021: https://www1.defence.gov.au/sites/default/files/2020-11/2020_Force_Structure_Plan.pdf.

— — —. 2020c. *Australia, Japan and US exercise in Philippine Sea*. 21 July 2020. As of 20 October 2021: https://news.defence.gov.au/media/media-releases/australia-japan-and-us-exercise-philippine-sea.

Australian Department of Foreign Affairs and Trade. 2017a. 2017 *Foreign Policy White Paper*. As of 20 October 2021: https://www.dfat.gov.au/sites/default/files/2017-foreign-policy-white-paper.pdf.

— — —. 2017b. Australia's International Cyber Engagement Strategy. As of 20 October 2021. As of 20 October 2021: https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf.

— — —. 2021. *Australia's Submission on International Law to be Annexed to the Report of the 2021 Group of Governmental Experts on Cyber*. As of 20 October 2021: https://www.internationalcybertech.gov.au/sites/default/files/2021-06/Australia%20Annex%20-%20Final%2C%20as%20submitted%20to%20GGE%20Secretariat.pdf.

Australian Department of Foreign Affairs and Trade and Australian Cyber Security Centre. 2020. *Unacceptable Malicious Cyber Activity*. 20 May 2020. As of 20 October 2021: https://www.dfat.gov.au/news/news/unacceptable-malicious-cyber-activity.

Australian Government. 2020. *Australia's Cyber Security Strategy 2020*. As of 20 October 2021: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

Australian Security Intelligence Organisation. n.d. *Counter Espionage and Foreign Interference*. As of 20 October 2021: https://www.asio.gov.au/counter-espionage.html.

Australian Signals Directorate. 2019. *Annual Report 2018–19*. As of 20 October 2021: https://www.asd.gov.au/publications/annual-report-2018-19.

— — —. n.d. *Portfolio Budget Statements 2019–20: Australian Signals Directorate*, Budget Related Paper No. 1.4A. As of 20 October 2021: https://www.asd.gov.au/sites/default/files/2019-10/defence_portfolio_budget_statement_australian_signals_directorate_extract_from_defence.pdf.

British Government. 2016. *National Cyber Security Strategy 2016–2021*. 1 November 2016. As of 20 October 2021: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Burgess, Mike (Director General of the ASD). 2019. *Director-General ASD Speech to the Lowy Institute*. 27 March 2019. As of 20 October 2021: https://www.asd.gov.au/publications/speech-lowy-institute-speech.

Council of Europe Cybercrime Convention Committee. 2013. *Report of the Transborder Group for 2013*. 5 November 2013. As of 20 October 2021: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79eb.

— — —. 2016. *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY.* 16 September 2016. As of 20 October 2021: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.

Criminal Code Act 1995. Australian Act No. 12. 1995 (as amended and in force on 1 July 2017). As of 20 October 2021: https://www.legislation.gov.au/Details/C2017C00235.

Eda, Satsuki (Japanese Justice Minister). 2011. Reply. 第177回国会衆議院法務委員会議録第14号: 10 [Minutes of the 177th Japanese House of Representatives Meeting No. 14: 10]. 27 May 2011. As of 20 October 2021: https://kokkai.ndl.go.jp/txt/117705206X01420110527/105.

Egan, Brian J. (Legal Adviser). 2016. *Remarks on International Law and Stability in Cyberspace, Berkeley Law School, California*. 10 November 2016. As of 20 October 2021: https://2009-2017.state.gov/s/l/releases/remarks/264303.htm.

Finnish Ministry of Foreign Affairs. 2020. *International Law and Cyberspace – Finland's National Positions*. 15 October 2020. As of 20 October 2021: https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf.

French Ministry of the Armed Forces. 2019. *Droit international appliqué aux opérations dans le cyberespace* [International law applicable to operations in cyberspace]. 9 September 2019. As of 20 October 2021: https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqué+aux+opérations+Cyberespace.pdf.

German Federal Constitutional Court. 2020. *In their current form, surveillance powers of the Federal Intelligence Service regarding foreign telecommunications violate fundamental rights of the Basic Law.* Press Release No. 37/2020. 19 May 2020. As of 20 October 2021: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-037.html.

Gold, Josh. 2020. 'The Five Eyes and Offensive Cyber Capabilities: Building a "Cyber Deterrence Initiative".' NATO Cooperative Cyber Defence Centre of Excellence. As of 20 October 2021: https://ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf.

Intelligence Services Act 2001. Australian Act No. 152. 2001 (amended and in force on 13 December 2019). As of 20 October 2021: https://www.legislation.gov.au/Details/C2020C00029.

Iwaya, Takeshi (Japanese Defense Minister). 2019a. Reply. 第198回国会参議院防衛委員会議録第4号: 16 [Minutes of the 198th Japanese House of Councillors Meeting No. 4: 16]. 19 March 2019. As of 20 October 2021: https://kokkai.ndl.go.jp/#/detail?minId=119813950X00420190319&spkNum=184&single.

— — —. 2019b. Reply. 第198回国会参議院防衛委員会議録第4号: 20 [Minutes of the 198th Japanese House of Councillors Meeting No. 4: 20]. 19 March 2019. As of 20 October 2021: https://kokkai.ndl.go.jp/#/detail?minId=119813950X00420190319&spkNum=222&single.

— — —. 2019c. Reply. 第198回国会衆議院会議録第24号: 15 [Minutes of the 198th Japanese House of Representatives Meeting No. 24: 15]. 16 May 2019. As of 20 October 2021: https://kokkai.ndl.go.jp/#/detail?minId=119805254X02420190516&spkNum=49&single.

Japanese Cabinet. 2018. *National Defense Program Guidelines for FY 2019 and Beyond.* 18 December 2018. As of 20 October 2021: http://www.cas.go.jp/jp/siryou/pdf/2019boueikeikaku_e.pdf.

Japanese Ministry of Defense. 2020a. *Defence of Japan 2020*. 7 September 2020. As of 20 October 2021: https://www.mod.go.jp/en/publ/w_paper/wp2020/DOJ2020_EN_Full.pdf.

— — —. 2020b. 我が国の防衛と予算: 令和３年度概算要求の概要 [Defence programmes and budget of Japan: Outline of the budget request for 2021]. 30 September 2020. As of 20 October 2021: https://www.mod.go.jp/j/yosan/yosan_gaiyo/2021/yosan_20200930.pdf.

— — —. n.d. *Regarding Response to a Cyber Attack*. As of 20 October 2021: https://www.mod.go.jp/en/publ/answers/cyber/index.html.

Japanese Ministry of Foreign Affairs. 2019. *Ninth Japan–United States–Australia Trilateral Strategic Dialogue (TSD).* 1 August 2019. As of 20 October 2021: https://www.mofa.go.jp/a_o/ocn/page4e_001053.html.

— — —. 2020. *Free and Open Indo-Pacific.* 7 August 2020. As of 20 October 2021: https://www.mofa.go.jp/policy/page25e_000278.html.

— — —. 2021. *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations.* 28 May 2021. As of 20 October 2021: https://www.mofa.go.jp/files/100200935.pdf.

Kono, Taro (Japanese Defense Minister). 2020. Reply. 第201回国会衆議院安全保障委員会議録第4号: 3 [Minutes of the 201st Japanese House of Representatives Meeting No. 4: 3]. 7 April 2020. As of 20 October 2021: https://kokkai.ndl.go.jp/#/detail?minId=120103815X00420200407&spkNum=13&single.

Liberal Democratic Party Political Survey Committee. 2020. 国民を守るための抑止力向上に関する提言 [Recommendations for improving deterrence to protect the people]. 4 August 2020. As of 20 October 2021: https://jimin.jp-east-2.storage.api.nifcloud.com/pdf/news/policy/200442_1.pdf.

Mattis, James N. (US Secretary of Defense). 2018. *Remarks at U.S. Indo-Pacific Command Change of Command Ceremony*. 30 May 2018. As of 20 October 2021: https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1535689/remarks-at-us-indo-pacific-command-change-of-command-ceremony.

National Center of Incident Readiness and Strategy for Cybersecurity (NISC). n.d. *About NISC*. As of 20 October 2021: https://www.nisc.go.jp/eng/index.html.

New Zealand Foreign Affairs & Trade. 2020. *The Application of International Law to State Activity in Cyberspace*. 1 December 2020. As of 20 October 2021: https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf.

Ney, Paul C., Jr. 2020. *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*. United States Department of Defense. 2 March 2020. As of 20 October 2021: https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference.

Oxford Institute for Ethics, Law and Armed Conflict (ELAC). n.d. *Cyber Due Diligence*. University of Oxford. As of 20 October 2021: https://www.elac.ox.ac.uk/cyber-due-diligence.

Penal Code. Japanese Act No. 45 of 24 April 1907 (Amended by Act No. 72 of 2017). As of 20 October 2021: http://www.japaneselawtranslation.go.jp/law/detail/?ft=2&re=2&dn=1&yo=刑法&x=51&y=14&ia=03&ja=04&ph=&ky=&page=1&id=3581&lvm=02.

Rasser, Martijn. 2021. 'Networked: Techno-Democratic Statecraft for Australia and the Quad'. Center for a New American Security. 19 January 2021. As of 20 October 2021: https://www.cnas.org/publications/reports/networked-techno-democratic-statecraft-for-australia-and-the-quad.

Reynolds, Linda (Australian Minister for Defence). 2020. *Speech – Australian Strategic Policy Institute*. 2 July 2020. As of 20 October 2021: https://www.minister.defence.gov.au/minister/lreynolds/speeches/speech-australian-strategic-policy-institute.

Schmitt, Michael N. and Vihul, Liis. 2017. 'Sovereignty in Cyberspace: *Lex Lata Vel Non?'. AJIL Unbound* 111: 213–218. As of 20 October 2021: https://doi.org/10.1017/aju.2017.55.

Schondorf, Roy (Israel's Deputy Attorney General). 2020. 'Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations'. EJIL: Talk!, 9 December 2020. As of 20 October 2021: https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations.

The Constitution of Japan. 3 November 1946. As of 20 October 2021: https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html.

The Guidelines for Japan–U.S. Defense Cooperation. 27 April 2015. As of 20 October 2021: https://www.mofa.go.jp/files/000078188.pdf.

Treaty of Mutual Cooperation and Security Between Japan and the United States of America (The Japan–US Security Treaty). 19 January 1960. As of 20 October 2021: https://www.mofa.go.jp/region/n-america/us/q&a/ref/1.html.

Turnbull, Malcolm (Australian Prime Minister). 2016. 'Launch of Australia's Cyber Security Strategy Sydney', *PM Transcripts from the Prime Ministers of Australia, Department of the Prime Minister and Cabinet*. 21 April 2016. As of 20 October 2021: https://pmtranscripts.pmc.gov.au/release/transcript-40308.

Suzuki, Atsuo (Director General of the Bureau of Defense Buildup Planning of Japanese Ministry of Defense). 2020. Reply. 第201回国会衆議院安全保障委員会議録第4号: 13 [Minutes of the 201st Japanese House of Representatives Meeting No. 4: 13]. 7 April 2020. As of 20 October 2021: https://kokkai.ndl.go.jp/#/detail?minId=120103815X00420200407&spkNum=86&current=-1.

Tsuchimichi, Akihiro (Director General of the Bureau of Defense Policy of Japanese Ministry of Defense). 2020a. Reply. 第201回国会衆議院安全保障委員会議録第4号: 5 [Minutes of the 201st Japanese House of Representatives Meeting No. 4: 5]. 7 April 2020. As of 20 October 2021: https://kokkai.ndl.go.jp/#/detail?minId=120103815X00420200407&spkNum=25&current=-1.

— — —. 2020b. Reply. 第201回国会衆議院安全保障委員会議録第4号: 13 [Minutes of the 201st Japanese House of Representatives Meeting No. 4: 13]. 7 April 2020. As of 20 October 2021: https://kokkai.ndl.go.jp/#/detail?minId=120103815X00420200407&spkNum=90&current=-1.

— — —. 2020c. Reply. 第201回国会参議院外交防衛委員会議録第9号: 5 [Minutes of the 201st Japanese House of Councillors Meeting No. 9: 5]. 16 April 2020. As of 20 October 2021: https://kokkai.ndl.go.jp/#/detail?minId=120113950X00920200416&spkNum=33&current=1.=1.

United Nations. 2001. 'A/56/10: Report of the International Law Commission on the work of its fifty-third session (23 April–1 June and 2 July–10 August 2001)'. *Yearbook of the International Law Commission*, Volume II Part 2, A/CN.4/SER.A/2001/Add.1 (Part 2): 1–208.

United Nations Office for Disarmament Affairs. n.d. *Developments in the Field of Information and Telecommunications in the Context of International Security*. As of 20 October 2021: https://www.un.org/disarmament/ict-security.

United States Department of Defense. 2018. *Summary: Department of Defence Cyber Strategy*. As of 20 October 2021: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

United States Department of State. 2019. *A Free and Open Indo-Pacific: Advancing a Shared Vision*. 4 November 2019. As of 20 October 2021: https://www.state.gov/wp-content/uploads/2019/11/Free-and-Open-Indo-Pacific-4Nov2019.pdf.

Wright, Jeremy (British Attorney General). 2018. *Cyber and International Law in the 21st Century*. Attorney General's Office, 23 May 2018. As of 20 October 2021: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

The Projection of Cyber Power by Australia and Japan:

Contrasting Their Doctrines and Capabilities for the Rule-Based International Order

This paper offers an analysis of how and under what guidance Australia and Japan now seek to build and employ their offensive cyber capabilities – the capabilities to disrupt, degrade, or deny a targeted computer system or network – to project their power outward across the region. In doing so, it offers the following observations. First, Australia has been advancing its offensive cyber capabilities with an eye on a full spectrum of situations covering "grey-zone" activities prevalent in the Indo-Pacific. These capabilities are housed in its major intelligence agency and are intended to discourage offshore malicious actors from targeting its networks in violation of cyber norms. Second, Japan has limited its external cyber capabilities to responses by its armed forces and to situations of an armed attack. Third, notwithstanding the importance of a collective approach to filling gaps in cyber capabilities between Australia and Japan, there is growing divergence between like-minded States over the applicability of some rules of international law to cyberspace – notably the principles of sovereignty and due diligence. This could have an adverse effect on their willingness to take concerted and effective cyber measures against the growing "grey-zone" cyber activities in the region.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH