Conference Report

Asia-Pacific Programme

March 2021

Security at the frontier

UK–Japan perspectives on cyberspace, outer space, the Arctic and electronic warfare

With essays by Emily Taylor, Alexandra Stickings, Aki Tonami and Jun Nagashima

CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Contents

Introduction

Increasing global connectivity has brought with it a new range of security threats that were unfathomable just decades ago. Global reliance on the internet and on virtual networks has revealed a range of new cyber vulnerabilities and threats, including to critical infrastructure and the Internet of Things (IoT).

Cyber technology has brought with it a new security focus on outer space, which has become key to the functioning of national and international infrastructure on the ground. Furthermore, technologies using the electromagnetic spectrum, which are increasingly integral to military operations, create new challenges and adversarial threats including the prospect of electronic warfare.

These challenges have expanded geographically too, as countries explore new physical frontiers, like the Arctic, as regions of strategic interest. This conference report, comprising of four expert essays and a meeting summary, draws upon Chatham House's December 2020 conference 'Security at the Frontier',[1] to examine the latest developments in cyberspace, outer space, the Arctic and electronic warfare, and considers how best the UK and Japan might respond to these challenges.

[1] See Chatham House (2020), 'Security at the Frontier', 10–11 December 2020, https://www.chathamhouse.org/events/all/research-event/security-frontier-uk-japan-perspectives.

UK–Japan cyber cooperation

By Emily Taylor
Associate Fellow,
International Security Programme,
Chatham House

The internet has come a long way since Vint Cerf and Bob Kahn developed the Transmission Control Protocol/Internet Protocol (TCP/IP) and made the pivotal decision not to put an upper limit on the number of networks that could be connected. Design choices matter; they define what is and isn't possible, and, in this instance, set the rules for the hardware, products and services that connect to the modern internet. They also have the potential to give economic and political advantage to any party that can alter them. This potential has seen the technology and standards that underpin the consumer-focused internet become a new focus for geopolitical rivalry.

Japan and the UK – both G7, G20 and OECD members – have each struggled to cope with the capricious, sometimes aggressive behaviour of their strongest ally, the US, while not being able or willing to take a hard line with respect to China on issues like 5G. As China continues to rise as a technological power, and as the risk grows that the internet's architecture fragments, it will be vital for like-minded allies such as the UK and Japan to continue to advocate the benefits to trade and social well-being of a single, open interoperable internet.

This essay builds on the discussions at Chatham House's 'Security at the Frontier' event and explores the need for closer collaboration between the UK and Japan on cyber issues, particularly in the field of technical standards, 5G and norms for responsible state behaviour in cyberspace. At stake is the need to avoid fragmentation, and to preserve the original vision of a single, open, interoperable internet in the face of authoritarian alternatives.

Background – close allies with shared values

The UK and Japan are close allies and have deeply connected military alliances and defence industry supply chains.

In October 2020, the UK and Japan signed a Comprehensive Economic Partnership Agreement (CEPA). Although CEPA represents a necessary post-Brexit replication and adaption of the EU–Japan economic partnership, its contents reflect the extension of the UK–Japan bilateral coordination on cyber that has been taking place for more than 12 years. In 2018 the total value of trade between the two countries was £29 billion. Under CEPA, trade between the two nations is projected to increase by £15.2 billion.[2]

The interconnectedness of the two nations' economies generates shared interests and challenges. For instance, the UK holds an enormous interest in the cybersecurity of big Japanese industrial companies that play an important role in the UK's critical national infrastructure including the energy, transport and financial sectors. Simultaneously, London and the UK are an important hub for Japanese businesses operating in the Europe, Middle East and Africa (EMEA) market.

With global spending on cybersecurity at $145 billion annually and predicted to grow to $1 trillion by 2035,[3] the UK and Japan have the potential to take advantage of this growth by virtue of the complementary strengths of each of their economies. For instance, Japan's highly developed manufacturing base is complemented by the UK's decades of global leadership in intelligence and signals intelligence, and its strong bases of intellectual property and talent development in advanced cybersecurity capabilities (such as artificial intelligence and machine learning), threat intelligence, and identifying insider threats.

With global spending on cybersecurity at $145 billion annually and predicted to grow to $1 trillion by 2035, the UK and Japan have the potential to take advantage of this growth by virtue of the complementary strengths of each of their economies.

These complementary strengths present opportunities for Japan and the UK to work together on joint commercial projects and towards a common vision for the internet. This is particularly important in the field of supply chain assurance in telecommunications, including in space technology, where there is a pressing need to ensure a diversity of products and services in the market, such as in the supply chain for 5G equipment.[4]

Today, both governments find themselves working to meet the connectivity, skills and research and development (R&D) needs of their increasingly technology-focused economies, while becoming uncomfortably wedged between the US and China, unable to completely meet the demands of either party and risking compromise of their own national interests. Fortunately, the two nations' deeply intertwined economic interests, their shared interest in an

[2] Department for International Trade (2021), *UK-Japan free trade agreement: the UK's strategic approach*, Policy paper, 4 January 2021, [footnote 3], https://www.gov.uk/government/publications/uks-approach-to-negotiating-a-free-trade-agreement-with-japan/uk-japan-free-trade-agreement-the-uks-strategic-approach#fn:3.
[3] World Economic Forum (2020), *Future Series: Cybersecurity, emerging technology and systemic risk*, Insight Report November 2020, Cologny/Geneva: World Economic Forum, http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf.
[4] For a recent analysis, see Department for Digital, Culture, Media & Sport (DCMS) (2020), *5G Supply Chain Diversification Strategy*, 7 December 2020, https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy.

open digital economy, and mutual security dependencies present a number of natural opportunities to collaborate. These opportunities hold the potential to help both nations to navigate an increasingly tense geopolitical dynamic as natural partners in promoting a free, open, peaceful, fair and secure cyberspace.

Shared interests, shared opportunities

Responsible state behaviour in cyberspace

The UK and Japan's shared interests have led to high-level recognition of each other as natural partners in promoting a rules-based international order in cyberspace and as each other's 'closest security partners respectively in Asia and Europe'.[5]

There is close bilateral communication between the two governments in the areas of cybersecurity and international law (as it relates to cybersecurity and stability), and the countries coordinate in multilateral forums, including the United Nations Group of Governmental Experts (UNGGE) on advancing responsible state behaviour in cyberspace and the Open-Ended Working Group (OEWG). Both Japan and the UK have historically supported the applicability of existing international law to cyberspace. Now that UN states have agreed that international law applies to cyberspace, the debate has moved to resolving the question of *how* it applies.

In recent years, discussion on the application of existing international law to cyberspace tended to focus on use of force (and armed conflict). But cyber operations rarely reach the required threshold to be considered a use of force under international law. This has re-emerged as a pressing issue in the context of the COVID-19 pandemic, which has seen a dramatic increase in the number of cyberattacks on critical national infrastructure, medical facilities and vaccine research centres.

These circumstances have brought concepts such as the relationship between sovereignty and cyberspace, legal mechanisms for attribution to states, and the applicability of due diligence obligations to cyberattacks to the top of policymakers' agendas. Japan and the UK have slightly differing interpretations on the application of international law to cyberspace, with the UK being more cautious about admitting the existence of violation of sovereignty beyond the principle of non-intervention. In general, however, the two states are well aligned on the importance of striking the right balance between freedom and regulation. Moving forward, there is an opportunity to create a closer dialogue between the UK and Japan across all stakeholder groups, including legal, technical, security and trade experts as well as civil society.

[5] Prime Minister's Office (2017), *Japan-UK Joint Declaration on Security Cooperation*, 31 August 2017, https://www.gov.uk/government/publications/japan-uk-joint-declaration-on-security-cooperation.

Norms for responsible state behaviour in cyberspace

Over the past five years, there has been intense activity by states in internet governance dialogues as well as extensive forum shopping – i.e. picking which conventions to respect – by a number of states that are developing and promoting different visions for the internet.

The UK–Japan joint declaration on security cooperation highlights cyberspace as a key area for collaboration and emphasizes the importance of common ground. The slight differences between the UK and Japan on the application of international law to cyberspace do not override the fact that these are democratic allies able to work together to promote responsible state behaviour, based on shared values and voluntary actions to foster peace and stability in cyberspace.

Data governance and the free flow of data

The UK and Japan have been working in concert for 12 years to sustain an open digital economy. Central to these efforts has been their collaboration in international forums to maintain the free flow of data. Both Japan and the UK have been working to support the global market in digital products and services by continuing the work of the G20 Osaka Track[6] in ensuring the free flow of data across international borders. The two countries also work together through the G7 to promote best practice cyber regulation, through the UNGGE to agree norms for responsible state behaviour in cyberspace, and through the Regional Forum of the Association of Southeast Asian Nations (ASEAN).

Although the 2020 CEPA bears a striking resemblance to the EU–Japan Economic Partnership Agreement, there are substantial differences between the two agreements in promoting the free flow of data. The CEPA has introduced provisions to facilitate the cross-border flow of data,[7] a prohibition on unjustified data localization requirements,[8] commitments to net neutrality,[9] and provisions for source code protections.[10] The agreement is meant to provide clear rules on the cross-border transfer of data and to grant greater protection of trade secrets related to algorithms and encryption. As trends for data sovereignty and data localization laws continue, it will be vital to maintain strong advocacy for the free flow of data across borders.

Additionally, there is close cooperation between both countries' regulatory bodies: the Bank of England works closely with the financial services payments agency of Japan on financial cybersecurity regulation. Both countries share a view on the importance of ensuring interoperability between different regulatory regimes across the world to promote low-friction trade in both products and services.

[6] European Council (2019), *G20 Osaka Leaders' Declaration,* 29 June 2019, https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.
[7] Foreign Commonwealth & Development Office (FCDO) (2020), *UK/Japan Agreement for a Comprehensive Economic Partnership*, Article 8.84, 23 October 2020, https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.
[8] FCDO (2020), *UK/Japan Agreement for a Comprehensive Economic Partnership*, Article 8.85.
[9] FCDO (2020), *UK/Japan Agreement for a Comprehensive Economic Partnership*, Article 8.78. For more on the concept of net neutrality, see Wu, T. (2003), 'Network Neutrality, Broadband Discrimination', *Journal of Telecommunications and High Technology Law*, 2: p. 141, https://scholarship.law.columbia.edu/faculty_scholarship/1281.
[10] FCDO (2020), *UK/Japan Agreement for a Comprehensive Economic Partnership*, Article 8.73.

They will also be looking to further this in relevant forums, such as in the Kyoto symposium on IoT security standards, while building on work that has been undertaken on the topic by the EU.

Huawei and 5G

For the past two years, what would previously have been a purely technical decision over procuring 5G infrastructure has been blown into a hotly contested political issue, elevated even to the level of heads of state. US concerns about the inclusion of 5G technology supplied by Huawei in critical national infrastructure, combined with a lack of choice of providers in the 5G marketplace has placed both the UK and Japan in a difficult position.

By denying Huawei access to part or the whole of a country's telecommunications infrastructure, countries are denying themselves access to functionality at a highly competitive price and putting themselves in the position of having to spend hundreds of millions of dollars to replace the legacy Huawei technology that is already in their infrastructure.[11] Neither the UK nor Japan wishes to alienate China, which could jeopardize extensive business relationships and inward investment. Yet each country must balance short-term and long-term security interests with their ongoing need for cost-effective industrial development.

When the controversy over 5G started to emerge in late 2018, both the UK and Japan were unable to commit themselves to an immediate outright ban, given the existing Huawei technology in their legacy systems (2G, 3G and 4G, on which the 5G infrastructure depends).

Opportunities for closer collaboration

Diversification of 5G equipment

The market for 5G equipment has three competitors currently with the proven capacity and capability to build out an entire country's network. The UK's ban on Huawei has reduced the market to two competitors, Nokia and Ericsson, and thus introduces a different kind of cybersecurity risk in the event that one of those suppliers fails.

The complementary industrial bases of the UK and Japan present a unique opportunity to collaborate to encourage diversification in the 5G supply chain – as demonstrated by the UK's recent trial with the Japanese supplier NEC to test their equipment in the UK market. The UK government has also brought forward publication of a diversification strategy for the 5G supply

[11] DCMS (2020), *The Telecommunications Security Bill 2020: National security powers in relation to high risk vendors*, 21 May 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/938036/The_Telecommunications_Security_Bill_2020___National_security_powers_in_relation_to_high_risk_vendors_-_FINAL_upload.pdf.

chain.[12] However, it is recognized that the market has significant barriers to entry and that existing customers (mobile operators) are understandably risk-averse in their purchasing behaviour.[13]

While there is the potential to reduce vendor lock-in through the adoption of interoperable components using Open RAN,[14] recent evidence indicates that Open RAN, although exciting, is not yet ready to build out at sufficient scale to be a viable alternative to Nokia and Ericsson and that 'there is more promise potentially from the vendors that are somewhat established, the Samsungs and the NECs'.[15]

Increasing divergence in technical approaches to internet governance in international forums is forcing many nation states to re-examine previous assumptions that the internet's basic infrastructure will remain the same.

A further opportunity to make an impact could arise from leveraging UK–Japan cooperation in the financial sector, to ensure that promising start-ups have access to finance and to minimize the risk of early buy-out by potentially hostile states.

Technical standards in the UN and the risk of fragmentation

At the announcement of the Osaka track of the G20 in 2019, the then director-general of the World Trade Organization (WTO), Roberto Azevêdo, stated, 'A fragmentation would hurt us all'.

Increasing divergence in technical approaches to internet governance in international forums is forcing many nation states to re-examine previous assumptions that the internet's basic infrastructure will remain the same. To date, the internet's architecture has served its global community of users well. Even during the pandemic, when traffic is estimated to have gone up by 30 to 50 per cent,[16] the internet has remained stable and resilient, supporting mass uptake, bandwidth-hungry video-conferencing and streaming applications.

Given the UK and Japan's shared interests in supporting the continuing free flow of data, there are growing concerns over China's proposals, made within the International Telecommunication Union (ITU), to standardize alternative architectures for the

[12] DCMS (2020), *5G Supply Chain Diversification Strategy*, 7 December 2020, https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy.
[13] Ibid.
[14] Open RAN is a collection of technologies that enable mobile network operators to use equipment from multiple vendors and still ensure interoperability.
[15] Evidence of Professor William Webb to the Public Bills Committee hearing on Telecoms (Security) Bill: Parliamentlive (2021), 'Telecommunications (Security) Bill Committee' (at 10:03), 19 January 2021, https://parliamentlive.tv/Event/Index/992328cd-1972-42e5-b6e9-b0b46aeaaf9c.
[16] Beech, M. (2020), 'COVID-19 Pushes Up Internet Use 70% And Streaming More Than 12%, First Figures Reveal', 25 March 2020, forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/?sh=6222e7c43104.

internet.[17] If adopted, the proposals would create a new vision and architecture for the internet and would replace the lightweight, interoperable protocols that hold the internet together and make it work.

The choice of forum is significant, as the ITU standards enjoy protections under WTO rules, in that equipment bearing those standards cannot be barred in international trade. So, there could be no repeat of the trade bans implemented against Huawei by several countries over the past five years.

Many commentators are sceptical that China's vision for a new internet would ever be successful, or that its proposals answer a real technical need. However, it is foreseeable that there could be an appetite for a different kind of internet from some countries, one that is optimized for the surveillance of its users. China's existing trade relationships through the Belt and Road Initiative, combined with its generosity towards developing countries in terms of providing technical infrastructure and equipment, could assist in creating a *de facto* 'splinternet'.

It is important for like-minded states with advanced technology capabilities – such as the UK and Japan – to work cooperatively to reduce geopolitical tensions and to promote shared values and the benefits of a single, interoperable internet based on openness and democratic values. Closer coordination on shaping the agendas of international institutions and encouragement of their respective private-sector technological innovators to participate more actively in standards bodies could help to achieve these goals.

Challenges – language and cyber preparedness

While there is an urgent need to strengthen UK–Japan collaboration, and further opportunities for closer cooperation to address pressing issues, there are also challenges.

Language remains a barrier in UK–Japan relations and may limit access to technologies even for prosperous and sophisticated users. While the internet has collapsed distance and enabled the free flow of data across borders, the web and domain name systems continue to favour the English language and Latin scripts.

For example, Japan has roughly twice the population of the UK, a GDP of $5 trillion compared to the UK's $2.8 trillion, and similar rates of GDP per capita (~$40,000).[18] Yet, while the .uk domain registry has more than 10 million registrations,[19] Japan's .jp recently announced that it had reached 1.6 million,[20] a long way short of the top 10 country code top-level domains.[21] Cooperation between engineers in Japan, China and South Korea in the early 2000s resulted in technical standards to support their shared character sets. Yet, so-called 'internationalized' domain names are still poorly

[17] See Hoffmann, S., Lazanski, D. and Taylor, E. (2020), 'Standardising the splinternet: how China's technical standards could fragment the internet', *Journal of Cyber Policy*, 5(2): pp. 239–264, doi: 10.1080/23738871.2020.1805482.
[18] The World Bank (n.d.), 'Data for Japan, United Kingdom', https://data.worldbank.org/?locations=JP-GB (accessed 24 Jan. 2021).
[19] Nominet (2020), '.UK Register Statistics – 2020', https://www.nominet.uk/news/reports-statistics/uk-register-statistics-2020 (accessed 24 Jan. 2021).
[20] JPRS (2020), 'JPドメイン名の登録数が160万件を突破', ('The number of registered JP domain names has exceeded 1.6 million'), press release, 2 October 2020, https://jprs.co.jp/press/2020/201002.html.
[21] Verisign (2020), *The Domain Name Industry Brief*, 17(4): p. 3, November 2020, https://www.verisign.com/assets/domain-name-report-Q32020_en_GB.pdf.

supported and do not work well in key applications like email, as unique identifiers for customer accounts in social media or even in some web browsers,[22] inhibiting their uptake. English is the language of 60 per cent of web content, a proportion that has been growing year-on-year. Japanese represents just 2 per cent of web content.[23]

In the cybersecurity field, the language issue has accentuated an existing divide. The UK, sharing a common language with the US, has been subjected to large-scale cyberattacks both from states and non-state actors for many years. As a result, the UK has developed significant capabilities in the cybersecurity industry as well as in its signals intelligence agency GCHQ and its public-facing National Cyber Security Centre. Meanwhile, Japan has been relatively shielded to date, perhaps due to its language. This has translated into a comparatively low level of cyber resilience and preparedness in comparison with international partners.[24] As a result of its experience, the UK government and its agencies are in a unique position to work with the Japanese government and private sector to enhance existing capacities and share cybersecurity best practices. Furthermore, the UK's universities and commercial cybersecurity sector is well placed to work with Japanese multinationals to improve their cyber resilience. This work may be especially useful if the Tokyo Olympics go ahead in 2021, as they are likely to attract significant cyber activity by hostile parties,[25] as previous events have experienced.[26]

Conclusions

The UK–Japan relationship on cybersecurity highlights shared values, mutual respect and goodwill, and an appetite to do business together. At the same time, there exists a sense of unfulfilled potential, perhaps because of language barriers, physical distance and limitations in the abilities to understand one another fully.

This essay has briefly summarized the areas where the two states could harness untapped potential for closer cooperation in matters of cybersecurity: diversification of the 5G equipment market; coordination over technical standards to maintain the free flow of data across borders and avoid fragmentation; and in developing norms for responsible state behaviour in cyberspace.

As we stand on the threshold of a new decade that is likely to see the dominance of an authoritarian technological superpower, it will be all the more important for states such as Japan and the UK, with similar values on communication, to find and extend common ground. Together, the two states can advocate for a positive vision of a single, global, interoperable internet, which improves language diversity, and removes barriers to the free flow of data across borders.

[22] IDN World Report (2020), 'Making all domain names work in all applications', https://idnworldreport.eu/universal-acceptance.
[23] W3Techs (n.d.), 'Usage statistics of content languages for websites', https://w3techs.com/technologies/overview/content_language (accessed 24 Jan. 2021).
[24] Tsukimori, O. (2020), 'As cyber attacks rise globally, Japan's digital security found lacking', *Japan Times*, 18 September 2020, https://www.japantimes.co.jp/news/2020/09/18/business/japans-cybersecurity-lacking.
[25] Cimpanu, C. (2020), 'UK says Russia was preparing cyber-attacks against the Tokyo Olympics', ZDNet, 19 October 2020, https://www.zdnet.com/article/uk-says-russia-was-preparing-cyber-attacks-against-the-tokyo-olympics.
[26] Greenberg, A. (2019), 'The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History', Wired, 17 October 2019 https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack.

Outer space: UK–Japan responses

By Alexandra Stickings
Research Fellow for Space Policy and Security, Royal United Services Institute

The security situation in outer space is under unprecedented scrutiny. The establishment of the United States Space Force in December 2019,[27] anti-satellite missile tests by China[28] and India,[29] and Russian activity involving co-orbital satellites[30] have made international headlines and prompted strong international responses. They have also increased rhetoric on the further militarization and possible weaponization of space, and raised concerns regarding an arms race in outer space.[31] Understanding these developments is essential for states and commercial space actors to continue to operate in orbit and work towards the long-term sustainability of this environment.

Space is an area of strategic competition. It is important for military and national security activities, through the provision of long-range, secure communication; intelligence, surveillance and reconnaissance (ISR) data; and position, navigation and timing (PNT) capabilities. Space capabilities also provide data for many aspects of daily life, including for finance, transportation and entertainment sectors. As such, space industry and space exploration activities have huge economic benefits for a range of industries in the form of communications, Earth observation and PNT signals. Recognition of these benefits has led to more satellites in orbit to meet an increased demand and further analysis of how space is understood in terms of military purposes.

[27] United States Space Force (n.d.), 'About the United States Space Force', https://www.spaceforce.mil/About-Us/About-Space-Force.
[28] Secure World Foundation (2010), *2007 Chinese Anti-Satellite Test Fact Sheet*, 23 November 2010, https://swfound.org/media/9550/chinese_asat_fact_sheet_updated_2012.pdf.
[29] Weeden, B. and Samson, V. (2019), 'Op-ed: India's ASAT test is a wake-up call for norms of behaviour in space', *SpaceNews*, 8 April 2019, https://spacenews.com/op-ed-indias-asat-test-is-wake-up-call-for-norms-of-behavior-in-space.
[30] BBC News (2020), 'UK and US say Russia fired a satellite weapon in space', 23 July 2020, https://www.bbc.co.uk/news/world-europe-53518238.
[31] Silverstein, B., Porras, D. and Borrie, J. (2020), *Alternative Approaches and Indicators for the Prevention of an Arms Race in Outer Space*, UNIDIR, Space Dossier 5, May 2020, https://unidir.org/publication/alternative-approaches-and-indicators-prevention-arms-race-outer-space.

There are, however, certain challenges that space actors face. The first of these is counterspace capabilities, which range from kinetic anti-satellite missiles that can destroy a satellite, to non-kinetic measures such as cyberattacks or jamming.[32] Such capabilities pose proliferation concerns as more countries are interested in acquiring them, putting space assets at risk and increasing concern of a future conflict in space.

The second challenge relates to the substantial increase in space actors since the beginning of the 21st century, and the resulting expansion in both the number of active satellites and pieces of space debris. As more states have become involved, there has been a huge expansion in commercial space activities. This has added an extra dimension to how all actors need to approach their operations in space.

Spacefaring states, particularly those with existing military space programmes, have reorganized the ways in which they operate, raising concerns among those advocating peaceful space activities that it is becoming increasingly militarized.

These challenges have been met with a range of responses from the international community. Spacefaring states, particularly those with existing military space programmes, have reorganized the ways in which they operate, raising concerns among those advocating peaceful space activities that it is becoming increasingly militarized. Newcomers to space often enter the sector through partnerships, recognizing the need to engage in activity in this environment. The last group are those who do not actively participate in orbital missions but recognize the reliance they have on space assets and the need to preserve the environment. It is necessary to understand the different perspectives with which various actors approach these challenges in order to find solutions.

Internationally, focus on arms control in space has increased, as have discussions regarding norms of behaviour and what it means to be a responsible space actor. As with all multilateral discussions, politics and existing rivalries affect the speed and effectiveness of such debates, as do the intentions of individual states and the ways in which they conceptualize the problems.

An argument can be made that it is incorrect and possibly even harmful to apply the term ‘arms race’ to the current situation in space (or, indeed, the term ‘space race’) – for example, as discussed in the United Nations Conference

[32] For an overview of each state’s capabilities, see Weeden B. and Samson, V. (eds) (2020), *Global Counterspace Capabilities: An Open Source Assessment*, Colorado and Washington: Secure World Foundation, https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf.

on Disarmament's Treaty on Preventing an Arms Race in Outer Space (PAROS).[33] Yet to understand these and other ongoing negotiations,[34] an approach that accepts the arms race narrative must be taken.

Within this narrative, an arms race is happening across multiple domains, and space capabilities are a part of this. Approaching it from this perspective also negates any idea of a 'space race' that is occurring independently of terrestrial developments. The role of space within this broader arms race has two characteristics. The first is the ways in which space assets support other systems, such as nuclear command and control and missile early warning systems, and so cannot be separated from developments in these areas. The second is the recognition that satellites can potentially be the weak points in these systems and can therefore be targeted through physical or cyber means, as well as the fact that satellites provide a great deal of support for military operations. As a result, a number of states have developed a range of counterspace capabilities.[35]

An arms race, by this definition, occurs within the strategic context and involves gaining an edge over an adversary in terms of qualitative or quantitative improvement of weapons. A 2020 report from the United Nations Institute for Disarmament Research (UNIDIR)[36] highlighted three indicators of an arms race dynamic: rivalries, corollary developments and acceleration of development, all of which can be seen to be applicable to the context of space. There has therefore recently been a renewed sense of urgency to address the potential for conflict in space.

In 2008, Russia and China introduced the Prevention of the Placement of Weapons in Orbit (PPWT) treaty,[37] although this has seen resistance from the West. Much of this resistance has arisen from the difficulty of defining a weapon in space, the multi-use and dual-use nature of many space capabilities and the difficulties of knowing what objects are capable of until they are used. Russia and China have also been called out for hypocrisy in promoting arms control treaties while at the same time developing advanced counterspace capabilities and, despite their push for the PPWT, neither has endorsed a recent British initiative regarding norms of behaviour. At present, PPWT discussions have stalled and show no signs of progressing.

Other initiatives include an EU Code of Conduct,[38] which has similarly been met with political blocks, but did reach some agreement that norms can help to preserve stability. The Group of Government Experts (GGE), the Conference on Disarmament and the Disarmament Commission have all failed to make significant progress in terms of reaching agreements on concrete measures that can be taken to improve security in outer space.

[33] Stickings, A. (2020), 'Are We In A Space Race?', *NITECH*, 11 December 2020, https://www.ncia.nato.int/nitech-magazine/new-edition-of-nitech-magazine-highlights-securing-the-space-domain.html.
[34] Such as the PAROS-associated Prevention of the Placement of Weapons in Orbit (PPWT) treaty and the UK-led discussions through the United Nations First Committee, discussed below.
[35] The term 'counterspace capabilities' is used in preference to 'space weapon'. Not all technologies are easily classified as a weapon, and not all act in space. For example, some will target ground control systems or ground-based receivers.
[36] Silverstein, Porras and Borrie, (2020), *Alternative Approaches and Indicators for the Prevention of an Arms Race in Outer Space*.
[37] Listner, M. and Rajagopalan, R. P. (2014), 'The 2014 PPWT: a new draft but with the same and different problems', *The Space Review*, 11 August 2014, https://www.thespacereview.com/article/2575/1.
[38] Johnson, C. (2014), *Draft International Code of Conduct for Outer Space Activities Fact Sheet*, Secure World Foundation, https://swfound.org/media/166384/swf_draft_international_code_of_conduct_for_outer_space_activities_fact_sheet_february_2014.pdf.

The most recent discussions, centred on a UK proposal to the United Nations General Assembly,[39] focus on the pursuit of norms of behaviour. They are intended to kick-start discussions on rules of engagement for capabilities such as rendezvous and proximity operations (RPO) and kinetic anti-satellite (ASAT) missiles. The potential success of this initiative, which emphasizes behaviour instead of capabilities, and which has received broad support internationally despite opposition from Russia and China, will provide evidence as to the likelihood of concrete future agreements among space actors being reached.

Within this complex environment, there are questions for how actors respond. This is particularly relevant for medium-sized space powers as they juggle their own ambitions with those of their partnerships and alliances, and as they cement their identities as space actors. The UK and Japan are two such states, and from the perspective of the UK, it is interesting to consider how Japan can be a useful ally in the future.

The UK context – what next for a medium space power?

While the UK was a relatively early entrant in space activity, with the launch of a satellite in 1971, it has somewhat lost its way since. Despite continuing, if at times minimal, activity, it has struggled to find its identity as a space actor. Various strategies and policies have been announced, particularly since the formation of the UK Space Agency in 2010. However, these have lacked cohesion and leadership, and as such the position of the UK as a space power has remained static. This is not to say that important work has not taken place. The role of UK industry in pioneering small satellites, which have had a large effect on the space environment, cannot be denied. Rather, space has not always been seen as a priority in the UK.

Recent events over the past few years, however, show that this is changing. Space is now a central policy area, and the UK is not alone in this regard. In the vast majority of states, the importance of space is being reflected in policy changes.

The UK has undertaken a number of steps to centralize its space governance. In April 2020, the Ministry of Defence appointed Air Vice-Marshal Harvey Smyth as its first director space,[40] a two-star position that has already provided leadership and cohesion of military space, bringing often disparate activities under one roof. Following its inclusion in the government's 2020 manifesto, it was announced that the UK would include an RAF Space Command within its defence strategy.[41] While this has raised some questions as to its purpose and role, not least due to the current small number of sovereign military satellites, it has also caused concern

[39] Rajagopalan, R. P. (2020), 'Assessing the British Proposal on Space Security', Observer Research Foundation, 11 December 2020, https://www.orfonline.org/research/assessing-the-british-proposal-on-space-security.
[40] Chuter, A. (2020), 'Former fighter pilot picked to lead British military's space command', *Defense News*, 15 January 2020, https://www.defensenews.com/global/europe/2020/01/15/former-fighter-pilot-picked-to-lead-british-militarys-space-command.
[41] ITV News (2020), 'UK to set up "RAF Space Command capable of launching first rocket"', 19 November 2020, https://www.itv.com/news/2020-11-19/pm-vows-to-end-era-of-retreat-with-biggest-military-investment-since-cold-war.

internationally that the UK is intending to raise its status as a military space power, perhaps even to the extent of developing its own counterspace capabilities. Currently available information suggests that the Space Command's primary remit will be to allow the UK to act more effectively in other areas of defence and with international partners. Transparency in this area is necessary to ensure that the rest of government and the international community fully understand the purpose of the Space Command and therefore the way that the UK perceives itself as a military space power. Nevertheless, the existence of the Space Command does highlight that the UK intends for the Ministry of Defence to play a larger role within military alliances when it comes to space, as well as to work more closely with domestic partners to assure and protect the UK's space assets.

Within the broader UK context, a new National Space Council became a Cabinet Committee in June 2020,[42] again with the intention of improving coherence across a wide variety of activities in various government departments and agencies. The Council ensures that those areas of government that do not have a central role in space activities, but that rely on the information that space provides, have a voice and are involved in discussions on future capabilities, how to protect existing assets and on ensuring continued access to orbit.

The central work of the UK is its leadership of multilateral discussions within the UN through its proposal on norms of responsible behaviour, pushing forward essential conversations regarding the long-term sustainability of orbit.

Within the foreign policy realm, the central work of the UK is its leadership of multilateral discussions within the UN through its proposal on norms of responsible behaviour, pushing forward essential conversations regarding the long-term sustainability of orbit. The UK will continue to take part in the other ongoing discussions, such as those within the Conference on Disarmament and the UN Office of Outer Space Affairs (UNOOSA). However, there are other ways in which space plays a role in foreign policy. Initiatives within the UK Space Agency work internationally to support programmes concerned with development, climate change and security. Multinational scientific and exploration missions are important for maintaining and increasing international relationships. It is possible that, for a medium space power that lacks the ability and resources to match the number of satellites and launch capability of the larger powers, more focus will be given to these diplomatic and soft-power activities as a way to increase the UK's international standing as a space power.

While there has been momentum towards this new reality over the last few years, it should be noted that much of what has taken place is related to the way in which the current government has approached space. There is full recognition of the

[42] UKspace (2020), 'UKspace welcomes addition of National Space Council to Cabinet Committees', 29 June 2020, https://www.ukspace.org/ukspace-welcomes-addition-of-national-space-council-to-cabinet-committees.

importance that space plays and its priority role in the economy, the indigenous industry and national security. The government also recognizes the threats that are faced, such as space debris and the counterspace capabilities of adversaries. The 2021 UK Integrated Review, which looked into all aspects of defence, national security and foreign policy, reflects how space plays a role across all of these elements. In short, space is no longer seen as something separate, understood and engaged in by a relatively small number of technical experts. Space is a cross-cutting enabler, without which the mechanisms of defence and national security cannot operate.

However, questions remain. While recent events and activities have seen the UK set the scene and lay down markers to play a bigger role internationally, this is only the start. Where does the UK go now? What capabilities does it want to develop, both military and civilian, and how can it improve governance to bring different areas closer together? Thought must also be given to how the UK can build on its existing international partnerships and alliances. On the military side, the UK needs to look at its role within NATO and the Five Eyes intelligence-sharing network, and how it might fill capability gaps to increase its standing, as well as explore further alliances with states that face similar threats. On the civilian side, the UK will need to balance its role and commitments as a member of the European Space Agency (ESA) with other existing and future international partnerships, particularly as the implications of Brexit and the role of EU funding to the ESA are realized.

The Japan context

As with the UK, Japan was an early entrant into space activity, with the launch of its first satellite in 1970, but similarly it did not make significant progress until more recently. Since the formation of the Japan Aerospace Exploration Agency (JAXA) in 2003,[43] it has become one of the leaders in space exploration. Recent successful missions, including its Hayabusa2 asteroid sample-return mission, have shown Japan to be at the forefront of technology in this area. The establishment of JAXA was followed by the adoption in 2008 of the Basic Space Law, leading to the formation of the Strategic Headquarters for National Space Policy. The law outlined Japan's approach to space development and use, 'contributing to the improvement of the lives of the citizenry and the development of the economy and society as well as contributing to the improvement of international peace and the welfare of humankind'.[44] This law has also outlined priorities including disaster management, space exploration and innovation, as well as Japan's commitment to undertake space activities in accordance with international agreements and to work towards the preservation of the space environment.

The evidence therefore supports the notion that Japan's space policies and activities were geared towards non-military use and the avoidance of conflict in space. However, the 2008 law does note 'national security ramifications', albeit

[43] Howell, E. (2016), 'JAXA: Japan's Aerospace Exploration Agency', *Space.com*, 19 May 2016, https://www.space.com/22672-japan-aerospace-exploration-agency.html.
[44] JAXA (2008), 'Basic Space Law (Law No.43 of 2008)', 21 May 2008, https://stage.tksc.jaxa.jp/spacelaw/country/japan/27A-1.E.pdf.

'based on the pacifism of the Constitution of Japan', and, in 2012, JAXA's remit was expanded to include military space development. Space was included as a priority area for advancing defence capabilities in the 2018 National Defense Program Guidelines, and this was followed in May 2020 with the launch of the Space Operations Squadron, part of the Japan Air Self-Defense Force.[45]

The new squadron is intended to provide protection for Japanese satellites from attack and to monitor the environment, as well as to provide support for other areas of defence. It is apparent that some of the impetus for its creation is the perceived threat from Russian and Chinese developments in counterspace capabilities as well as concerns over a nascent North Korean space programme. Japan is in this sense responding to changes in the security environment rather than actively looking to engage in space-based military activity, such as through the development of offensive capabilities. It is likely that unless a Japanese satellite is attacked, and such an attack can be proven, this approach to space will remain the status quo.

Japan has also been active in multilateral discussions regarding the space environment. For example, in February 2020, the government of Japan put out a joint statement with the United Nations Office for Outer Space Affairs (UNOOSA) on space debris, outlining its intention to take on a leadership role in tackling the problem.[46] Working through multilateral institutions is a way for Japan to respond to the identified threats – both to its own space assets and to the space environment as a whole – without compromising the limitations that it may set itself in military activity.

Although there are obvious differences between the two, there are similarities between the UK and Japan in terms of their space programmes that suggest they have much to gain by working together. Primarily, both are states that have until recently had minimal activity within the realm of military space, focusing instead on civil and commercial opportunities, and are now expanding in this area. Both appear reluctant to travel too far down this path through the creation of offensive counterspace capabilities, relying instead on the international community as a route to security, safety and sustainability of orbit.

Areas for cooperation

It is clear that in order to confront the myriad challenges in space, international cooperation is key. As two medium-sized space powers with similar outlooks, the UK and Japan are well placed to work together in a number of areas, either bilaterally or with other like-minded states. Doing so would not only increase the security of each but would also build upon a growing coalition of space actors working towards the long-term sustainability of this environment.

[45] Yamaguchi, M. (2020), 'Japan launches new unit to boost defense in space', *Defense News*, 18 May 2020, https://www.defensenews.com/global/asia-pacific/2020/05/18/japan-launches-new-unit-to-boost-defense-in-space.

[46] Ministry of Foreign Affairs of Japan (2020), 'Joint Statement on Space Debris by the Government of Japan and the United Nations Office for Outer Space Affairs (UNOOSA)', 7 February 2020, https://www.mofa.go.jp/press/release/press4e_002773.html.

As mentioned earlier, the first area for cooperation is in multilateral discussions taking place through UN mechanisms. Although the UK has led on the most recent agreements on the need for norms of behaviour, continued support from Japan is essential for ensuring momentum is not lost. Well-respected space actors such as Japan can also assist with reaching out to states that may be more sceptical of such measures. Cooperation in this area is perhaps the way in which states such as the UK and Japan, while limiting their own military space capabilities, can best respond to the proliferation of counterspace capabilities and the direct threats to their own space assets.

The second area for cooperation is in the area of space situational awareness (SSA) or space domain awareness (SDA). These activities, which involve monitoring and understanding the space environment, such as through tracking space debris and warning of potential satellite conjunctions, have traditionally been carried out by militaries. But in recent years there has been a shift to civil and even commercial entities, thereby removing barriers to information-sharing that is needed to gain as full a picture as possible of orbit. State support for commercial SSA data providers through bilateral and multilateral agreements on information-sharing and data interoperability could help in building up this picture.

And finally, there are many opportunities for collaboration in the areas of science and exploration. As already mentioned, Japan is well established in the field of space exploration, and future missions could benefit from incorporating British expertise, such as the technology required for close approach and rendezvous[47] and the recent initiative to explore the uses of nuclear energy for space exploration.[48] From the UK perspective, not only can Japan provide experience but it also offers an additional partnership option should the UK wish to look beyond its work with the ESA. There are also a number of ways in which the two states could collaborate closer to home, such as through scientific space programmes in the fields of climate research and monitoring solar weather. Leading on and partnering in multinational missions can provide impetus for working towards a space environment that remains peaceful, and can also provide opportunities for states without the means to access space independently to play more of a role.

For space to remain secure, safe and sustainable, leadership from a small number of actors can go a long way. The UK and Japan are medium-sized space powers that have shown an unwillingness to go too far down the route of militarizing space. Yet, both have the stature and readiness to bridge gaps between the larger space powers that exist because of sensitivity and ongoing rivalries.

[47] University of Surrey (n.d.), 'RemoveDEBRIS: Mission Overview', https://www.surrey.ac.uk/surrey-space-centre/missions/removedebris.
[48] Rolls Royce (2021), 'Press release: Rolls-Royce & UK Space Agency launches first study into nuclear power for space exploration', 12 January 2021, https://www.rolls-royce.com/media/press-releases/2021/12-01-2021-rr-uk-space-agency-launches-first-study-into-nuclear-power.aspx.

UK–Japan responses in the Arctic

By Aki Tonami
Associate Professor of International Relations and Economics,
University of Tsukuba

Looking from Japan, it is never straightforward to understand the issue of Arctic security. To begin with, it appears that the definition of the Arctic region is not unanimously agreed. The most common definition is that the Arctic is the region above the Arctic Circle, an imaginary line around 60°N latitude. Other definitions, which are mostly based on natural sciences, describe the Arctic as the area north of the arctic tree line, or are based on temperature. In politics, however, the Arctic has been consistently contested, depending on the context and constellation of 'who' is talking about the region.[49] For example, Iceland is one of the eight Arctic states of the Arctic Council, which is the most influential intergovernmental forum on the area, even though its coastline is below the Arctic Circle.

Therefore when discussing the Arctic and its security from the outside, it appears crucial that we pay attention to political actors and how they define this region, to what they view as 'security problems', and to what they attempt to project when defining the region and its security. To explain Arctic international relations and its history of mostly peaceful cooperation, Elana Wilson Rowe listed actor groups in the Arctic region from a historical perspective – namely, indigenous peoples and their organizations, commercial actors, states and their representatives, scientists, and NGOs and their representatives.[50] Note that those actor groups began with the actual people living in the Arctic, not states. This element – that Arctic cooperation and contestation have to be viewed from the perspective of the people actually living and working in the region – is something that makes the Arctic distinct from Antarctica, as well as from other 'frontiers' discussed in this conference on 'Security at the Frontier', such as cyberspace, outer space and electronic warfare.

Since the first explorers reached the North Pole at the beginning of the 20th century, the Arctic has remained a peripheral region especially for people who live outside it. Partly because it is covered by thick ice, the Arctic has often been described

[49] Rowe, E. W. (2018), *Arctic Governance: Power in Cross-Border Cooperation*, Manchester: Manchester University Press, p. 6.
[50] Ibid. pp. 18–33.

(or imagined) as a pristine, white northern hinterland disconnected from any human activities or civilization.[51] During the Second World War, the strategic value of the region rapidly increased as a result of critical naval convoys and the importance of outposts for weather prediction. At the dawn of the Cold War, the Arctic became an even more strategically crucial region, both beneath and above the Arctic Ocean. As the Cold War ended, views on the Arctic shifted to more comprehensive security issues, such as the effects of global warming and climate change. Due to climate change, the Arctic has become ice-free for longer periods and over a greater area with each passing year.

Seemingly negative changes to the Arctic have revealed the new possibilities in the region, such as oil drilling, natural gas and precious metals that used to be covered in ice, or for developing shipping routes such as the Northern Sea Route and the Northeast Passage.

Simultaneously, these seemingly negative changes to the Arctic have revealed new possibilities in the region, such as oil drilling, natural gas and precious metals that used to be covered in ice, or for developing shipping routes such as the Northern Sea Route (NSR) and the Northeast Passage. The Arctic and its complex governance system, based on the Arctic Council and non-legally binding soft laws in the post-Cold War period, have been contested. Nonetheless, working relationships between various Arctic actor groups have been largely cooperative. The most recent developments of contestation, however, are the (perceived) rise of the great power competition between the US, Russia and China in the Arctic. Prompted by this perceived competition, the US increased its engagement in Greenland, for example, by reopening its consulate there after 67 years. With these recent developments in mind, as well as ‘who’ is talking about the Arctic and its security, what are the UK and Japan’s ambitions in the region, and what opportunities are there for strengthening and developing the rules-based order in the Arctic?

Finding a role in Arctic affairs

In answering this question, a unique feature of the Arctic that must be considered is that it is physically surrounded by European and North American coastal states, each with competing governance claims. Those states have been at the centre of global economic and political gravity for much of the 19th and 20th centuries. Given this, it is worth noting that Japan has been one of only a few non-Western, geographically distant states to engage in the polar regions since 1911. In fact,

[51] Tonami, A. (2016), *Asian Foreign Policy in a Changing Arctic: The Diplomacy of Economy and Science at New Frontiers*, London: Palgrave Macmillan, p. 2.

there are only 16 states in the world that place priority on both the Arctic and the Antarctic, based on their status as both signatories of the Antarctic Treaty and members/observers of the Arctic Council.[52] The UK and Japan are two of those 16 states. In this regard, the UK and Japan's ambitions in the region should always be interpreted as an attempt to show 'legitimate great power' status through membership of international institutions.[53] Arguably, the symbolic importance of the Arctic for the UK and Japan allows both countries to be flexible in their engagement but at the same time non-committal regarding the interests of the people who actually live and work in the region.

Those who govern the Arctic have not been entirely welcoming to non-coastal states like the UK or Japan. For instance, there have always been calls for the creation of a new international regime for the Arctic, such as a legally binding Arctic Treaty. In 2008, however, in the Illulissat Declaration, the Arctic coastal states formally rejected any need to develop a new comprehensive international legal regime to govern the Arctic Ocean. They acknowledged that the existing legal framework created around the United Nations Convention on the Law of the Sea (UNCLOS) is sufficient and the Arctic legal order should remain more flexible than rigid, based on soft law instruments and non-binding cooperative frameworks. This limits the participation of the UK and Japan or other non-Arctic actors in the decision-making process, since they are – legally speaking – 'outsiders'. It can, however, allow the UK and Japan to play a role in developing norms in or about the Arctic. For example, by lobbying an Arctic state or a Permanent Participant of the Arctic Council, both the UK and Japan are able to propose projects that advance or reinforce their views on specific issues. This role is not insignificant, but different from the role that the UK and Japan expect of themselves as 'legitimate great powers' in other settings.

Within those confines, the UK and Japan have crafted their own official Arctic policies and acted upon them. In the UK's 2018 Arctic policy[54] – the country's second Arctic policy paper – the UK government proposed that the vision of 'Global Britain' would be materialized in the Arctic to advance Arctic prosperity and security. Another dimension is the Scottish Arctic policy: Scotland published its own Arctic policy, Arctic Connections, in 2019.[55] Japan adopted its first official Arctic policy in 2015.[56] It lists research and development, international cooperation and sustainable use (of natural resources) as specific initiatives. For the fiscal year 2020, the Japanese government allocated ¥1.3 billion (approximately $13 million) to matters related to the Arctic. Much of it was spent on research and development, including the launch of the ArCS II (the Arctic Challenge for Sustainability II) Project[57] (¥953 million, or $9.2 million), which most Arctic-focused

[52] Tonami, A. (2017), 'Influencing the Imagined "Polar Regions": The Politics of Japan's Arctic and Antarctic Policies', *Polar Record,* 53(5): pp. 489–97.
[53] Suzuki, S. (2008), 'Seeking "Legitimate" Great Power Status in Post-Cold War International Society: China's and Japan's Participation in UNPKO', *International Relations*, 22: pp. 45–63.
[54] HM Government (2018), *Beyond the Ice: UK policy towards the Arctic*, London: Polar Regions Department, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/697251/beyond-the-ice-uk-policy-towards-the-arctic.pdf.
[55] Scottish Government (2019), *Arctic Connections: Scotland's Arctic Policy Framework*, Edinburgh: The Scottish Government, https://www.gov.scot/publications/arctic-connections-scotlands-arctic-policy-framework/pages/8.
[56] Cabinet Office, Government of Japan (2015), *Japan's Arctic Policy (provisional translation)*, 16 October 2015, https://www8.cao.go.jp/ocean/english/arctic/pdf/japans_ap_e.pdf.
[57] Arctic Challenge for Sustainability II (n.d.), 'ArCSII', https://www.nipr.ac.jp/arcs2/e.

researchers based in Japan participate in. To advance international cooperation, Japan signed the 'Agreement to Prevent Unregulated High Seas Fisheries in the Central Arctic Ocean' (CAO Fishing Agreement) in 2018.[58] On sustainable use, Mitsui, one of Japan's largest general trading companies, took a 10 per cent stake in Russia's Novatek Arctic liquefied natural gas (LNG) project.[59] This was supported by JOGMEC, a Japanese semi-governmental organization. The ice-breaking LNG vessel 'Vladimir Rusanov' operated by the Mitsui O.S.K. Lines arrived in the Tokyo Bay LNG Terminal in the summer of 2020, after departing from Russia's Yamal LNG station.[60] It was the first time an ice-breaking LNG tanker had arrived in Japan. At the time of writing, there is also talk of the 'Arctic Connect' project, which is a submarine communication cable project led by Finland to connect Europe and Asia.[61] The cable is supposed to run along the NSR. Keen to become a port of discharge is Hokkaido, Japan's most northern prefecture, where they claim that their cool climate is suitable for data centres; they already have broad experience of hosting data centres there.

Developing rules for the Arctic

The CAO Fishing Agreement is an interesting example of new rules being developed or due to be developed with regard to the Arctic.[62] It was signed by the Arctic states (Canada, Iceland, the US, Norway, Denmark (Greenland and the Faroe Islands) and Russia) and by non-coastal states and bodies (Japan, China, South Korea and the European Union). The inclusion of non-coastal states like Japan was legitimized as the US created a new categorization, 'major fishing nations'. This is a clear example of the fact, as critiqued in the conference's session, that the term 'the rules-based international order' is not a neutral term. When we talk about 'rules-based', it precisely depends on 'who' is talking about the rules and 'who' the listener is. With the CAO Fishing Agreement, the aforementioned limitations of being a non-Arctic state were no longer relevant for the UK (formerly as an EU member state) and Japan. What mattered was whether they were invited to the table to develop the rules.

One area where the UK and Japan can collaborate is on human rights. The Arctic Council places importance on human rights, especially those of indigenous peoples. The UK and Japan have claimed to be leaders in respecting the rights of indigenous peoples as well. The Scottish Arctic policy devotes an entire page to promoting and protecting indigenous languages, especially noting experiences from the promotion of Scottish and Gaelic languages. Within Japan's nationwide Arctic research programme, there are already a number of scientist-led projects to promote the culture of the Arctic indigenous peoples. For Japanese scientists, however, the importance of indigenous peoples and their rights in the Arctic appears to be

[58] Ministry of Foreign Affairs of Japan (2018), *Agreement to prevent unregulated high seas fisheries in the central Arctic ocean,* 3 October 2018, https://www.mofa.go.jp/files/000449233.pdf.
[59] Reuters (2019), 'Russia's Novatek to sell 10% of Arctic LNG 2 to Japan's JOGMEC, Mitsui', 29 June 2019, https://www.reuters.com/article/us-russia-arctic-novatek-japan-idUSKCN1TU0F3.
[60] Mitsui O.S.K. Lines (2020), 'Ice-Breaking LNG Carrier makes first call at Japan – Northern Seas Route Voyage from Yamal, Russia to Japan', https://www.mol.co.jp/en/pr/2020/20038.html.
[61] Submarine Cable Networks (2020), 'The Arctic Connect telecom cable project becomes more international: Cinia having new partners from Japan, Norway and Finland', https://www.submarinenetworks.com/en/systems/asia-europe-africa/arctic-connect/arctic-connect-cable-project-becomes-more-international.
[62] Ministry of Foreign Affairs of Japan (2018), *Agreement to prevent unregulated high seas fisheries in the central Arctic ocean*.

something learned gradually as Japan has increased its engagement in the region. It is hoped that Japan's experience in the Arctic will have a positive effect on how the country regards its own indigenous people, the Ainu, and their rights.

It is notable that questions from the conference audience centred around China, even though the session was supposed to be about the Arctic, the UK and Japan. In recent years, the presence of China in the region has increased greatly. There is also speculation that China uses scientific research as a cover to carry out surveillance and intelligence operations. While we should be cautious of making a judgment in haste given that China has – thus far – respected maritime international law in the Arctic, it could be argued that there is a greater need to understand China's unique logic of securitization and external relations. Much like ideas of 'soft power', China defines its ability to shape international discourse as 'institutional discourse power'. For example, it has sought to shape discourse around the Arctic and around China's interpretation of international law. It could also be argued that China is gradually becoming an 'interpretive power', as pointed out in the session, in the sense that it is increasingly confident about expressing its views about interpretations of certain provisions of treaties and conventions in ways that suit China's interests.

While it is naturally attractive to look at Arctic security from the perspective of wider geopolitics, a practical vision for Arctic security is one that prioritizes the machinery of collaboration. For instance, for Japan and its scientists, the fact that the majority of all scientific collaboration with Russia has come to a halt since the 2014 Crimean crisis is more relevant than China's ambition in the Arctic. Russia plans to increase traffic via the NSR by 90 million tonnes by 2030.[63] However, it has been extremely difficult for Japanese scientists and ship operators to obtain basic data on navigation, such as marine observational data or data on accidents and contamination. This is due to a combination of obstruction and ineptitude on the part of the Russian administrative bodies that take such a long time to process paperwork submitted by Japanese scientists. Barriers also exist in working with the US. Under President Donald Trump, the US failed to maintain solidarity with other Arctic states and the international community by withdrawing from the Paris Climate Agreement. The 2019 Arctic Council Ministerial Meeting ended in disagreement when the US blocked adoption of a declaration. It has subsequently proven very difficult for Japan and its scientific community to initiate any collaborative projects on the Arctic with the US. These are examples of small but significant stumbling blocks for scientific cooperation.

The US return to the Paris Agreement could offer the UK and Japan an opportunity to invest diplomatic capital in unblocking scientific initiatives halted in response to the Crimean crisis in 2014. One area for realistic multilateral scientific cooperation with Russia is within the field of humanities and social sciences – for example, a joint project on promoting and protecting indigenous languages. Unexciting as it may sound, such trivial details perhaps capture the reality of Arctic security. Today, the Arctic is no longer a hinterland disconnected

[63] Digges, C. (2020), 'Russia Releases Official Plans for the Northern Sea Route', *The Maritime Executive*, 1 November 2020, https://www.maritime-executive.com/editorials/russia-releases-official-plans-for-the-northern-sea-route.

from any human activities or civilization – it is entangled in the movement of people, money and technology coming in and out of the region.[64] To make this complex web of interaction work, we need more cooperation rather than contestation – and that cooperation begins with small, tedious steps, rather than talk of a grand geopolitical strategy.

[64] Dodds, K. (2020), 'Pandemic 2020 and The Polar Regions: The Geopolitical Year in Review with Prof. Klaus Dodds', *Polar Geopolitics*, 23 December 2020, https://www.podbean.com/eu/pb-4b9tq-f5af9f.

UK–Japan cooperation in response to electronic warfare

By Jun Nagashima
Senior Research Adviser,
Nakasone Peace Institute

Diversity

The history of electronic warfare (EW) began in the 19th century with a series of scientific developments in electronics and electromagnetics. EW has continued to evolve, largely influenced by the rapid advances in technology. Incapacitating or deceiving an adversary's electronic sensors by an electromagnetic attack (EA) is a typical form of EW. The battle between electronic countermeasures (ECM) and electronic counter-countermeasures (ECCM) is an unending competition. As ECM gains superiority, newly developed ECCM comes up and negates this. Because all progress in this battle is relative, the competition among nations in EW is one with no end in sight.

Since the 1970s, the US has gained an advantage in the electromagnetic spectrum (EMS) by increasing the survivability of its war-fighting capability with stealth technology, rather than physically neutralizing the capabilities of adversary radar by EA. Although stealth technology was a winner strategically in terms of the vertical (technological) evolution of EW, its superiority has been rapidly compromised by the use of new EMS countermeasures in the infrared and visible light wavelengths. This is a back-and-forth technological battle of EW. For example, in order to gain an advantage over an adversary in the new operating environment, more active EMS capability has been installed in the latest stealth aircraft in addition to passive stealth technology. In the future, innovative advanced technologies such as artificial intelligence (AI), quantum computing and big data will be incorporated into EW operations. In the struggle for superiority in the EW domain, we can expect to see an increase in revolutionary speed and diversity.

Since the end of the Cold War, Russia and China have rapidly and boldly improved their EW capabilities.[65] Consequently, Japan and the UK each face increased EMS threats, both geographically and strategically. This essay will outline some of the developments in EW and EMS and highlight the importance of Japan–UK–US trilateral cooperation in this field, in order to maximize each country's capabilities and encourage interoperability.

Deterrent approach

What should Japan and the UK both do regarding measures against the ever-evolving nature of EW? The ultimate aim is to prevent an adversary from easily carrying out an EA. It is also useful to convince an adversary that even if an attack is made, the effect will be lower than expected and little advantage can be obtained through these actions. Yet the effectiveness and scale of EW attacks is expanding. If carried out in urban domains, an attack could lead to serious and direct impacts on the lives of citizens by, for example, interfering with GPS reception or causing large-scale disruptions to civilian infrastructure such as power facilities and broadcasting stations. If full-scale war were to occur in outer space, cyberspace and across the EMS, the biggest victim would not be the military, but unprotected civilians who most benefit from these domains in daily life.[66] It is thus necessary to consider a strategy that focuses more on deterrence than on coping with the consequences of an attack. One could consider this as an approach of 'deter the adversary by knowing the adversary's EA capability'.

To achieve this, it is necessary to construct an EMS architecture that enables tactical decentralization of command and delegation of authority to the field in order to make immediate decisions and take appropriate actions in a complex EW environment. AI and autonomous systems will play the central role in this function. A series of processes that harness the power of big data and predictive analytics to provide various response options for commanders are key to this architectural construct.[67] AI is a digital ecosystem that continues to evolve by equipping algorithms and data, and is broadly classified into two types: 'narrow AI' that has human-like ability to specialize in individual areas and exert its abilities; and 'Artificial General Intelligence (AGI)' that solves various and complicated problems in different areas. Moreover, AI evolves through the repeated input of new data while being used empirically. In this sense, the quality and quantity of EMS data collected from tactical edges is vitally important. It is expected that narrow

[65] US Government Accountability Office (2020), 'ELECTROMAGNETIC SPECTRUM OPERATIONS: DOD Needs to Address Governance and Oversight Issues to Help Ensure Superiority', 10 December 2020, https://www.gao.gov/products/GAO-21-64.

[66] Russia and North Korea have significantly affected the lives of citizens by conducting EMS attacks on GPS signals emitted by satellites and by blocking their functions, thereby demonstrating the increasing vulnerability of space systems to EMS.

[67] O'Shaughnessy, T. J. (2020), 'Decision Superiority Through Joint All-Domain Command and Control', *Joint Force Quarterly* 99, 19 November 2020, https://www.16af.af.mil/News/Article/2421718/decision-superiority-through-joint-all-domain-command-and-control.

AI (focused on a specific task) will be implemented through the accumulation of 'big data' and in deep learning. Optimal EMS options will be created through the accurate understanding of the real-time EMS situation in the field combined with predictive analytics based on accumulated historical data and executed by an AI-based autonomous system. Narrow AI will therefore provide support to commanders dealing with the human stress of making consequential tactical decisions as the war-fighting situation rapidly changes. As a result, commanders will be able to maintain sophisticated insight in any environment, understand the effects of EMS operations more clearly, and make optimal decisions at all times.

While advanced technical cooperation between Japan and the UK in terms of security is not widely established, the foundations of cooperation on dual-use technology are steadily being formed.

In addition to big data, the development of advanced technologies such as quantum computing, high-precision sensors, image recognition systems and ultra-high-speed networks is indispensable for accelerating AI and autonomous system capabilities. While advanced technical cooperation between Japan and the UK in terms of security is not widely established, the foundations of cooperation on dual-use technology are steadily being formed. For example, the UK–Japan Quantum Technology Workshop, a private initiative that has been held since 2017,[68] seeks to share information and discuss future UK–Japan collaboration on quantum technology projects. As quantum characteristics attract new attention, the time for practical application of quantum computers may be gradually approaching; countries, including Japan, are looking to develop their knowledge of this field. If miniaturized quantum computers, mounted on AI systems (the core of EW) were to be realized in the future, the speed of decision-making regarding EW would increase dramatically. In addition, an AI-powered, autonomous EW system would be able to identify unknown threats and respond in real time to increase the success rate and survivability of operations.[69] And, if quantum radars using quantum entanglement could be put into practical use, revolutionary and high-performance surveillance systems, with higher survivability and airtightness would be realized, leading to an additional increase in deterrent effectiveness. While realization of these developments remains some way off, the prospect of these huge technological advances means that it is extremely important to develop a 'deter the adversary by knowing the adversary's capability' approach by incorporating these emergent advanced technologies into electromagnetic equipment faster than the adversary is doing. Structural, strategic and rapid incorporation of technology is critical to survival in the electromagnetic race.

[68] National Institute of Information and Communications Technology (2016), 'The 3rd UK-Japan Quantum Technology Workshop/The 4th Quantum ICT Forum', 13 October 2016, https://www.nict.go.jp/en/quantum/event.html.
[69] Defense Advanced Research Projects Agency (n.d.), 'Adaptive Radar Countermeasures (ARC)', https://www.darpa.mil/program/adaptive-radar-countermeasures.

To achieve this, Japan and the UK should find space to develop their technical cooperation. The advanced technologies required for an EMS deterrent approach are dual-use technologies that can be used for both civilian and defence purposes. Japan and the UK confirmed cooperation in dual-use technology in the context of security and defence cooperation at the 2017 Japan–UK Summit Meeting.[70] However, there is one challenge here. In recent years, despite remarkable progress in advanced technology fields, including AI and quantum mechanics, it has been difficult to align these advances with the methods used in the development of conventional defence equipment. However, parallel research and development ingenuity is being studied and practised worldwide, mainly by the private sector, where the implementation of these technologies is progressing at a faster pace. In consideration of this, Japanese and British private-sector engineers and operators should work together to quickly demonstrate the effectiveness of fast-moving civilian advanced technologies, which could aid the speed at which these new technologies are implemented within defence equipment. Joint utilization of private-sector expertise would also enable both Japan and the UK to save costs. Japan's civilian sector includes research institutes such as the National Institute of Information and Communications Technology (NICT) and the Advanced Telecommunications Research Institute International (ATR), that are famous for developing emerging or destructive technologies (EDTs). In this sense, the foundation for technical cooperation on EMS between Japan and the UK has already been established.

Cross-domains operation

At present, due to the rapid advance of science and technology, including innovative information and communications technology (ICT), the connection between the conventional operational domains of land, sea and air has deepened. However, new domains of outer space and cyberspace have been added to the overall operational battle space, and it is important that all operational domains be integrated. In view of this situation, in 2015, China established the People's Liberation Army (PLA) Strategic Support Force[71] to lend assistance to other PLA forces from outer space, cyberspace and the EMS. The US, Russia, France and the UK have also been trying to establish independent specialized organizations in these new domains.

While the world has seen a reduction in large-scale wars with vast physical consequences, low-intensity conflicts involving the illegal operations of non-state actors in these new domains do occur. As a general trend, the main axis of conflict has shifted towards asymmetric operations in the new domains. As a forerunner, China seems to be considering military operations that cross the new domains, using faster and more advanced EMS threats designed to avoid traditional defences. For example, in order to attack major cyberspace networks and to deny the adversary access to necessary operational information, China is advancing 'Integrated

[70] Ministry of Foreign Affairs of Japan (2017), 'Japan-UK Joint Declaration on Security Cooperation', 31 August 2017, https://www.mofa.go.jp/files/000285569.pdf.
[71] Ni, A. and Gill, B. (2019), 'The People's Liberation Army Strategic Support Force: Update 2019', *China Brief,* 19(10), 29 May 2019, https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019.

Network Electronic Warfare', which is based on the combined use of networks and EW, in conjunction with launching asymmetrical warfare in the real world. This is accelerating the trend towards militarization of cyberspace as a war-fighting domain, along with the EMS.

5G and 6G communication networks, combined with the emergence of new technology such as quantum communications, will increase the affinity between cyberspace and the EMS, while offensive operations across such domains will become more common. Turning to outer space, the networking of space systems has advanced, and while the utilization of laser beam communications in the construction of satellite constellations is more common, there is concern about the increase in EMS threats to individual link segments of the space system due to radio interference and interception of communications.

In the future, there will be little choice but to develop an integrated, comprehensive security perspective of the so-called global commons. Japan has begun to focus on 'cross-domain operations' that organically combine the capabilities of new domains with those of conventional land, sea and air domains.[72] The EMS is included alongside outer space and cyberspace as a domain of interest. Unlike other domains, the EMS is not a strategically independent domain, but has the exclusive property of unilaterally influencing all domains.[73] Therefore, the military use of the EMS, which directly affects the safety of these domains, must be considered more comprehensively and strategically. This means that Japan, the UK and their allies should utilize and increase activation of their existing international cooperation frameworks, whether public or private.

Challenges

What approach should be taken to the various evolutions of EW? In the future, as dual-use technology rapidly evolves, the benefits and utility of the global commons will increase for the private sector. On the other hand, instability and insecurity due to horizontal expansion (degree of use) will remain a major concern. The emergence of new risks and threats, along with continuing vertical advancements, will require a cost-effective application of national resources to manage these developments. This will necessitate innovative multilateral cooperation that challenges traditional considerations of national sovereignty.

In the Asia-Pacific region, there is no collective security organization like that in Europe, and because of history, politics and regional characteristics, it is not realistic to establish a new NATO-type military organization to cope with emerging risks and threats. Rather, it will be an urgent priority to apply existing security cooperation frameworks such as the bilateral Japan–US alliance, the 'Quad' of the

[72] Ministry of Defense, Japan (2020), 'Responses in the Domains of Space, Cyber-space and Electromagnetic Spectrum' in *Defense of Japan 2020*, pp. 266–74, https://www.mod.go.jp/e/publ/w_paper/wp2020/pdf/index.html.
[73] Parkinson, J. (2019), 'Is Fluidity the Key to Effective Multi-Domain Operations?', *The 2019 Joint Air & Space Power Conference 2019 Read Ahead*, Kalkar: Joint Air Power Competence Center, https://www.japcc.org/is-fluidity-the-key-to-effective-multi-domain-operations.

US, Australia, India and Japan, the 'Five Eyes' that share values such as diplomacy, security and human rights, and the 'Free and Open Indo-Pacific' (FOIP) to this new regional security framework in a multi-layered manner.

What is needed to realize deterrence under this framework? Firstly, Japan, the UK and other like-minded countries should start to issue strategic messages to potential adversaries in a coordinated manner. From the perspective of public diplomacy, holding regular summits and existing 2+2 meetings under these security frameworks would have a significant deterrent effect, as would publishing an agreed communiqué.

Secondly, in order to further ensure effective deterrence options, it is essential for these countries to maintain interoperability in EMS operations and to develop combined military operational capabilities. In fact, if there is a lack of communication between the countries involved and physical linkages between assets cannot be achieved, efforts to carry out cooperative actions will come to nothing. In this regard, the regular implementation of combined exercises and training events by the countries concerned, as well as the implementation of table-top exercises, would have immediate and remarkable effects. In this context, it is extremely important to make efforts to stimulate communication among the cooperating countries and mitigate the capability gap.[74] Japan and the UK are already established strategic partners that share the values of 'freedom, democracy, human rights, the rule of law and the market economy', which underline their efforts to tackle the 'various global challenges confronting the international community'.[75] Thirdly, from a geopolitical point of view, Japan and the UK are both sea powers,[76] and through trilateral partnership with the US, their common ally, the environment in which Japan and the UK can contribute to world security beyond the boundaries of their own region is already in place. The maintenance of interoperability between the technologies of these countries will be a major prerequisite for the countries concerned to act together.

Trilateral cooperation and prospects for operational interoperability

In 2021, the UK will send HMS Queen Elizabeth and her Carrier Strike Group to the Indo-Pacific region.[77] There are plans for this group to participate in naval activities to commemorate the 50th anniversary of the Five Power Defence Arrangements (FPDA), a military alliance between the UK, Singapore, Malaysia, Australia and New Zealand, and to conduct combined exercises with regional partners.[78]

[74] In multilateral joint training, mutual efforts between Japan and the UK began in the 1980s. For example, RIMPAC (Rim of the Pacific Exercise, 1986), Quad (Malabar, 2020), NATO (Exercise in the Baltic Sea, 2018).
[75] Ministry of Foreign Affairs of Japan (2008), 'Speech by Mr Shintaro Ito, State Secretary for Foreign Affairs, at a Reception to celebrate 150 Years of Diplomatic Relations between the United Kingdom and Japan at the Foreign & Commonwealth Office, London', 16 September 2008, https://www.mofa.go.jp/region/europe/UK/speech0809.html.
[76] Mackinder, H. J. (1943), 'The Round World and The Winning of The Peace', *Foreign Affairs*, July 1943, https://www.foreignaffairs.com/articles/1943-07-01/round-world-and-winning-peace.
[77] Ministry of Foreign Affairs of Japan (2021), 'Press Releases: Fourth Japan-UK Foreign and Defence Ministers' Meeting ("2+2")', 3 February 2021, https://www.mofa.go.jp/press/release/press3e_000163.html.
[78] Storey, I. (2020), 'Can the UK Achieve Its Naval Ambitions in the Indo-Pacific?', *The Diplomat*, 7 November 2020, https://thediplomat.com/2020/11/can-the-UK-achieve-its-naval-ambitions-in-the-indo-pacific.

The Queen Elizabeth's air wing will include the F-35B Lightning, a fifth-generation fighter equipped with stealth technology and the latest EW system. Japan also has this common force platform (consisting of 147 F-35s, including 42 F-35Bs), as the realization of the future air defence system under the 2018 National Defense Program Guidelines. It is expected that combined training by the F-35s of Japan, the US and the UK will be carried out in the vicinity of Japan in the near future, just as British Air Force Typhoons came to Japan in 2016 and conducted combined training with Air Self-Defense Force fighters. In this context, combined training in EW would mean that interoperability between Japan, the US and the UK in the EMS field would be improved through the sophisticated EW capabilities of the F-35, and at the same time, it would have an effect as a major strategic message to neighbouring countries that have been enhancing their EMS capabilities. Furthermore, this effect will contribute to the improvement of operational interoperability by eliminating the capability gap related to EW. By continuing this practical relationship in EW, it will be possible for the UK and Japan to contribute to regional stability through the strengthening of their bilateral partnership, and to global stability through their trilateral cooperation in new domains alongside the US.

Conclusion

EW has continued to evolve as a means of offence and defence in warfare, but it has also gained strategic value through technological breakthroughs and the development of operational tactics. In the future, as militarization of cyberspace and outer space as well as the integration of these domains progresses, use of the EMS, which plays a catalytic role at the centre of these domains, will have increasingly important security implications. Moreover, as its potential impact on the private sector becomes more direct and serious, every country will have to continue to improve their capabilities. Developing EMS capacity is also a race against time as well as a competition against adversaries for accumulating EMS information (big data) and advanced technologies. A single country's response will likely be insufficient; cooperation among Japan, the UK and the US is key to competing effectively in the EMS. For this purpose, it is important to make steady efforts to strengthen interoperability while identifying and eliminating capability gaps one by one, through joint training and defence exchanges.

Meeting summary: Security at the Frontier

10–11 December 2020

Session 01

Cyberspace: UK–Japan responses

The UK and Japan have developed a close alliance on matters of cyberspace since 2012. Their cooperation on, as well as their responses to, international issues arising in this area was the focus of the first session of the conference. Masahiro Kurosaki chaired the session and opened the discussion. In his address, he posed a range of questions regarding the two countries' relationship, its successes and its future. Kurosaki also highlighted the need to promote a 'free, open, peaceful, fair and secure' cyberspace amid diverging approaches to cybersecurity at national levels. Kurosaki's questions functioned as the backdrop to the following discussion.

Jamie Saunders spoke as a practitioner in the field, having held positions within the UK government, as well as business roles in the cybersecurity industry. He focused his address on the importance of bilateral collaboration between the UK and Japan in the political and business contexts. He highlighted three key reasons for the relationship. First, the UK and Japan's mutual security dependencies: both states are tied by shared military supply chains, business interests in each other's markets, and by the role of Japanese companies in the UK's critical national infrastructure. Second, the countries' shared interest in sustaining an open and global digital economy: the UK and Japan support each other's positions regarding cyberspace in international forums, such as the UN, G7 and the ASEAN Regional Forum. Third, there are ample opportunities in global cybersecurity that the UK and Japan can explore together. Saunders pointed to the states' complementary domestic strengths in cybersecurity, as well as opportunities to win joint business in the global marketplace. He concluded by emphasizing the value of the relationship of interoperability, mutual recognition, and development of 'future-proof' regulations – policies that foresee technological advances and are apt for dealing with them.

Tomohiro Mikanagi explored the legal aspects of UK–Japan cyberspace collaboration. He commenced his remarks by stating that the countries are 'natural partners' given their shared viewpoints regarding cyberspace. He continued by discussing the application of existing international law to cyberspace, the difficulties of this practice, and UK–Japan responses to this. He enumerated three fundamental concepts that pose a challenge to the effective application of existing law: sovereignty, attribution and due diligence. Mikanagi explained that the nature of cyber operations blurs traditional notions of sovereignty transgressions and non-intervention, which tests the applicability of existing law. The UK is very cautious about the violation of sovereignty, which renders this a point of disagreement between the UK and Japan, despite their overarching agreement on the applicability of international law. Mikanagi then turned to attribution. He stated that evidence of cyber operations emanating from foreign territories is hard to obtain, given the common use of proxies. This has destabilized current practices regarding the legal attribution of state conduct. Mikanagi therefore argued for circumstantial, as opposed to concrete, evidence to be admitted in legal accusations. While the UK is said to be more active than Japan in making diplomatic (rather than legal) accusations, they are in agreement on the need to admit circumstantial evidence of cyber operations. Regarding due diligence, Mikanagi highlighted the obligation of states to protect the international community from the action of non-state actors (NSAs) from their territories. This obligation is useful in the cyberspace debate since it deters states from supporting NSAs and using them as proxies for cyber operations. He commented that this was another area on which the UK and Japan agree. Mikanagi concluded by restating the importance of the free flow of data, the application of international law, and the maintenance of a rules-based international order across cyberspace activities.

Emily Taylor deliberated on the 5G debate, and the international standards applied to internet infrastructure. Regarding 5G technology, she maintained that concerns about the security implications are 'absolutely valid' in the decision-making process, domestically or otherwise. She cited several reasons: lack of competition in the 5G market, the long-term commitments of infrastructure choices, as well as the nature of cybersecurity. She argued that, when these considerations reach the international level, mostly regarding Huawei, the experience of the UK and Japan have been similar, with both caught in the middle of strident US–China rhetoric. Both states are strong allies of the US in their respective regions, but neither has been willing to alienate China. Taylor moved on to discuss the international standards applied to the internet. In a recent UN International Telecommunication Union (ITU) meeting, China proposed a suite of changes to the basic internet architecture (TCP/IP address). Taylor noted that if these changes are passed, the very foundations of the internet could change. Faced with the possibility of a 'new internet', Taylor urged that states must establish norms for responsible cyber behaviour. These should be discussed in well delineated forums, to stop the practice of 'forum shopping on ideals' – i.e. picking and choosing which conventions to abide by. Finally, Taylor noted the benefits of UK–Japan relations in this context, claiming that its bilateral nature is helpful, given the global drop in confidence in multilateral partnerships. Both countries' adherence to shared values and voluntary actions have also proven positive, as these dissipate geopolitical tensions and promote peace and stability.

During the question-and-answer session, the panellists agreed on the grandiosity of the term 'cyberspace'. Saunders aligned himself with William Gibson, who referred to the term as a 'shared hallucination'. In Taylor's view the term is sector-specific. She explained that the terminology is not often used in technological circles, but that the policymaking world favoured it for its umbrella-like quality. Mikanagi reinforced this division, explaining that the international law community prefers to avoid the term given its implication of a physical space, which creates difficulties for the application of the existing legal framework. The second half of the Q&A session gave way to a discussion on the importance of maps and geography in a world of virtual connectivity. Taylor first reiterated the importance of geography and topography in the construction of essential internet infrastructure as 'it is rooted in the ground'. She also addressed the point of data mapping, highlighting the visual value of maps when it comes to organizing the internet. Saunders furthered this by claiming that data visualization enables management, especially in a crisis. Mikanagi made a pragmatic point regarding international treaties, noting that while the internet has made the world smaller, treaties on cyberspace are agreements between countries, thereby rooting them in geography.

Session 02
Outer space: UK–Japan responses

Session two focused on the key governance and security challenges of outer space. This session was chaired by Patricia Lewis, who introduced the theme through a series of questions: What are the rules governing space activity? What are the latest developments in UK–Japan outer space policies? How can the two countries work together with others to create a secure and peaceful policy that ensures the long-term sustainability of outer space? Lewis then introduced the three speakers, who made their opening remarks.

Daniel Porras highlighted the international debate on how to prevent an arms race in outer space. According to Porras, arms races can be seen in multiple domains, including among delivery vehicle companies, cyber capabilities, social media, and so on. The increased attention given to outer space technology is part of this trend. Porras indicated three markers of an arms race that are present within the space domain: rivalries, corollary weapons and accelerated developments. Regarding rivalries, he noted the low level of trust between powers and their allies. He then pointed to corollary developments in counterspace technology. This can take the shape of anti-satellite missiles, co-orbital drones and vehicles. Next, Porras commented on the acceleration in the development of outer space technology: he cited the heightened interest in military outer space forces, a renewed sense of urgency regarding conflict, and the surge in policies pursuing defensive capabilities in outer space. Interestingly, these defensive pursuits have proven to support technology that also has offensive capabilities. Porras concluded his opening statement by acknowledging the international desire to establish norms for space behaviour. He also commented, however, that there have so far been few achievements in this pursuit, despite the number of international forums and discussions dedicated to the subject.

Following on from Porras' international overview, Alexandra Stickings offered the UK outlook on the outer space question. She noted that, despite early entry to space activity, the UK has struggled with its identity as a space actor. Throughout its history, the UK has lacked cohesion in, and has not prioritized, its approach to outer space. However, according to Stickings, this behaviour is changing and the UK is now taking meaningful steps to develop its space identity. On the domestic front, Stickings alluded to the Ministry of Defence's appointment of its first director space, the planned formation of a UK Space Command, and the establishment of a National Space Council. In the international arena, the UK is leading multilateral discussions around behaviours and norms. Stickings claimed these are the actions of a medium-sized space power; that is, a power that lacks the hardware but is diplomatically strong in the sector. Arriving at this position, the UK must now question its future: the potential of its space capabilities, the implications on governance, and the best ways to build on this new identity to form international partnerships. Stickings closed her remarks by drawing a parallel between the British and the Japanese positions as medium powers, commenting that, together, the states could lead the international discussions on long-term sustainability of outer space, which is an exciting prospect.

In the international arena, the UK is leading multilateral discussions around behaviours and norms. Stickings claimed these are the actions of a medium-sized space power; that is, a power that lacks the hardware but is diplomatically strong in the sector.

Setsuko Aoki provided the Japanese outlook on outer space. She began her statement by introducing Japan's Basic Space Plan (BSP). This document, written and adopted in 2020, sets out directives for Japan's behaviour as a space actor. The vast majority of these items promote international rule-making, demonstrating the country's priority in the space domain. Aoki continued by recognizing and praising the role of the UK in one of Japan's recent BSP accomplishments. Only three days prior to the conference, on 7 December 2020, the UN General Assembly adopted an energy resolution led by the UK and backed by Japan. This accomplishment, Aoki claimed, demonstrates Japan's willingness and expectation to work alongside the UK in maintaining, promoting and enhancing space security. Aoki went on to comment that prioritizing space security has become a new ideal in Japan. Previously, Japan had been unable to develop a strong space presence due to its constitutional restrictions regarding offensive military capabilities. When, in 2008, defensive military actions in outer space were internationally legitimized, Japan was liberated to become a peaceful space actor. Since then, the country's position has slowly changed to incorporate elements of security. Indeed, the current BSP was the first national space document to focus on space security. Aoki concluded her remarks by stating that she is optimistic about future promotion and commercialization of the outer space industry.

During the Q&A, three important themes were discussed: the expense of outer space technology, the need for international best practice norms, and communication on outer space. First, Aoki and Porras outlined the huge expense of outer space developments, resulting in the need to create alliances in this industry. Porras furthered this idea by suggesting that states should identify areas in which they can add value to specific projects and team up with partners to execute them. Second, Lewis pointed to the reluctance of countries to commit to cementing hard laws in place on outer space, given the difficulties this can lead to when adapting to future technological advances. Stickings was pragmatic, urging states to accept that space is now militarized, and that international forums should come to an agreement on responsible behaviour in this new reality. Third, panellists agreed that communication on outer space must improve to include the general public in the debate. This engagement would create the political pressure that is necessary for leadership to move on these topics. Finally, the session concluded with a reminder from Stickings that, despite all the talk of competition, outer space also has the potential to bring individuals and countries together, through the realization that there is much more out there, beyond our planet.

Session 03
Engaging the Arctic: UK–Japan responses

Session three was opened by the chair Caroline Kennedy-Pipe. She announced the topics of the session, focusing on the relationship between the UK and Japan over Arctic issues, and alluded to the events in the region. She then introduced the panel.

Kazuko Shiraishi drew from her experience as Japan's ambassador to the Arctic to affirm the official Japanese position on matters relating to the Arctic. Shiraishi explained that despite being involved in Arctic research since the 1950s, Japan had only created an official policy document on the Arctic in 2015. This document aimed to define Japan as an important player on Arctic issues. It centred on three initiatives: research and development through international cooperation, the importance of the rule of law, and sustainability. The first initiative supports Arctic research whereby Japan seeks to better understand climate mechanisms and its effects on human communities across the world. The country takes part in international projects (such as the Arctic Challenge for Sustainability, or ArCS) and data-sharing systems to promote international cooperation. The second initiative endorses a free and open maritime order in the Arctic region, based on the rule of law. Shiraishi stressed the need for treaties between actors engaging with the Arctic to regulate activity in that region. The third initiative also urges responsible behaviour given the climate challenges facing the Arctic. It also recognizes the economic opportunities offered by the Northern Sea Route. Shiraishi assured participants that this third initiative seeks to balance both elements. She concluded by commenting that UK–Japan partnership on Arctic matters contributes to the international community, to scientific research and to rule-making. She noted her hopes for their future cooperation with Arctic states to ensure the freedom and openness of the Arctic region.

Aki Tonami began by commenting that Japan engages two types of situational awareness with regard to the Arctic: a traditional security approach, and one that encompasses a broader understanding of global security. First, Japan relies on the Arctic for economic, energy, climate and food security. Tonami noted how ongoing competition and collaboration between China, South Korea and Japan impacts each of these dependencies. She continued that, despite calls for a legally binding agreement to govern Arctic activity, the Arctic corridor states had already officially rejected the need for such a legal regime, preferring soft law instruments and cooperation between Arctic states instead. This set-up limits the participation of the UK and Japan, which are not Arctic states, in the governance of the region. Yet, it does not hinder it. According to Tonami, the UK and Japan are still able to propose projects that reinforce their views on specific issues. Lastly, Tonami drew attention to the fundamental differences in the way that Arctic states and Asian states – such as China, South Korea and Japan – see the region. Arctic states take a more liberal institutional approach, while Asian actors are inclined to be realists. Tonami concluded her presentation by calling for the strengthening of a rules-based international order in the Arctic region and beyond.

Nengye Liu discussed three topics in his presentation: the UK's Arctic policy, the rules-based international order, and the extent to which the UK and Japan strengthen that order in the Arctic. First, he recognized the UK as an influential Arctic player given its history, geographical proximity and economic-military power. He explained that British policy in the Arctic exists alongside parallel European Union and Scottish policies but that these largely disseminate the same values on Arctic sustainability. Second, Liu criticized the term 'rules-based international order', which is abundantly present in policy talks. He suggested that there is an inherent power structure implied in its use that marginalizes states seen as potential rule-breakers. In his view, these 'rule-breakers' represent potential changes to the international power structure. He reminded the audience that rules are being created in the Arctic now, and that differing visions should not marginalize traditionally weak states. Third, he highlighted the importance of the Arctic Council. Liu claimed that the UK and Japan can best support the Arctic by championing the Arctic Council. As the representative of the Arctic people, Liu concluded that the Council is in the best position to make appropriate decisions about the freedoms and sustainability of the region.

During the Q&A panellists were asked about China's behaviour in the Arctic region, and whether it was disruptive. Shiraishi recognized that Chinese vessels only sail in the high seas, violating no international law. Yet, the increased presence of these vessels demands vigilance from all nations interested in the region. Similarly, Tonami agreed that China has acted responsibly in the Arctic, noting that this contrasted hugely with the country's behaviour in the South China Sea. Liu suggested that this was due to the varying importance of the regions, commenting that while the South China Sea is a 'core interest' for China, the Arctic is not. This difference could be used to explain the differences in behaviour that the international community has observed.

Session 04
Military use of the electromagnetic spectrum and electronic warfare: UK–Japan responses

The final session of the conference was chaired by Mathieu Boulegue. He introduced the topics for discussion, namely the military and security implications of the use of electronic warfare, and the British and Japanese responses to this growing challenge. Boulegue then went on to introduce the speakers.

Chris Fogarty drew upon his experience as a military practitioner to make his opening remarks. His presentation relayed the advantages, prevalence, legal requirements and counter methods of electromagnetic technology and strategy. To begin, Fogarty outlined both the importance and prevalence of electromagnetic technology, commenting that technologies such as GPS, Bluetooth and Wi-Fi are all dependent upon electromagnetic waves. He then defined the three dimensions of electronic warfare (EW): surveillance, defence and attack. Given the demonstrated importance of this technology for modern warfare, Fogarty shared an overview of different nations' positions, outlining government spending, recent technological developments and military organization of EW for several powers: the US, Australia, South Korea, Japan, China, Russia, Iran, North Korea. He then turned to the legalities of this type of warfare. Domestically, he explained that any EW activity within the UK requires a warrant or permission. Internationally, however, there is less certainty, with a noticeable lack of unambiguous (and ratified) treaties on the topic.

Zysk followed by stating that Russia places high value on information superiority, and that EW could be used as a tool to disrupt the backbone of its adversaries' information systems.

Katarzyna Zysk discussed the role of Russia in the EW debate. She explained the driving forces behind Russia's strong focus on EW, contextualizing these forces within the wider framework of Russian defence. First, she confirmed Russian commitment to the electromagnetic domain in contemporary warfare. This, she argued, is part of the country's strategy to close its military capability gap with its potential opponents. Zysk followed by stating that Russia places high value on information superiority, and that EW could be used as a tool to disrupt the backbone of its adversaries' information systems. There is a belief in Russia that this technology can be especially useful against an opponent that is militarily stronger. Lastly, Zysk referred to the use of psychological operations (using propaganda to create fear and uncertainty among opposing forces) to demonstrate the scope of Russia's EW offensive capabilities. These advances in EW technology and interpretations are projected to continue at least until 2027, when the current state armament programme will end. These developments represent the growing complexity of Russian power projection in the international arena. Zysk concluded by predicting continued growth in EW as new technologies are adapted to military use, and reminded the audience of the importance of the role of NATO in this contested space.

The final speaker, Jun Nagashima, discussed the Japanese position. He tackled three themes: an overview of the current situation, Japan's position and future challenges. First, he defined EW and noted some of the commonplace defence and attack tactics that are used in this domain. Nagashima also discussed the arms race in EW technology, claiming that the US is working hard to catch up with other powers' capabilities. He forecast that countries would see the integration of artificial intelligence (AI) and quantum technology with EW technologies, and the further integration of the digital and physical worlds in this domain. Second, Nagashima focused on Japan's position and efforts in EW. In recent years, the country has demonstrated significant interest in the defence of its electromagnetic domain, as well as the integration of traditional and contemporary warfare tactics. Nagashima shared Japanese intentions in this space, regarding equipment investment and alliances, underlining the importance of NATO, and the need for defensive readiness. Third, Nagashima looked to the future, particularly regarding the use of quantum technology. He claimed that the use of quantum particles, rather than quantum waves, has not been explored for military use. He predicted a development along these lines to be the next step in modern warfare tactics. He closed by urging Japan and its allies to eliminate EW vulnerabilities and strengthen their electronic resilience.

Boulegue opened the Q&A by asking the experts about the West's performance in the EW race. On the one hand, Fogarty recognized the difficulties in the procurement of military technology given the rapid pace of general technological advancement. On the other hand, he confirmed that the West has been adapting its military units and creating integrated commands to act on new domains. Zysk reminded the audience that Russia had invested so many resources in EW because it has been identified as a weakness in its opponents' strategies. On the effects of EW in times of peace, Nagashima raised two important points: the invisibility of these actions, and more importantly, the impossibility of determining the magnitude of the damage prevented. Zysk and Fogarty agreed that employing EW tactics in times of peace had become the 'new normal', requiring resilience from civilian and military electronic equipment. Lastly, Boulegue asked the panellists how EW can affect the lives of individuals. Fogarty listed medical consequences, such as infertility, cancer or pacemaker violation, and also highlighted the psychological damage that could arise if everyday technology is severely disrupted. Zysk took a broader stance, pointing out that EW has the potential to damage everything from the economy to information dissemination systems, with the potential to cause huge societal chaos.

Participants

Setsuko Aoki, Professor of Law, Keio University Law School, Keio University, Japan

Mathieu Boulegue, Research Fellow, Russia and Europe Programme, Chatham House

Chris Fogarty, Commanding Officer, 14th Signal Regiment (Electronic Warfare), The British Army

Caroline Kennedy-Pipe, Professor of International Security and International Relations, Loughborough University, UK

Masahiro Kurosaki, Associate Professor of International Law, National Defense Academy of Japan

Patricia Lewis, Research Director, Conflict, Science and Transformation; Director, International Security Programme, Chatham House

Nengye Liu, Associate Professor; Director, Centre for Environmental Law, Macquarie Law School, Macquarie University, Australia

Tomohiro Mikanagi, Deputy Director-General of the International Legal Affairs Bureau (Deputy Legal Adviser), Ministry of Foreign Affairs, Japan

Jun Nagashima, Senior Research Adviser, Nakasone Peace Institute, Japan

Daniel Porras, Director of Strategic Partnerships and Communications, Secure World Foundation, US

Jamie Saunders, Fellow, Oxford Martin School, University of Oxford

Kazuko Shiraishi, Ambassador of Japan in charge of Arctic Affairs (2015–17)

Alexandra Stickings, Research Fellow for Space Policy and Security, Royal United Services Institute (RUSI)

Emily Taylor, Associate Fellow, International Security Programme, Chatham House

Aki Tonami, Associate Professor of International Relations and Economics, University of Tsukuba, Japan

Katarzyna Zysk, Professor, Deputy Director and Head, Security Policy Centre, Norwegian Institute for Defence Studies, Norway

About the authors

Emily Taylor is an associate fellow with the International Security Programme at Chatham House. She is CEO of Oxford Information Labs, author of several research papers, and is a frequent panellist and moderator at conferences and events around the world. She has previously held roles in the Internet Governance Forum Multistakeholder Advisory Group, in the Global Commission on Internet Governance research network, as chair of the ICANN WHOIS Review Team and director of legal and policy for Nominet. She has written for the *Guardian, Wired*, *Ars Technica*, the *New Statesman* and *Slate*. Emily is a graduate of Cambridge University, qualified as a solicitor in England and Wales, and has an MBA from the Open University.

Alexandra Stickings is a research fellow for space policy and security in the Military Sciences team at RUSI. Her research covers military space programmes, space warfare, counterspace capabilities, space situational awareness, arms control and the intersection of space and missile defence. She has written articles and research papers for a variety of publications, is a frequent speaker at international conferences and regularly provides expert commentary to the media. Alexandra holds an MSc in international security and global governance from Birkbeck College, University of London, a BA (Hons) in international studies from the Open University and a BSc (Hons) in physics with astronomy from the University of Nottingham.

Dr Aki Tonami is an associate professor in international relations and economics at the University of Tsukuba. She is also a senior research fellow at the Nordic Institute of Asian Studies, University of Copenhagen. Having worked as research adviser for the Ministry of Foreign Affairs of Japan, Dr Tonami is a specialist in foreign policy and development in Asia, with research interests in economic diplomacy and governance of the Polar Regions. She has a PhD in global environmental studies (2008) and a MA in economics (2004) from Kyoto University, and a BSc in commerce from Santa Clara University. Her recent publications include ‘The rise of Asia and Arctic legal order-making: political-economic settings’ (in Shibata et al. (eds) (2019), *Emerging Legal Orders in the Arctic: The Role of Non-Arctic States*, Routledge), and *Asian Foreign Policy in a Changing Arctic: The Diplomacy of Economy and Science at New Frontiers* (Palgrave Macmillan, 2016).

Lieutenant General (Retired) Jun Nagashima is a senior research adviser with the Nakasone Peace Institute and an executive member of DESI Japan. He has previously served as a Japanese government cabinet councillor starting in August 2013 and also as deputy assistant chief cabinet secretary, in the National Security Secretariat, from January 2014. He is the first military officer to hold the position of cabinet councillor in Japan. As an intelligence expert, his extensive career includes critical assignments as defense attaché, liaison officer to NATO and the EU, Embassy of Japan in Belgium; director, logistics (J-4), Joint Staff Office; and defense intelligence officer, Defense Intelligence Headquarters. He retired in August 2019. He is a graduate of the National Defense Academy and earned his master’s degree (European security) from Tsukuba University. He is a prolific writer of academic essays, including ‘Proliferation of Ballistic Missile and Security of East Asia’, *Journal of National Defense* (November 1994), which won the prestigious 1994 Kamiya Fuji Prize.

Chatham House does not express opinions of its own. The opinions expressed in this publication are the responsibility of the author(s).

Cover image: An H-2A rocket carrying the ASTRO-H satellite, developed in collaboration between the Japan Aerospace Exploration Agency (JAXA), NASA and other groups, lifts off at the Tanegashima Space Center in Kagoshima Prefecture, southwestern Japan on 17 February 2016.

Photo credit: Copyright © JIJI Press/Stringer/Getty Images

ISBN 978 1 78413 462 4

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

CHATHAM HOUSE

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223