

POLICY BRIEF

Promises and Challenges of Digital Connectivity¹

Abstract

Digital connectivity – loosely defined as connecting people through digital means – promises to enhance our quality of life, as envisaged in Japan’s ‘Society 5.0’, which aims to spur economic growth and solve social problems digitally. On the other hand, digital connectivity also creates challenges and demands a quest for optimum equilibrium between economic growth and national as well as human security.

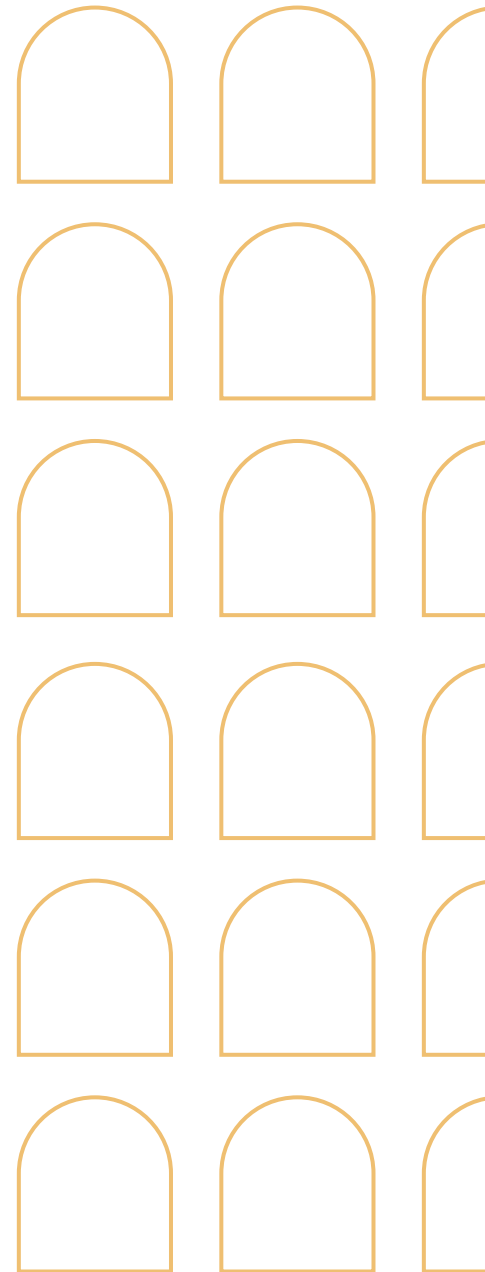
The COVID-19 pandemic which erupted in late 2019 has accelerated world dependence on digital connectivity in order to sustain human contact. Digital means have allowed us to continue our lives, work and pleasure connections, and have simultaneously expanded digital risks at home and globally. The COVID-19 scenario has also demonstrated how digital technology can even threaten our sovereignty and basic values such as freedom, democracy, privacy, human rights and dignity.

Japan and the EU approach the digital age with a common emphasis on leading standards to set and promote a human-centred digital connectivity. The two zones can cooperate bilaterally and beyond in responding to challenges on digital connectivity, as is stipulated in three key documents, namely Japan-EU Economic Partnership Agreement (EPA), Japan-EU Strategic Partnership Agreement (SPA) and Japan-EU Partnership on Sustainable Connectivity and Quality Infrastructure.

¹ The author sincerely thanks Dr. Maaïke Okano-Heijmans, Senior Fellow at the Netherlands Institute for International Relations, Clingendael, for her insightful advice and comments in drafting the policy brief. Any flaws in the paper, however, is the author's.

Authors

Akiko Fukushima, Senior Fellow, The Tokyo Foundation for Policy Research, Japan



EU-Asia project

Issue 2021/23
June 2021

1. Introduction

Digital economy is growing at an unprecedented pace. The COVID-19 pandemic has spurred such growth due to restrictions on human movement and physical contact through lockdowns and state of emergency declarations. Although vaccines have been developed and supplied, we might continue to be restricted in our physical contacts for a while. The void of face-to face interaction has been filled most notably by digital technology. The world has seen a surge of teleworking, online meetings, online shopping and even online concerts and theatres. Even when we purchase physically at shops, we pay with smartphones rather than with cash, which we rarely use. The pandemic has accelerated unmanned digitalised operations and communications.

'Data Age 2025' predicted in 2018 that the annual size of the Datasphere – the sum of the world's data – would grow from 33 zettabytes in 2018 to 175 ZB in 2025 – multiplication by fivefold.² This represents an explosion of data traffic from diversified origins and formats. With the pandemic, the size of the data traffic has, no doubt, increased much more than the original prediction made in 2018. For this quantity of data to flow without problems, we need reliable and resilient digital infrastructure and governance frameworks.

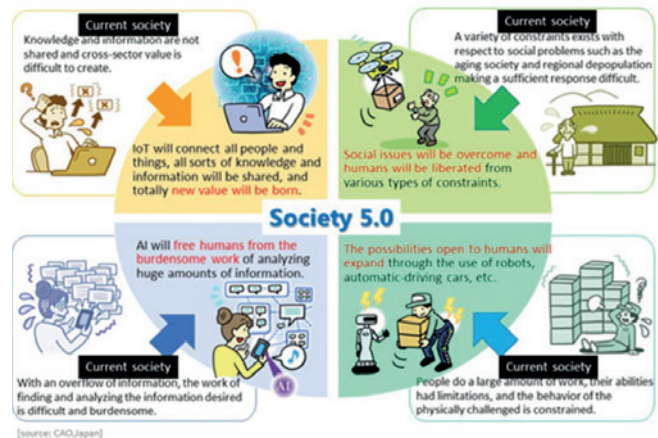
This paper begins with a comparison of Japanese and EU policies on digital connectivity, followed by case studies, namely data flow, subsea cables and fifth-generation mobile network (5G) and beyond, to identify promises and challenges of digital connectivity. The paper concludes with observations on cardinal factors to be weighed in the quest for optimum equilibrium between economic growth and security for both nations and humans.

2. Comparing Japan's and EU's approach towards a digital age

It has been observed that US and China are leading in the digital field, while Japan and EU member states are lagging behind³. However Japan and the EU have lately placed priorities on 'digital' investment. Both are striving to adapt to a digital age and aim to lead rather than to be led.

Japan launched 'Society 5.0' in the 5th Science and

Technology Basic Plan, announced in 2018. Society 5.0 aims at a 'human-centred society that balances economic advancement with the resolution of social problems through a system that highly integrates cyberspace and physical space.'



Source Cabinet Office, https://www8.cao.go.jp/cstp/english/society5_0/index.html

Why is it named as Society '5.0'? The number symbolises the process of evolution, from Society 1.0, based on hunting and gathering to the agriculture-based Society 2.0, further to industrial Society 3.0, and then to information Society 4.0. What is the difference between Society 4.0 and Society 5.0? Both are based on information technology. In the information-based Society 4.0, people have been overwhelmed by the data and information available; they have had to select data they want to use and to process it. In a new information Society 5.0, convergence between cyberspace and physical space is achieved through artificial intelligence (AI). In other words, in Society 4.0, users had to access a cloud service via Internet and search for information or data they need. In Society 5.0, information from sensors in physical space is accumulated in cyberspace. This information is analysed by AI and the results are fed back to humans in physical space, by AI and robots. It is therefore ready to be used by people. In Society 5.0, Japan seeks to achieve both economic growth and solutions to social problems through digital means. The plan would free human beings from everyday cumbersome work and tasks.⁴ This approach strives to solve social problems, such as how to best manage an aging population.

2 Alex Woodie, 'Global DataSphere to Hit 175 Zettabytes by 2025, IDC says,' Data Nami, November 27, 2018, available at <https://www.datanami.com/2018/11/27/global-datasphere-to-hit-175-zettabytes-by-2025-idc-says/>, last accessed on 9 February 2021.

3 McKinsey & Company and ACCJ, 'Japan Digital Agenda 2030,' p.10, available at <https://static1.squarespace.com/static/5eb491d611335c743fef24ce/t/603cb0268d95692ce3c854a8/1614590006613/Japan+Digital+Agenda+2030+en.pdf>, last accessed on 20 April 2021.

4 Cabinet Office (Japan), 'Society 5.0,' 2018, available at https://www8.cao.go.jp/cstp/english/society5_0/index.html, last accessed on March 9th, 2021.

In order to realise Society 5.0, in June 2020, Japan's Ministry of Internal Affairs and Communications launched 'Beyond 5G Promoting Initiative'. Looking ahead to 2030,⁵ the Initiative emphasises secure and sustainable digital infrastructure, including the next generation of 5G. As a backbone of Society 5.0, digital infrastructure will integrate

cyberspace with physical space through the operation of Cyber-Physical Systems (CPSs). In the 2030s the Initiative plans that advanced CPSs will create flexible and resilient society where daily life and economic activities are fully maintained within cyberspace, even if there are unexpected crises in the physical world. Thus, in the 2030s the Initiative expects society to be inclusive, sustainable and dependable: everyone, including the elderly and those with disabilities, can benefit and live harmoniously together. The Initiative emphasises R&D to develop a range of technologies from wireless, low energy and secure networks with emerging technologies on quantum technology and AI. The Initiative also calls for cooperation with strategic partners such as the EU and the US, not only in development but also for standards setting. In March 2021, a Consortium to promote Beyond 5G Initiative was launched involving all the stakeholders, including the government, academia and industry.⁶ Japan plans to demonstrate the progress of its Initiative in the 2025 Osaka Expo as a Beyond 5G showcase.

Furthermore Japan adopted Social Principles of Human-Centered AI in 2019 and has established the Council for Social Principles of Human-centric AI for implementation⁷. The principles assert that AI plays a significant role in realising Society 5.0 for the efficiency and convenience of residents as well as for the public good of humanity as a whole. The basic philosophy of the principle is to use AI for dignity, diversity, inclusion and sustainability. Human-centred AI principles include education/literacy and privacy protection. These principles also emphasise cybersecurity. The Council continues to examine the most recent AI research and discussions at home

and abroad. The latest Council meeting held in December 2020 examined the development of AI research in Japan as well as international discussion on AI. Included in the discussion was the Council of Europe's Ad hoc Committee on AI (CAHAI) and its perspective on the definition and legal framework on AI as well as a feasibility study, now underway, which reflects interests Japan embrace in identifying its future orientations on AI.

Moreover, Japan plans to create an agency dedicated to promoting digital transformation in fall 2021. In his Diet Policy speech in January 2021, Prime Minister Yoshihide Suga mentioned that he has set aside 1 trillion yen (approximately 8 billion euro) to enable digital transformation from administrative procedures to education. Suga also announced that for private sector companies, the government will support corporate digital investment with tax incentives. He stated that Japan plans 'to be a front runner in the digital arena by advancing research and development across the public and private sectors and also by leading global rule-making on telecommunication standards.'⁸ The Japanese Diet passed digital transformation bills in April 2021 to promote further digital transformation of Japan's administrative services and education.

Meanwhile, in her State of the Union in September 2020, Ursula von der Leyen, President of the European Commission stated that EU should 'lead the way on digitalisation and should not follow the way of others, who are setting standards for us.' She emphasised data, AI and infrastructure in promoting the digital age for the Union. She stated that the EU will take a 'coherent approach to connectivity and digital infrastructure development.'⁹

Further, in March 2021, the European Commission presented a vision and several avenues for Europe's digital decade up to 2030 entitled 'Digital Compass' with four principles of skills, infrastructures, business and government. Included in this vision is training for 20 million ICT specialists, digital

5 Ministry of Internal Affairs and Communications, 'Beyond 5G Promoting Strategy,' June 2020 available at https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/200414_B5G_ENG_v01.pdf last accessed on 1 April 2021. Further details are available in Japanese language at https://www.soumu.go.jp/main_content/000696613.pdf, as well as https://www.soumu.go.jp/main_content/000702111.pdf, last accessed on 1 April 2021.

6 Ministry of Internal Affairs and Communications, 'Beyond 5G suishin konso-siammu no tachiageni tuite[Launch of Beyond 5G Promotion Consortium,]' March 2021, available in Japanese language at https://www.soumu.go.jp/main_content/000736079.pdf, last accessed on 5 April 2021.

7 'Social Principles of Human-Centric AI, 15 February 2019, available at <https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/humancentricai.pdf> last accessed on 9 March 2021.

8 Yoshihide Suga, Policy Speech to the 204th Session of the Diet, 18 January 2021, the text is available at https://japan.kantei.go.jp/99_suga/statement/202101/_00013.html, last accessed on 3 March 2021.

9 Ursula von der Leyen, State of the Union, 'Building the World we must live in: A Union of Vitality in a World of Fragility,' 15 September 2020, the text is available at https://ec.europa.eu/info/sites/info/files/soteu_2020_en.pdf, last accessed on 3 March 2021.

transformation of businesses, secure and sustainable digital infrastructure and digitalisation of public services. The Digital Compass also embraces connectivity, including 5G everywhere. It plans to double the EU share of cutting-edge semiconductors in global production by the year 2030.¹⁰ On 19 March 2021, EU Member States announced declarations to promote international connectivity including the rollout of clean digital technologies, the improvement of the regulatory environment for start-ups and scale-ups to promote Europe's green and digital transformation.¹¹

Regarding AI, on 8 April 2019 the EU announced ethics guidelines for trustworthy AI which emphasise lawful, ethical and robust AI.¹² This proposal invited an open consultation which resulted in the final Assessment List for Trustworthy AI in July 2020. On 21 April 2021, the European Commission announced its proposal for a regulation establishing harmonised rules on artificial intelligence.¹³ The proposed rules limit improper use of data in order to protect democracy, rule of law and basic rights within the EU. The proposed regulations will affect businesses outside of the European Union and will need further coordination with other countries but represent an important step forward in securing trust for data transfer.

Ana Gascon Marcen, Assistant Professor at University of Zaragoza, observes that while the EU and Japan are losing the race on AI against the US and China they are now promoting AI and its governance. EU is implicating its Horizon Europe programme and Japan, its Moonshot program. The EU promotes Ethic Guidelines for Trustworthy AI and places its respect for human rights, the rule of law and democracy in AI.¹⁴

The above analysis reveals some commonalities in Japan's and the EU's approaches to a digital age. Both are explicitly aiming 'to lead rather than to be led' in digitalisation and in standards setting; Japan,

through its Society 5.0 vision, Beyond 5G Initiative and Digital Transformation laws, and the EU through its Digital Compass. While both Japan and the EU prioritise development of digital infrastructure and connectivity, it is notable that they take a human-centred approach. The digital age can improve our quality of life as envisaged in Society 5.0 but can also undermine people's safety and security if proper attention is not paid to protection of data: this may adversely affect privacy and human rights. With these commonalities in policy orientations in mind, Japan and the EU can foster digital development together with due protection of people and with proper bases for economic growth for their respective benefits and beyond. Both assert that the digital age must be developed alongside ethics.

3. Harnessing Digital Connectivity

Digital connectivity is frequently alluded to in official documents, articles and speeches. What does this term mean? It is used rather loosely to define digital infrastructure that connects people, business, communities and countries. The Japan-EU Partnership on Sustainable Connectivity and Quality Infrastructure signed on 27 September 2019 identified digital connectivity as 'a powerful enabler of inclusive growth and sustainable development, including digital and data infrastructure as well as policy and regulatory frameworks.' Furthermore, it acknowledges that digital connectivity is the base that digital economy depends on and includes 'an open, free, stable accessible, interoperable, reliable and secure cyberspace, and data free flow.'¹⁵

Moreover, digital and cyber are recognised as areas of strategic cooperation in the Strategic Partnership Agreement (SPA). Specifically, Article 21 on 'information society' stipulates the fostering of discussions on 'respective policies and regulations in the area of information and communications technologies to enhance cooperation on key issues, including electronic communications (internet gov-

10 The European Commission, 'Europe's Digital Decade: digital targets for 2030,' 9 March 2021, available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en, last accessed on 10 March 2021.

11 Press release by the European Commission and the Portuguese Presidency of the Council of the EU, 19 March 2021, the text is available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1186 last accessed on 20 March 2021.

12 'Ethics guidelines for trustworthy AI,' 8 April 2019, the text is available at 2019 EU's ethic guideline on trustworthy AI (<https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>), last accessed on 20 March 2021.

13 'The Commission has proposed rules on AI,' 21 April 2021, available at <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence> last accessed on 27 April 2021.

14 Ana Gascon Marcen, 'Society 5.0: EU-Japanese cooperation and the opportunities and challenges posed by the data economy,' 2 April 2020, available at http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/asia-pacific/ari11-2020-gascon-society-5-0-eu-japanese-cooperation-and-opportunities-and-challenges-posed-by-data-economy last accessed on 9 March 2021.

15 'The Partnership on Sustainable Connectivity and Quality Infrastructure Between the European Union and Japan,' signed in September 2019, paragraph 6.

ernance and online safety and security,) interconnection of research network, and standardisation and dissemination of new technologies.’ Furthermore Article 36, which concerns ‘cooperation on cyber issues’, stipulates that the EU and Japan ‘shall enhance the exchange of views and information on their respective policies and activities on cyber issues in international and regional areas.’ SPA encourages Japan and the EU ‘to cooperate in establishing norms and to promote confidence building in cyberspace.’

As Maaïke Okano-Heijmans, Senior Fellow at the Netherlands Institute for International Relations, Clingendael, argues that Japan and the EU, in harnessing digital connectivity between the two regions and beyond, we face a multitude of promises as well as challenges involving multiple stakeholders, including international organisations, governments, business and people. Okano-Heijmans has pointed out ‘the three practical elements of digital connectivity – namely, telecommunications infrastructure, business and regulation’¹⁶ – are intertwined and embrace a whole spectrum of challenges. Challenges we face today are further complicated by the balance we must strike between business potential digital technology offers and state and human security issues that can be undermined, depending on the reliability of communication networks and regulations. While there are whole range of aspects in digital connectivity, this paper examines cases of data governance, subsea cables and fifth-generation mobile network –5G-- to examine promises and challenges in harnessing digital connectivity.

Digital Silk Road

China has been advancing digital connectivity under the banner: Digital Silk Road (DSR) since 2015 as a part of its Belt and Road Initiative (BRI). In BRI, China initially focused on land and sea infrastructure: digital development came the third. However in 2021 China has prioritised its digital focus. Eurasia Group observed that China, through its promotion of DSR, encourages Chinese leading platform players such as Alibaba, Tencent and Baidu as well as Huawei and state-backed telecom carriers including China Mobile, China Telecom, and China

Unicom to promote exports of Chinese digital products and services. Chinese companies are competing in emerging markets with leading US companies in so-called over the top (OTT) services, including smart cities, cloud services, mobile payments and social media applications. It is argued that China ultimately aims to introduce Chinese standard technology including 5G to BRI countries so that ‘BRI countries will insist that China standards be adopted as global standards or be viewed as an advantage in international negotiation of standards.’¹⁷ China advances its technological independence at home while aiming to be a centre of global digital network under DSR.

This aggressive Chinese DSR has alarmed Japan, the EU and the US. Their companies will be operate at a disadvantage if China is successful in achieving their objective of seizing a leadership position on standards setting. Japan, the EU and the US will be compelled to adopt Chinese standards or to ensure parallel standards. Moreover, many people are concerned that data in DSR countries may be transferred to China through their surveillance network. As a matter of fact, the Chinese Cybersecurity Law in 2020 compels Chinese firms to surrender data when asked by the Beijing Government. Such an eventuality affects not only the economy but also the security of inhabitants The alternative would be for Japan and the EU, and, for that matter, the US and like-minded countries, to offer diverse digital connectivity options to those countries which need assistance on digital infrastructure.

Promoting Data Governance

‘The engine for growth is fuelled no longer by gasoline but more and more by data’¹⁸, argued Japan’s former Prime Minister Shinzo Abe¹⁹. And the key to digital connectivity is data flow. Data such as medical, industrial, traffic and other most useful, non-personal, anonymous information should flow freely and safely across borders. to promote economic activities. On the other hand, personal data, data embodying intellectual property, national security intelligence and people’s safety and privacy should be carefully protected.

16 Maaïke Okano-Heijmans, ‘The Case for EU-Japan digital connectivity and digital ODA,’ Elcano 20, 25 March 2020, available at <http://www.realinstitutoelcano.org/wps/wcm/connect/929a9c22-6664-4fa2-82ed-ec98c86f89d8/ARI30-2020-Okano-Heijmans-The-case-for+EU-Japan-digital-connectivity-and-digital-ODA.pdf?MOD=AJPERES&CACHEID=929a9c22-6664-4fa2-82ed-ec98c86f89d8> last accessed on 9 March 2021.

17 Eurasia Group, ‘The Digital Silk Road: Expanding China’s Digital Footprint,’ April 8th, 2020, available at <https://www.eurasiagroup.net/files/upload/Digital-Silk-Road-Expanding-China-Digital-Footprint-1.pdf> last accessed on 20 February 2021.

18 Speech by Prime Minister Shinzo Abe at the World Economic Forum Annual Meeting, ‘Toward a New Era of Hope-Driven Economy,’ 23 January 2019, the text available at https://www.mofa.go.jp/ecm/ec/page4e_000973.html last accessed on 3 March 2021.

19 Ibid., Shinzo Abe in January 2019.

As Maaïke Okano-Heijmans and Brigitte Dekker argue in their Clingendael Report in 2020, countries take diverging approaches to governing the cross-border movement of data, which sometimes even hampers the interoperability of systems. Data governance legislative frameworks must calculate the trade-off of privacy, business interests and state security. The US places priorities on business interests and stresses data free flow. China, on the other hand, prioritises state security.²⁰ The EU has emphasised privacy and has taken a human-centred approach as reflected in its General Data Protection Regulation (GDPR) that limits the transfer of personal data for protection with strong focus on ethics. As for data flow from the EU, a recipient country has to receive an adequacy decision from EU to make sure data flowing out from the EU is protected after the transfer.

Japan takes an approach in between the US and the EU. It regards data free flow as indispensable for digital economy and e-commerce but takes a human-centred approach to data protection through the Act on the Protection of Personal Information (APPI), which was revised in 2015 and further amended in 2020 and 2021. However, the inadequacy of personal data flow protection was revealed in the case of LINE corporation, a messaging app provider used by over 86 million people in Japan. It was revealed that LINE corporation's personal data had been accessed by technicians in China, without users being informed as required by the Law in March 2021.²¹ The Japanese APPI, revised in 2020 allows the overseas transfer of customers' personal information but requires providers to inform users which countries the data is transferred to. LINE corporation has entrusted a Chinese affiliate to develop artificial intelligence technologies and had allowed them to access to its database including users' names, phone numbers and email addresses along with their messages. The Line app has been widely used in Japan as a main social communications tool and is being used by local governments and other organisations in Japan as well as in Taiwan, Thailand and Indonesia. This LINE case revealed a

lack of personal data protection; this is to be further rectified.

Meanwhile, Japan has taken initiative on data governance. In preparing for the Osaka G20 summit, former Prime Minister Shinzo Abe stressed data governance in the Davos World Economic Forum Annual Meeting on January 23rd, 2019. He proposed a regime to be built, Data Free Flow with Trust (DFFT).²² At the side-lines of G20 Osaka Summit in June 2019, Japan, EU, US, China and 21 other states discussed the need for free flow of data with mutual trust. Prime Minister Abe launched 'Osaka Track' for DFFT. Leaders formally signed the Osaka Declaration on Digital Economy to work on international rule-making.²³ It is significant that data and data flow were highlighted for the first time in the G20 summit. DFFT ought to be developed by calculating the trade-offs between personal protection, business interest and state security. The 'T' in DFFT matters a great deal. Trust was identified as the prime enabler for free flow of data, highlighting the importance of interoperability.

Challenges for data governance are how to promote open, free and yet secure digital flow, how to reconcile the regulatory divergence among nations, how to fill the gap between incumbent regulations and new innovations and how to ensure enough convergence for interoperability. While large scale surveillance of human traffic was tolerated in 2020 for the purpose of halting infection from the COVID-19 virus, Yuval Noah Harari cautions the danger that could be caused by data flow; 'a large scale surveillance by digitalisation threatens our privacy and can open a way for unprecedented authoritarianism.'²⁴ Data flow, unless properly protecting privacy, can create a means for state surveillance of people as well as a political system. We need to find optimum equilibrium for data flow between economic growth and privacy protection, at the least.

Furthermore DFFT has to be discussed at a global level, most notably at the World Trade Organization (WTO) as was agreed in the Japan-EU Partnership on Sustainable Connectivity and Quality Infrastructure. Japan and the EU have agreed 'to promote

20 Brigitte Dekker and Maaïke Okano-Heijmans, 'Europe's Digital Decade?' Clingendael Report, October 2020, available at <https://www.clingendael.org/publication/europes-digital-decade>, last accessed on 21 March 2021.

21 'Personal data of LINE users in Japan disclosed to Chinese development firm,' The Japan Times, 17 March 2021. Available at <https://www.japantimes.co.jp/news/2021/03/17/business/corporate-business/line-data-shared-china/>, last accessed on 21 March 2021.

22 Speech by Prime Minister Shinzo Abe at the World Economic Forum Annual Meeting, 'Toward a New Era of 'Hope-Driven Economy,' 23 January 2019, the text available at https://www.mofa.go.jp/ecm/ec/page4e_000973.html last accessed on 3 March 2021.

23 Ministry of Foreign Affairs, 'Osaka Declaration on Digital Economy,' 28 June 2019, available at https://www.mofa.go.jp/mofaj/gaiko/g20/osa-ka19/pdf/special_event/en/special_event_01.pdf, last accessed on 3 March 2021.

24 Yuval Noah Harari, 'Korona ha kagaku ga sukuu, Seiji ha douka,' Nihon Keizai Shimbun, 9 March 2021.

international policy discussions, inter alia, international rule-making on trade-related aspects of electronic commerce at the WTO'.²⁵ The EU has been an outstanding norm entrepreneur. With Japan's initiative on DFFT as a precedent, Japan and the EU can lead data governance framework together, balancing better protection for privacy, intellectual property and cybersecurity vis-à-vis economic and social development. Such discussion ought to engage the US and, for that matter, China, which has also signed the DFFT and Osaka Track.

Constructing secure 5G networks and sub-sea cables

Data flow requires a conduit. Among digital infrastructure items to carry data, this paper examines mobile communication networks and subsea cables. Subsea cables carry over 95 % of transborder data traffic, and is thus called as the world's information super-highway.²⁶ The balance, that is 5%, is via satellites. Subsea cables excel over satellite communication in terms of communication capacity, speed and bandwidth. Around the globe, there are approximately 400 subsea cables worldwide, carrying videos, telephone calls, transactions for credit cards, ATMs and stock exchange transactions to be processed remotely.

In fact subsea cables have a long history, dating back to 1851 when the first subsea cable was laid under the Dover Strait. For Japan, it was in 1872 that subsea cable was first laid between Nagasaki and Shanghai which connected Japan to the international cable network. Over time, subsea cables have shown its geo-strategic face, in addition to its role of carrying information to its destination. Subsea cables have been subject to surveillance for critical strategic information often related to warfare. Although since 1980s, cable networks have used optical fibre, which is less susceptible to information leakage as opposed to copper, concern over data leakage surfaced prominently in 2013 when Edward Snowden, a former staff member of National Security Agency (NSA), disclosed top secrets to media and leaked NSA's Operation Upstream. This

incident sparked concerns over the safety of cyberspace including terrestrial and subsea cable as well as data centres. Furthermore when subsea cable is cut by accident or intentionally, it can disturb global communication, as happened in Egypt in 2013.

In the world market, as of 2020, ownership of subsea cables is approximately 90% by SubCom in the US, Alcatel Submarine Networks (ASN) in France, and NEC in Japan combined.²⁷ Meanwhile China's Huawei's subsidiary, Huawei Marine Systems, controls 10% of the market through the laying of more than 50,000 km of subsea cables across 90 projects.²⁸

Despite the current small Chinese share, owing to active project proposals on subsea cables under DSR, countries are increasingly concerned. Motohiro Tsuchiya, professor at Keio University, stated that China requests recipients of its assistance in subsea cable connection to purchase other equipment as a package including landing stations, data centres, 5G cell phones, conversation applications by WeChat or cashless payment systems such as Alipay. Through these aids to DSR countries, China is able to monitor people in BRI countries through their systems.²⁹ Moreover the Chinese Cybersecurity Law in 2020 compels Chinese firms to surrender data to the government whenever Beijing requests. This possible data surveillance is a strong concern.

Concerned with the possible surveillance of data through subsea cable networks, some countries have taken measures to alternate landing points of their respective subsea cable projects. For example, Pacific Light Cable Network (PLCN) by Google, Facebook and Dr. Peng Telecom & Marine Group was about to land subsea cables in Hong Kong which connects Los Angeles to Asia, the US inter-agency Team Telecom on 17 June 2020 advised against the plan, and the project decided not to do so, after the island's demonstrations over China's new National Security Law. PLCN eventually landed the subsea cable in the Philippines instead.

Countries are today more actively bidding for subsea cable projects in the Indo-Pacific and beyond.

25 The Partnership on Sustainable Connectivity and Quality Infrastructure Between the European Union and Japan, signed in September 2019, Paragraph 6, available at https://eeas.europa.eu/sites/eeas/files/the_partnership_on_sustainable_connectivity_and_quality_infrastructure_between_the_european_union_and_japan.pdf last accessed on 3 March 2021.

26 Jonathan E., Hillman, 'Securing the Subsea Network: A Primer for Policymakers,' CSIS, March 2021, available at <https://www.csis.org/analysis/securing-subsea-network-primer-policymakers>, last accessed on 10 March 2021.

27 Motohiro Tsuchiya, 'Kaitei Cable wo meguru Kokusai Kankei [International Relations over Submarine Cable],' Research Report, The Japan Institute of International Affairs, 29 September 2020, available at <https://www.jiia.or.jp/column/post-10.html> last accessed on 5 February 2021.

28 Vlad Savov, 'Huawei is selling off its undersea cable business,' The Verge, 3 June 2019. Available at <https://www.theverge.com/2019/6/3/18650220/huawei-undersea-cable-business-sale-trump-ban-smartphone-production> last accessed on 20 February 2021.

29 Kazuya Omuro 'Kaitei Cable de Okita Beichu no Haken Arasoi,' Asahi Shimbun Globe, 1 November 2020, available at <https://globe.asahi.com/article/13885191> last accessed on 24 February 2021.

In July 2020 Chile announced that it has chosen Japan and its NEC for its first undersea fibre-optic trans-Pacific cable to connect South America and the Asia Pacific through Australia. This proposal takes advantage of the existing cable link between Japan and Oceania. Other European and American companies will join in the project.³⁰ In January 2021, Ellalink announced that its subsea cable network will connect Latin America and Europe with the next generation low-latency submarine cable system which will be operational in the second quarter of 2021³¹.

In addition to these projects led by Japanese and European companies, like-minded countries are now acting in tandem to assist countries in need of new subsea cable networks. As an illustration, in the Indo-Pacific, Japan, Australia and the US signed an agreement to finance the Palau subsea cable project in January 2021. The project is the very first case to be conducted under 'the Trilateral Partnership for Infrastructure Investment in the Indo-Pacific' between Japan, Australia and the United States. Hence, it will be a symbolic project of the trilateral cooperation for their pursuit of the Free and Open Indo-Pacific³². Similar undertakings can be made with Europe, which will make digital connectivity robust.

While faults to subsea cables are mainly caused by fishing and shipping activities including anchorage³³, a possible cyberattack is a concern. Jonathan E. Hillman, Senior Fellow of Center for Security and International Studies (CSIS) argues in his report that hardened landing stations and physically-secured equipment in stations are required. In order to prepare for possible faults, backup power supplies and other redundant components are required to protect data integrity.³⁴ While subsea cables and

their landing stations are planned, developed and operated by the private sector, like-minded countries ought to consider how they can protect data in transit in order to reduce risks. Hillman also advises that governments can use their licenses as a means for security. In fact, while there are institutions such as International Cable Protection Committee (ICPC) and International Telecommunications Union (ITU), there is no dedicated intergovernmental mechanism to oversee subsea cables.³⁵

Against the backdrop of active exports of subsea cables along with landing stations and related terrestrial equipment under the banner of DSR, Japan, EU, the US and like-minded countries should consider further funding for digital connectivity to assist countries in need. Also Official Development Assistance (ODA) rules for digital infrastructure including technical assistance and capacity building assistance are essential.

Fifth-generation mobile network – 5G and beyond

Closely related to subsea cable is the fifth generation mobile network – 5G. In Japan the first mobile system was commercialised in 1970. Fifty years later in March 2020, the fifth-generation mobile communication system, 5G, launched its commercial service. Data traffic volume has phenomenally expanded by an annual growth of approximately 20%, due to larger content sizes, the growth of IoT devices, and further digitalisation.³⁶ Due to the globalisation of business activities and growing transnational services through Internet, JETRO reported in 2018 that aggregate transborder data traffic has grown by 165 times from 2001 to 2016.³⁷ As of 2020, Huawei controlled 28 % of the overall telecom market.³⁸ The Trump administration pressured its partners

30 'Chile picks Japan's trans-Pacific cable route in snub to China,' Nikkei Asia, July 29th, 2020, available at <https://asia.nikkei.com/Business/Telecommunication/Chile-picks-Japan-s-trans-Pacific-cable-route-in-snub-to-China>, last accessed on 30 March 2021.

31 Ellalink, 'Ellalink's transatlantic submarine cable has already anchored in Portugal,' January 6th, 2021, available at <https://ella.link/2021/01/06/ellalinks-transatlantic-submarine-cable-has-already-anchored-in-portugal/>, last accessed on 21 March 2021.

32 Ministry of Foreign Affairs, 'Signing Ceremony for Palau Submarine Cable Project,' available at https://www.palau.emb-japan.go.jp/itpr/en/11_000001_00166.html, last accessed on 17 February 2021.

33 Alan Mauldin, 'Cable Breakage: When and How Cables Go Down,' TeleGeography, 3 May 2017.

34 Jonathan E., Hillman, 'Securing the Subsea Network: A Primer for Policymakers,' CSIS, March 2021, available at <https://www.csis.org/analysis/securing-subsea-network-primer-policymakers>, last accessed on 10 March 2021.

35 Kazuya Omuro 'Kaitei Cable de Okita Beichu no Haken Arasoi,' Asahi Shimbun Globe, November 1st, 2020, available at <https://globe.asahi.com/article/13885191> last accessed on 24 February 2021. Also Jun Murai, 'Nihonjin ga Shiranai Taiheiyō no Kaitei Meguru Fukai Jijyo,' Toyo Keizai Online, API Chikeigaku Briefing, 25 January 2021. Available at <https://toyokeizai.net/articles/-/406082> last accessed on 28 February 2021.

36 Ministry of Internal Affairs and Communication, 'The White Paper on Information and Communications in Japan 2020,' p.30, available at https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/whitepaper/index.html last accessed on 1 April 2021.

37 JETRO, 'Kyuzousuru Sekai no Data Ryutsuryō [Rapidly growing world data traffic,' 2018, available at <https://www.jetro.go.jp/biz/areareports/2018/380fd5f0d9c4bb4d.html>, last accessed on 2 April 2021.

38 Jonathan E. Hillman, Laura Rivas, 'Global Networks 2030,' CSIS, March 2021, p.13.

and allies not to use Huawei products or technology. As an illustration, Mike Pence, then US Vice President, said during his speech at the annual Munich Security Conference in 2019 that ‘we must protect our critical telecom infrastructure, and the United States is calling on all our security partners to be vigilant and to reject any enterprise that would compromise the integrity of our communications technology or national security systems.’³⁹ This US policy has compelled US allies and partners to debate whether they should include or exclude 5G products provided by Chinese vendors, most notably Huawei. The concern about Chinese products increased particularly after China introduced the Cybersecurity Law 2020, that compels Chinese firms to surrender data to the government whenever Beijing requests it. Australia has taken the lead in excluding Huawei and has subsequently faced coercive measures by China. In January 2020, the European Commission recommended that member states ‘avoid dependency on suppliers considered to be high-risk.’ Each state responded in a varied manner, from exerting an all-out ban to imposing a restricted ban on core components.

As an illustration, in the Netherlands, Huawei controlled over 9% of the Dutch mobile phone market share in September 2020. The Clingendael Institute’s Foreign Affairs Barometer survey reported in December 2020 that over 41% of people in the Netherlands polled disagree with the statement ‘I’d rather not have a Chinese phone, because the Chinese government could use it to spy on me.’ Meanwhile, around 27% agreed with the statement. However, in the survey on telephone networks, 43% said ‘no’ to Chinese network infrastructure, due to security concerns. One can observe a clear distinction between mobile phones and networks by the public. The Dutch government in December 2020 decided that ‘the buildout of the 5G network should include comprehensive security and supervision of network equipment.’⁴⁰

The Japanese government has not banned technology by any specific country or vendor. In allocating a 5G spectrum in April 2019, vendors have been asked to ensure the cybersecurity of their 5G services. Some observe this policy as a de facto exclu-

sion of Chinese vendors. However, it is a solid fact that one can still purchase Huawei smartphones in Japan. Mihoko Matsubara, Chief Cybersecurity Strategist of NTT Corporation, points out that 5G has triggered a heavy debate because there are a limited number of vendors, causing ‘vendor lock-in.’ Instead of exclusion, Matsubara argues that Japan has adopted a policy to facilitate more competition in 4G and 5G, taking cross-vendor approach.⁴¹ The Japanese government in 2020 and 2021 offers tax incentives to support network service providers to invest in 5G infrastructure. This approach also reduces supply-chain risks. As of March 2021, Sony Mobile, Sharp, NEC and Fujitsu offer 5G smartphones in Japan. In addition, Apple, Samsung and LG from the Republic of Korea and Huawei, ZTE, OPPO and Xiami from China are also selling their products in Japan. Thus, there are smartphone options for people to choose from.

In addition to the aforementioned Japanese government initiatives on ‘Beyond 5G,’ business alliances are underway for 5G. In June 2020, NTT and NEC have unveiled an alliance to develop equipment for 5G base stations in compliance with Open Radio Access Network (O-RAN) and to cooperate on high-quality and low-cost information technology products, such as digital signal processor chips. What is O-RAN? It ‘refers to a disaggregated approach to deploying mobile networks by using open and interoperable protocols and interfaces. It is an alternative way of building communications networks that consists of radio frequency spectrum, towers, base stations and mobile devices to deliver mobile connectivity. It allows for increased flexibility over traditional RAN systems which are limited to proprietary software and hardware’⁴². Thus O-RAN can be implemented with vendor-neutral hardware and software-defined technology based on open interfaces and industry-developed standards. Global coalitions are effective for establishing international standards for a multi-vendor approach. Japanese network service providers are members of the O-RAN Alliance. Cybersecurity Strategist Matsubara argues that these coalitions are key to adopting international standards for the interface between

39 Vice President Pence Remarks at 2019 Munich Security Conference, C-Span, 16 February 2019, available at <https://www.c-span.org/video/?458010-1/vice-president-pence-calls-allies-withdraw-iran-nuclear-deal> last accessed on 30 March 2021.

40 Clingendael, ‘Telephones yes, networks no,’ December 2020, available at https://www.clingendael.org/sites/default/files/2021-02/Barometer_Alert_China_Dutch_Attitudes_2020.pdf, last accessed on 21 March 2021.

41 Mihoko Matsubara, ‘Japan’s 5G Approach Sets a Model for Global Cooperation,’ Lawfare, 14 September 2020, available at <https://www.lawfareblog.com/japans-5g-approach-sets-model-global-cooperation>, last accessed on 1 March 2021.

42 Jonathan E. Hillman, Laura Rivas, ‘Global Networks 2030,’ CSIS. March 2021, p.12.

different components of radio access networks in order to ensure the flexible combination of RAN units, make the interface open to multiple vendors and avert 5G vendor lock-in.⁴³ European operators announced Open RAN deployment in the United Kingdom, Germany, France, Spain and Brazil.⁴⁴

Furthermore new alliances within the industry are underway for beyond 5G. NTT has launched a project on Innovative Optical and Wireless network (IOWN) which is an innovative end-to-end communication infrastructure with full stack acceleration, all photonics and wireless network for 6th generation mobile network, to be available around 2030.⁴⁵ In October 2019, Sony, NTT and Intel launched IOWN Global Forum in the United States to develop a network. As of January 2021, Ericsson, NVIDIA and others have joined the Forum.⁴⁶

A debate is in progress over whether to exclude a specific country's 5G telephone or network or include it, with some conditions. This may eventually lead to dual standards, one by China and the other by the US, the EU and Japan. If a dual standard is established, other countries may not be able to provide their products to DSR countries. Eurasia Group argues that this may also lead to the export of a Chinese techno-authoritarian model to DSR countries.⁴⁷

In November 2019, Japan, Australia and the US announced the Blue Dot Network to promote high-quality, trusted standards for global infrastructure development in an open and inclusive framework. The Blue Dot Network evaluates and certifies nominated infrastructure projects based on adherence to commonly accepted principles and standards that promote market-driven, transparent and financially sustainable infrastructure development in the Indo-Pacific region and around the world. This initiative combined with private sector alliances on development of 5G and beyond may allow us

to go beyond the realm of vendor lock-in. It is time for liberal cooperation for digital connectivity.

On 16 April 2021, at the Japan-US Summit meeting, Prime Minister Suga and President Biden 'affirmed their commitment to the security and openness of fifth generation wireless networks... The United States and Japan will engage with others through our enhanced Global Digital Connectivity Partnership'.⁴⁸ In the Fact Sheet on US-Japan Competitiveness and Resilience (CoRe) Partnership adopted at the Japan US Summit meeting, they also agreed to strengthen their cooperation in developing, testing and deploying secure networks and advanced ICT, including 5G and next-generation mobile networks.⁴⁹ When Japan, the US and Europe join hands on digital connectivity, it will make connectivity robust and sound.

4. Conclusion: Enhancing digital connectivity with trust

If we fail to secure trustworthy digital connectivity, people's lives will certainly be threatened. If 5G network base stations have a backdoor, high precision image information for military use, for example, can be leaked, which would undermine state and human security. On the other hand, if we fail to secure robust and stable digital connectivity, data essential for economic and human activities would not be available, which would be detrimental to economic and human activities.

The above brief analysis reveals complex and diverse challenges concerning digital connectivity. While we rely heavily on digital means such as the Internet, and have done so particularly during the COVID 19 pandemic, it is crucial to improve computing capacity, to reduce power consumption and to minimise latency in order to ensure stable data transmission and to stay connected. Digital technology has changed the nature of interdepen-

43 Ibid., Matsubara.

44 Ibid., Hillman. p.13.

45 Shigeru Iwashina, Yosuke Aragane, Kunihiko Minamihata, Katsuji Shindo, Masakatu Fujiwa, 'IOWN Koso Jitugen ni Muketa Torikumi [In realizing IOWN]' NTT Gijutu Journal, January 2020. Available at <https://journal.ntt.co.jp/wp-content/uploads/2020/05/JN20200134.pdf>, last accessed on 31 March 2021.

46 'Sanka Kigyo ni Ondosa. NTT no Daitan sugiru IOWN Koso [Temperature differences among companies joining IOWN Initiative,]' Nikkei Tech, 3 February 2021.

47 Eurasia Group, 'The Digital Silk Road: Expanding China's Digital Footprint,' April 8th, 2020, available at <https://www.eurasiagroup.net/files/upload/Digital-Silk-Road-Expanding-China-Digital-Footprint-1.pdf> last accessed on 20 February 2021.

48 Ministry of Foreign Affairs (Japan), 'U.S. – Japan Joint Leaders' Statement,' 16 April 2021, available at <https://www.mofa.go.jp/mofaj/files/100177718.pdf>, last accessed on 22 April 2021.

49 The White House, 'Fact Sheet: US-Japan Competitiveness and Resilience (CoRe) Partnership', 16 April 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/fact-sheet-u-s-japan-competitiveness-and-resilience-core-partnership/> last accessed on 22 April 2021.

dence. Digital infrastructure offers opportunities for people, communities and businesses to take full advantage of convenience offered. Yet as people rely more heavily on digital communication, digital connectivity must be robust with fail safe mechanisms of redundancy so as not to suddenly disrupt people's lives, be it through subsea cable or mobile networks. In addition, digital connectivity must not rely solely on one conduit, that of a certain political system or ideology nor permit data surveillance to undermine human rights and privacy.

Technological advances beyond the 5G world should be designed for the ultimate benefit of people. For that, a compartmentalised approach is no longer tenable. In the 2020s, geo-economics and geo-politics can no longer be discussed in separate domains but must be addressed together. Economic statecraft is one element of such discussions. Digital connectivity demands engagement of multiple stakeholders from people, communities, businesses, states and multilateral institutions. Business and governments must spearhead technological advances to avoid vendor lock-in as experienced in 5G and to promote cross vendor approach. That will allow us to avoid the politico-economic challenges of including or excluding a specific vendor in one's network. Governments must also be in sync with the technological trend up front, to achieve convergence of a global governance regime including standardisation for interoperability of systems and a calculation of the trade-offs among human security, business interests and national security.

It should be noted that while Japan, Europe and the US enjoy access to digital infrastructure that allows people to continue working, learning, shopping, playing and talking with family and friends, nearly half of the world's population still does not have access to the Internet. Advanced countries should assist those that lack digital connectivity to improve their choices. It is incumbent on Japan, Europe and the US to breach the digital divide and to offer viable alternatives.

As discussed in this paper, Japan and the EU have some commonalities in their approaches to a digital decade in the 2030s. They both intend to advance technology as leaders, not followers. They are willing to set norms and standards of digital connectivity as exemplified by Japan's leadership on DFFT, where 'T' matters. They also take a human-centred approach for the digital age, with people in mind as the ultimate beneficiary, and with determination to protect universal values. Japan and the EU can take advantage of opportunities offered by the dig-

ital age and capitalise on their norm-setting initiatives with converging common values. As actors sharing values and principles, they can promote liberal cooperation befitting to a digital age strengthened by existing agreements. For developing trustworthy digital connectivity in the future, they, along with like-minded countries, can together build open, free, and safe digital connectivity that ensures human security and dignity.

The Global Governance Programme

The Global Governance Programme (GGP) is research turned into action. It provides a European setting to conduct research at the highest level and promote synergies between the worlds of research and policy-making, to generate ideas and identify creative and innovative solutions to global challenges. The Programme is part of the Robert Schuman Centre for Advanced Studies of the European University Institute, a world-renowned academic institution. It receives financial support from the European Commission through the European Union budget. Complete information on our activities can be found online at: globalgovernanceprogramme.eui.eu

Robert Schuman Centre for Advanced Studies

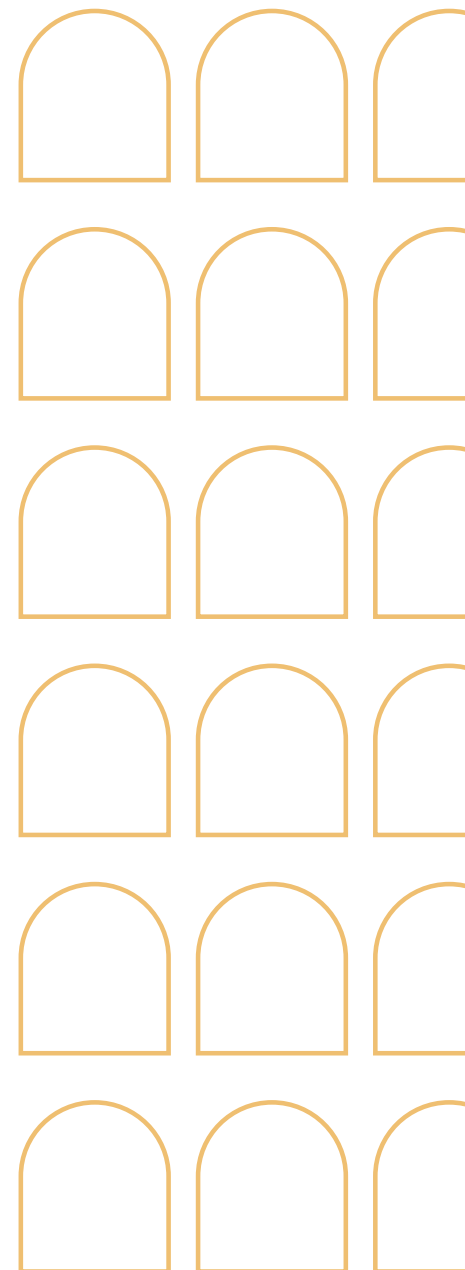
The Robert Schuman Centre for Advanced Studies (RSCAS), created in 1992 and directed by Professor Brigid Laffan, aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics. The Centre is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and ad hoc initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

www.eui/rsc



Co-funded by the
Erasmus+ Programme
of the European Union

Views expressed in this publication reflect the opinion of individual authors and not those of the European University Institute or the European Commission.
© European University Institute, 2021
Content © Akiko Fukushima.



doi:10.2870/780739
ISBN:978-92-9084-989-6
ISSN:2467-4540
QM-AX-21-023-EN-N