THE DIGITAL DECADE:
THE EU, PARTNERSHIPS AND GOVERNANCE IN THE INDO-PACIFIC

CSDS IN-DEPTH REPORT

DECEMBER 2022

RALUCA CSERNATONI
RAMON PACHECO PARDO

VUB BRUSSELS SCHOOL OF GOVERNANCE
CENTRE FOR SECURITY, DIPLOMACY AND STRATEGY

The Indo-Pacific Futures Platform

Funded by the European Union

THE DIGITAL DECADE: THE EU, PARTNERSHIPS AND GOVERNANCE IN THE INDO-PACIFIC

CSDS IN-DEPTH

DECEMBER 2022

RALUCA CSERNATONI
RAMON PACHECO PARDO

Funded by the European Union

The Indo-Pacific Futures Platform

This publication has been prepared with the financial assistance of the European Union. The views expressed herein are those of the research team and therefore do not necessarily reflect the official position of EU institutions

VUB
BRUSSELS SCHOOL OF GOVERNANCE
CENTRE FOR SECURITY, DIPLOMACY AND STRATEGY

TABLE OF CONTENTS

Abstract

The geopolitical and geoeconomic weight of the Indo-Pacific region is expanding at an unprecedented rate. The region has become both the epicentre of global power dynamics and home to fast growing and vibrant digital ecosystems. From digital trade, investments in innovation, connectivity partnerships, critical infrastructures, supply chains, and data flows, the Indo-Pacific is likely to impact global digitalisation megatrends across businesses and societies. The European Union and the Indo-Pacific are highly interconnected. This report aims to assess the role of digital governance and partnerships in the EU's Indo-Pacific Strategy and to understand whether there is a pan-Indo-Pacific digital governance and cybersecurity framework.

To this end, this report maps the architecture of digital governance initiatives in the Indo-Pacific and it examines the EU's engagements in the region and potential digital governance synergies. Additionally, the report zooms in on cybersecurity in the Indo-Pacific and the EU's approach, and it proposes seven recommendations for the EU's promotion of multilateralism and (digital) partnerships in the Indo-Pacific. Overall, the report observes that, for the EU to become a stronger digital and cybersecurity actor in the region, it should take a holistic and cross-sectoral approach to digital governance and cybersecurity. The Union should also help develop critical infrastructures and get involved in a wide range of issues, including supply chain resilience, critical infrastructure, data governance, and digital trade. It is further recommended that the EU should work closer together with the largest number of like-minded partners as possible, but especially Australia, Japan, New Zealand, Singapore, and South Korea.

EXECUTIVE SUMMARY

The geopolitical and geoeconomic weight of the Indo-Pacific region is expanding at an unprecedented rate. The region has become both the epicentre of global power dynamics and home to fast growing and vibrant digital ecosystems. From digital trade, investments in innovation, connectivity partnerships, critical infrastructures, supply chains, and data flows, the Indo-Pacific is likely to impact global digitalisation megatrends across businesses and societies. The European Union and the Indo-Pacific are highly interconnected.

As a relative newcomer in the geopolitical vocabulary, the Indo-Pacific region has become central to the EU, with many shared interests with like-minded actors regarding digital governance and partnerships, particularly in areas related to digital agreements, securing technology and information flows, and human-centric digital transformation. In recent years, the EU has made it a priority to expand its bilateral and multilateral engagements in the region, and with key partners such as Australia, Japan, New Zealand, Singapore, and South Korea.

Against this background and by building on the 2021 EU Strategy for Cooperation in the Indo-Pacific, this report starts by first mapping the architecture of digital governance initiatives in the Indo-Pacific; second, it examines the EU's engagements in the region and potential digital governance synergies; third, the analysis zooms in on cybersecurity in the Indo-Pacific and the EU's approach; and fourth, it proposes recommendations for future steps in terms of the EU's promotion of multilateralism and (digital) partnerships in the Indo-Pacific. Special consideration is given to the EU's expanding network of digital partnerships agreements with Indo-Pacific partners, the implementation of connectivity partnerships, and strengthening cooperation on research and innovation and regarding cybersecurity concerns.

In doing so, the report aims to assess the role of digital governance and partnerships in the EU's Indo-Pacific Strategy to understand whether there is a pan-Indo-Pacific digital governance and cybersecurity framework. While the EU has been developing its institutional, regulatory, and normative frameworks to address the challenges of the digital transition and the impact of emerging technologies, including the risks and threats emanating from cyberspace, the Indo-Pacific region is far away from developing a multilateral digital governance framework. More broadly, given the diversification of global supply chains in high-tech sectors to countries other than China, this is an opportunity for the EU to boost investments in other Indo-Pacific economies and expand into these markets.

Furthermore, and also following from these megatrends, it is unclear whether Indo-Pacific digital governance can become reality. Cybersecurity standards and data protection in the Indo-Pacific are also fragmented and countries differ over how they approach questions related to national security with regard to surveillance-driven versus openness-led models. Given such challenges, how should the EU adapt its digital and cybersecurity strategies in the Indo-Pacific, and what bilateral cooperation formats and multilateral institutional fora should it prioritise going forward until the 2030s?

Considering the above dynamics, the report proposes seven recommendations to the EU moving forward in order to strengthen its position in the digital governance of the Indo-Pacific. For the EU to become a stronger digital and cybersecurity actor in the region, it should take a holistic and cross-sectoral approach to digital governance and cybersecurity. Connectivity cooperation to develop critical infrastructures is another forward-thinking and pragmatic approach to engage in the region, alongside principled efforts to establish multilateral dialogue on digital norms and standards. The EU should get involved in a wide range of issues including supply chain resilience, critical infrastructure, data governance, and digital trade. It is further recommended that the EU should work closer together with the largest number of like-minded partners as possible, but especially Australia, Japan, New Zealand, Singapore, and South Korea.

While EU-led multilateral cooperation should be encouraged, the Union will need to prioritise bilateralism over multilateralism, when necessary, since digital governance in the Indo-Pacific region is very unlikely to become multilateral for the foreseeable future. One constructive and pragmatic area of both bilateral and multilateral engagement is capacity building in the region. Accordingly, the EU should support effective capacity building in the Indo-Pacific, bilaterally or together with third parties, such as Japan, Singapore, or South Korea. Furthermore, there is a demand in South and Southeast Asia for this type of productive cooperation, focusing on areas such as critical infrastructure building, digital connectivity, data governance framework development, digital trade facilitation, or research and development projects.

INTRODUCTION

Digital governance and partnerships are one of the seven priority areas of the EU's Strategy for Cooperation in the Indo-Pacific. Indeed, with the launch of the EU and Japan digital partnership in May 2022, Japan has become the first partner country with which the EU has formed a digital partnership.[1] The EU and the Republic of Korea (RoK, hereafter South Korea) enhanced their bilateral cooperation agenda in the digital sector with the 2022 EU-South Korea Digital Partnership, complementing South Korea's decision to start discussions to become an associated member of the 2021-2027 Horizon Europe Framework Programme. Moreover, following the agreement to strengthen bilateral digital trade in December 2021, the EU and Singapore signed a Digital Partnership in December 2022.

Noteworthy is the fact that the EU's digital partnership frameworks put forward a comprehensive bilateral instrument going beyond dialogue and exchanges towards delivering concrete deliverables on digital issues in line with the Digital Compass:[2] from fostering economic growth to focusing on human-centric digital transformation to building the resilience of global supply chains and data infrastructures to strengthening digital connectivity[3] and interoperability between digital markets, to name a few.

The closely related area of digital connectivity is another one of these priorities.[4] In this respect, the end goal is to foster meaningful connectivity in the region, which is more than digital infrastructures and technologies. Rather it is about "secure, resilient and responsible"[5] digital infrastructures, centred around norms and standards for trusted connectivity. This equally underscores the centrality that the EU affords to the digital domain as part of its strategy to become a more central actor to Indo-Pacific geoeconomics and geopolitics, by linking the digital trajectories and future of the EU and the region. Digital governance in the Indo-Pacific is intrinsically linked to the digital economy, high-tech innovation, trusted connectivity,[6] and trade, as well as to (cyber) security. Therefore, digital governance and concomitant partnerships cannot be circumscribed to any particular area. Due to their cross-cutting nature, they encompass all aspects of the EU's strategy towards the Indo-Pacific.

1 European Commission, 'Japan-EU Digital Partnership – Factsheet', 12 May 2022, https://digital-strategy.ec.europa.eu/en/library/japan-eu-digital-partnership-factsheet.
2 European Commission, 'Europe's Digital Decade: Digital Targets for 2030', accessed 18 November 2022, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.
3 European Commission, 'Joint Communication to the European Parliament and the Council: The EU Strategy for Cooperation in the Indo-Pacific' (JOIN[2021] 24 final), 16 September 2021, https://www.eeas.europa.eu/sites/default/files/jointcommunication_2021_24_1_en.pdf.
4 Christina Stansell, Fabial Hohmann, and Elisabeth Gager, 'Digital Connectivity and Opportunities for Development Cooperation between Asia and Europe', AESCON Policy Brief Series, April 2022, 9, https://www.aescon.org/wp-content/uploads/2022/10/AESCON-PB-04-FINAL.pdf.
5 'Digital Connectivity and Opportunities for Asia and Europe', AESCON, accessed 18 November 2022, https://www.aescon.org/.
6 Priyadarshini D., 'Putting Trust Back in Trusted Connectivity: A Call for More Congruence in Cross-Border Data Transfer', AESCON Policy Brief Series, April 2022, https://www.aescon.org/wp-content/uploads/2022/10/AESCON-PB-03-final.pdf.

As the global centre of gravity is fast moving towards the Indo-Pacific, the region and the EU should become natural partners by building strong and lasting cooperation on matters related to the digital agenda, the governance of emerging disruptive technologies (EDTs), and cyber policy. The "Indo-Pacific" is equally a relatively recent geopolitical construct intended to capture various issues, from regional institution-building, the rule of law, geostrategic balancing against the rise of China, to securing (digital) technology and information flows. Concerning the latter, the region accounts for the largest and fastest growing base of Internet users across the globe; a booming digital ecosystem encompassing cutting-edge fintech and e-commerce applications; increased efforts to boost homegrown digital and data governance solutions; and enhanced efforts to promote secure digital connectivity, digital spaces, and e-services. Relatedly, there has also been a quest for domestic and regional alternatives to the evolving geopolitical rivalry and tech race between the United States and China, exacerbated by the Covid-19 pandemic and further manifested in escalating trade wars and critical supply chain disruptions such as in the case of semiconductors.

The starting point of any evaluation about the role of digital governance and partnerships in the EU's Indo-Pacific Strategy is to understand whether there is a pan-Indo-Pacific digital governance and cybersecurity framework, but both remain elusive at the time of writing. This is also the case at the global level. However, the EU has managed to develop its own internal digital governance framework, the Digital Agenda for Europe for the decade 2010-2020,[7] and is working to implement the 2020 EU's Cybersecurity Strategy in the Digital Decade.[8] The EU has been developing its institutional, regulatory, and normative frameworks to address the challenges of the digital transition and the impact of EDTs such as artificial intelligence (AI), including the risks and threats emanating from cyberspace.

In sharp contrast, the Indo-Pacific region is far away from developing a multilateral digital governance framework. Countries in the region seem to be divided between those prioritising consumer protection and data privacy, as the EU itself does; openness and the free flow of data, which the US is trying to promote in the region; and national sovereignty and local data storage, the approach preferred by China.[9] Countries in the Indo-Pacific region seem to be torn between strengthening digital connectivity or focusing on resilience, and this affects the way in which they approach digital governance. Indeed, and in line with geo-economic megatrends in the Indo-Pacific, countries in the region are being pulled into two opposite directions: further state-led and market-driven integration also including China or US-fostered (potential) partial decoupling from China.[10] More broadly, given the diversification of global supply chains in high-tech sectors away from China, this is an opportunity for the EU to boost investments in other Indo-Pacific economies and expand into these markets. Furthermore, and also following from these megatrends, it is unclear whether Indo-Pacific digital governance can become reality. So far, the different efforts at creating a framework for the region seem to have focused on either the Asia-Pacific or East Asia. This seems logical when considering the decades-long tension in the region when it comes to the development of trade and economic agreements.

7 European Parliament, 'Digital Agenda for Europe', accessed 18 November 2022, https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe.
8 European Commission, 'The EU's Cybersecurity Strategy in the Digital Decade', 16 December 2020, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade.
9 According to UNCTAD, Japan, Malaysia, New Zealand, South Korea, or Thailand would be closer to the EU's approach; Australia, Philippines, or Singapore would be closer to the US's approach; and India, Indonesia, and Vietnam would be closer to China's approach. See UNACTAD, 'Digital Economy Report 2021. Cross-border Data Flows and Development: For Whom the Data Flow', accessed 18 November 2022, https://unctad.org/page/digital-economy-report-2021.
10 Ramon Pacheco Pardo, 'Geo-economic Megatrends in the Indo-Pacific: Integration or (Partial) Decoupling?' CSDS Policy Brief, 17 September 2021, https://brussels-school.be/sites/default/files/CSDS%20Policy%20brief_2117.pdf.

Cybersecurity standards and data protection in the Indo-Pacific are also fragmented and countries differ over how they approach questions related to national security with regard to surveillance-driven versus openness-led models. When it comes to the People's Republic of China, in the past few years it has upgraded its cybersecurity data protection legal efforts,[11] notably with the promulgation in 2016 of the Cybersecurity Law, and in 2021 of the Personal Information Protection Law and the Data Security Law. Such legislative efforts have had substantial effects on data flows within China and may impact other countries with close digital ties to China. China's cybersecurity and data protection architecture primarily serves to "regulate the relationship between large technology companies and consumers, as well as prevent cyber crime", yet it does not impose meaningful constraints for the collection and use of data by the state. This approach has been labelled as a "third way"[12] between the privacy-driven EU approach to data protection and the market-oriented US model.

Conversely, Japan's data protection law, the Act on the Protection of Personal Information (APPI),[13] was adopted as early as 2003 and was one of the first data protection regulations in Asia. After receiving substantial revisions in 2015 and 2020, the amended APPI imposed wider obligations on data transfers, specifically regarding offshore entities, and on the handling of data breaches. The new amendments that entered into force in April 2022 closely aligned the APPI to the EU's General Data Protection Regulation (GDPR), especially by expanding the scope of Japanese data subjects' rights and restricting the range of personal information that can be shared with third parties. South Korea's main law and regulations on data protection are enshrined in the 2011 Personal Information Protection Act,[14] which were further amended in 2020. They cover the collection, usage, disclosure, and other processing practices of personal information by both public and private entities and individuals throughout the lifecycle of handling personal data.

With respect to these regulatory regimes, the "data" is in the details. In other words, while the data privacy landscape has fast evolved in the Indo-Pacific, the challenges to data protection, cybersecurity, and safety are never straightforward, due to obstacles related to different interpretations of the concept of "privacy", the efficacy and flexibility of such laws, their cross-border application, and differing definitions of data breach notification requirements.

In order to unpack such dynamics, the report starts by first mapping the baroque architecture of digital governance initiatives in the Indo-Pacific; second, it examines the EU's engagements in the region and potential digital governance synergies; third, the analysis zooms in on cybersecurity in the Indo-Pacific and the EU's approach; and fourth, it proposes recommendation for future steps in terms of the EU's promotion of multilateralism and (digital) partnerships in the Indo-Pacific.

11 Rogier Creemers, 'China's Emerging Data Protection Framework', Journal of Cybersecurity 8, no. 1 (24 August 2022): 1, https://doi.org/10.1093/cybsec/tyac011.
12 Emmanuel Pernot-Leplay, 'China's Approach on Data Privacy Flaw: A Third Way between the US and the EU?' Penn State Journal of Law & International Affairs 8, no. 1 (May 2020): 49–117.
13 DataGuidance, 'Japan – Data Protection Overview', accessed 18 November 2022, https://www.dataguidance.com/notes/japan-data-protection-overview.
14 DataGuidance, 'South Korea – Data Protection Overview', accessed 18 November 2022, https://www.dataguidance.com/notes/south-korea-data-protection-overview.

DIGITAL GOVERNANCE IN THE INDO-PACIFIC

There are several overlapping initiatives in the Indo-Pacific region competing to set the principles and standards to underpin digital governance, as well as, to an extent, cybersecurity. Arguably, it was the Asia-Pacific Economic Cooperation (APEC) that first sought to develop a framework in this domain. Already in 2002, APEC members endorsed a Cybersecurity Strategy. Over the years, APEC has launched different initiatives.[15] Eventually this led to the adoption of an Internet Digital Economy Roadmap first discussed in 2014 and finally adopted in 2017.[16]

Among its better-known initiatives, APEC has a Cross-Border Privacy Rules (CBPR) System allowing for certified firms to transfer data across borders.[17] So far, APEC initiatives have adopted a model somewhere between the EU's and China's. But it should be noted that only CBPR is binding ¬– at least in theory – even though there are no effective enforcement mechanisms. As a result, in May 2022 the US led a group of nine APEC members also including Japan, Singapore, and South Korea in launching a new CBPR initiative explicitly excluding China and Russia that, therefore, is expected to come up with a new system closer to the US model.

The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) effective since 2018 includes a chapter on e-commerce or digital trade.[18] The successor to the Trans-Pacific Partnership (TPP) following the US's withdrawal in 2017, CPTPP is nonetheless based on many of the principles preferred by the US. In the case of the e-commerce chapter, CPTPP essentially reproduces the chapter that was to be adopted by TPP and, for example, has fairly strong protections underpinning the free flow of data.[19] Nonetheless, countries such as Vietnam have been able to carve out exceptions thanks to the absence of the US from the agreement. And enforcement mechanisms are weak even though the CPTPP includes provisions for a dispute-settlement mechanism. With China having applied to join CPTPP, however, it could be that CPTPP standards become more common across the Asia-Pacific.

The Regional Comprehensive Economic Partnership (RCEP) effective since 2022 also includes a chapter on e-commerce.[20] However, this chapter is less comprehensive than the CPTPP equivalent.[21]

15 APEC Telecommunications and Information Working Group. Security and Prosperity Steering Group, 'APEC Framework for Securing the Digital Economy', November 2019, https://www.apec.org/docs/default-source/publications/2019/11/apec-framework-for-securing-the-digital-economy/219_tel_apec-framework-for-securing-the-digital-economy.pdf?sfvrsn=a7ae9f31_1.

16 APEC, 'APEC Internet and Digital Economy Roadmap' (2017/CSOM/006), 6–7 November 2017, http://mddb.apec.org/Documents/2017/SOM/CSOM/17_csom_006.pdf.

17 'The APEC Cross-Border Privacy Rules (CBPR) System', CBPRs, accessed 18 November 2022, http://cbprs.org/.

18 MFAT New Zealand, 'Comprehensive and Progressive Agreement for Trans-Pacific Partnership Text and Resources', accessed 18 November 2022, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text-and-resources/#bookmark0.

19 MFAT New Zealand, 'Consolidated TPP Text – Chapter 14 – Electronic Commerce', accessed 18 November 2022, https://www.mfat.govt.nz/assets/Trade-agreements/TPP/Text-ENGLISH/14.-Electronic-Commerce-Chapter.pdf. MFAT New Zealand, 'Regional Comprehensive Economic Partnership (RCEP) Text and Resources', accessed 18 November 2022, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/regional-comprehensive-economic-partnership-rcep/rcep-text-and-resources/.

20 MFAT New Zealand, 'Regional Comprehensive Economic Partnership (RCEP) Text and Resources', accessed 18 November 2022, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/regional-comprehensive-economic-partnership-rcep/rcep-text-and-resources/.

21 MFAT New Zealand, 'RCEP Agreement – Chapter 12 – Electronic Commerce', accessed 18 November 2022, https://www.mfat.govt.nz/assets/Trade-agreements/RCEP/RECP-Agreement-112020/Chapter-12.pdf.

Furthermore, the digital trade provisions are based on the principles preferred by China. As a result, it is very restrictive in this area and there is no dispute-settlement mechanism, meaning that it cannot be enforceable. On the other hand, it is the largest trade agreement in the world and the only one to include three of Asia's four biggest economies: China, Japan, and South Korea.

Three CPTPP members—Chile, New Zealand, and Singapore—signed the Digital Economy Partnership Agreement (DEPA) in 2020. DEPA is a so-called "new type" of digital trade agreement in that it covers areas such as artificial intelligence, fintech, digital identities, or digital inclusivity.[22] Even though DEPA is small in membership, it is by far the most comprehensive digital trade agreement in the Asia-Pacific. Plus, China and South Korea have already asked to join, and it is likely that more countries will follow. It should be remembered that CPTPP traces its origins back to the 2005 Trans-Pacific Strategic Economic Partnership Agreement signed by the three DEPA members plus Brunei. In particular, China joining DEPA would indicate an important departure with its preferred approach to digital governance.

In recent months and since it is not a member of CPTPP, DEPA, or RCEP, the US has sought to develop its own digital governance and cybersecurity frameworks. Other than the APEC group mentioned above, the US launched discussions towards negotiations leading to the establishment of a standard-setting Indo-Pacific Economic Framework for Prosperity (IPEF) in May 2022. Countries across the Indo-Pacific including Japan, Singapore, South Korea, and, notably, India, are part of these discussions. They include specific reference to trade in the digital economy.[23] Indeed, the US and 12 IPEF partners issued a ministerial statement in September 2022 laying out the scope of future trade negotiations. Australia, Indonesia, Japan, South Korea, and Singapore have signed it.[24] (Noticeably, India has not.) IPEF excludes China. But it should be noted that the US has explicitly excluded market access provisions from IPEF, and it is also unclear whether it will have any enforcement mechanisms.

In addition, the US-led Quad has launched a Cybersecurity Partnership to develop joint cyber principles to strengthen cyber resilience, which the group links to critical infrastructure protection, supply chain resilience, workforce development, or software security standards. The Quad has also launched an Infrastructure Coordination Group focusing on digital connectivity, among others.[25] Quad members are working together, or looking into working together, with countries such as New Zealand, Singapore, South Korea, or Vietnam. This is recognition that the group, because it is perceived as anti-China and has a small membership, has been ineffective so far. In the area of cybersecurity and digital connectivity, South Korea and Taiwan are considered important (potential) partners due to their high-tech economies.

22 MFAT New Zealand, 'DEPA Text and Resources', accessed 18 November 2022, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-text-and-resources/.
23 The White House, 'Statement on Indo-Pacific Economic Framework for Prosperity', 23 May 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/statement-on-indo-pacific-economic-framework-for-prosperity/.
24 Office of the United States Trade Representative, 'The Indo-Pacific Economic Framework for Prosperity: Biden-Harris Administration's Negotiating Goals for the Connected Economy (Trade) Pillar', 23 September 2022, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/september/indo-pacific-economic-framework-prosperity-biden-harris-administrations-negotiating-goals-connected.
25 The White House, 'Fact Sheet: Quad Leaders' Tokyo Summit 2022', 23 May 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-quad-leaders-tokyo-summit-2022/.

Critical (digital) infrastructures, from 5G infrastructure protection to the security of the undersea fibreoptic cables linking the Indo-Pacific region to the rest of the world, have emerged as both the next frontier for high-speed economic growth and connectivity and a source of rising geostrategic tensions.

The EU has not been immune to such dynamics, as the European Commission is considering cofinancing the Far North Fiber project,[26] including the Alaskan company Far North Digital and Finland's Cinia, thus funding a submarine fibre optic cable to connect Scandinavia and Ireland to Japan via the Artic. Undersea cables carry over 95% of the international data traffic in the Indo-Pacific and they are equally subject to various vulnerabilities and threats.[27] Whoever controls or disrupts such networks possesses significant geopolitical power. In response to the Nord Stream pipeline leaks, the EU has started to pay closer attention to increasing the protection of undersea cables, via a five-point plan to improve critical infrastructure. Undersea fibreoptic cables are an important area where the EU and like-minded partners in the Indo-Pacific can work more closely together to propose joint ventures and increase protections.

Relatedly, 5G networks are ripe for cyberattacks at a scale never seen before. Moreover, taking critical decisions to use or not use certain Chinese, Western, or indigenous network vendors creates geopolitical complications in the Indo-Pacific. The backlash against Huawei's 5G offerings has reverberated in the EU as well, the bloc putting forward its 5G toolbox in early 2020, namely the "Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures".[28] The goals of this instrument are to identify possible measures to mitigate the cybersecurity risks of 5G networks and prioritise plans across EU member states and at the EU level to create a robust framework of mitigation measures. In this area of the cybersecurity of 5G networks, the EU should take active steps to promote its 5G toolbox as an avenue for cooperation with Indo-Pacific countries.

The above suggests that the EU's stated goal of promoting multilateralism in the Indo-Pacific faces important obstacles in the area of digital governance and partnerships, as well as when it comes to cybersecurity. These obstacles include, above all, Sino-American competition across the region and rising challenges to critical infrastructures. This has led to tensions between connectivity including China and (potential) decoupling from China, between different approaches to digital governance, and also between different geographical realities: Asia-Pacific, East Asia, and Indo-Pacific itself. This means that the EU will have to consider the trade-offs between its own interests and the goal of promoting multilateralism in the region. In the next section, we examine the area of digital governance and partnerships. We then analyse approaches to governing cyberspace and cybersecurity-related implications. We finish this report with a discussion about foresight to 2030 and recommendations.

26 Luca Bertuzzi, 'EU Eyes Arctic Internet Cable to Connect Europe to Asia via Alaska', EURACTIV, 14 October 2022, https://www.euractiv.com/section/digital/news/eu-eyes-arctic-internet-cable-to-connect-europe-to-asia-via-alaska/.
27 Anthony Bergin and Samuel Bashfield, 'Options for Safeguarding Undersea Critical Infrastructure: Australia and Indo-Pacific Submarine Cables', Australian Strategic Policy Institute, 1 June 2022, https://www.aspi.org.au/journal-article/options-safeguarding-undersea-critical-infrastructure-australia-and-indo-pacific.
28 European Commission, 'Cybersecurity of 5G Networks – EU Toolbox of Risk Mitigating Measures', 29 January 2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

THE EU, DIGITAL GOVERNANCE, AND PARTNERSHIPS IN THE INDO-PACIFIC

In recent years, the massive surge in the use of digital technologies, impacting the speed and volume of information and communications, public data spaces, digital services platforms, and trade, has brought about numerous concerns. The past decade has been transformative for technological innovation, signalling what some have labelled as the Fourth Industrial Revolution. Emerging disruptive technologies such as AI, quantum computing, big data, autonomous systems, and future generations of networks are expected to radically transform existing systems of (digital) governance and trigger complex debates about their design and deployment in a data driven world.

Their rapid adoption and constant evolution affect privacy, trust, and (cyber)security, shaping the daily lives of European citizens in manifold ways. The EU aims to address these issues via a complex digital governance framework of horizontal and sectoral policies ranging from research, innovation, and industrial initiatives in critical technological areas to strengthening the bloc's digital and technological sovereignty.[29] The framework also includes creating a level playing field in digital markets dominated by large platforms, spearheading regulatory initiatives for human-centric and trustworthy AI and proposing secure digital services, data spaces, and infrastructures.

Already, the EU's 2010 Digital Agenda for Europe[30] highlighted the need to harness the potential of information communication technologies and their key enabling role for the Union's digital transition goals; followed by the 2015 Digital Single Market Strategy for Europe,[31] which developed the digital agenda further to capitalise on the benefits of an open, fair, and secure digital environment. The 2020 Digital Agenda for Europe builds on such breakthroughs and sets the stage for the EU's digital strategy, while zooming in on three key objectives shaping Europe's digital future: firstly, technology that works for people; secondly, a fair and competitive economy; and thirdly, an open, democratic, and sustainable society.

In 2021, the strategy was accompanied by the 10-year Digital Compass for the EU's Digital Decade,[32] which puts the EU's digital ambitions for 2030 into concrete terms around four cardinal points: skills, government, infrastructures, and business. Importantly, the EU's digital strategy has been anchored in a new EU funding programme for digital technology for the 2021-2027 period, the Digital Europe Programme,[33] which will provide strategic funding to finance project in five key domains, namely AI, supercomputing, cybersecurity, advanced digital skills, and mainstreaming digital technologies across society and economy also via European Digital Innovation Hubs.[34]

29 Raluca Csernatoni, 'The EU's Rise as a Defense Technological Power: From Strategic Autonomy to Technological Sovereignty', Carnegie Europe Article, 12 August 2021, https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134.
30 European Commission, 'A Digital Agenda for Europe' (COM[2010]245 final), 9 May 2010, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF#:~:text=The%20overall%20aim%20of%20the,structural%20weaknesses%20in%20Europe's%20economy.
31 European Commission, 'A Digital Single Market Strategy for Europe' (COM[2015]192 final), 6 May 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN.
32 European Commission, 'Europe's Digital Decade: Digital Targets for 2030', accessed 18 November 2022, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.
33 European Commission, 'The Digital Europe Programme', accessed 18 November 2022, https://digital-strategy.ec.europa.eu/en/activities/digital-programme.
34 European Commission, 'European Digital Innovation Hubs', accessed 18 November 2022, https://digital-strategy.ec.europa.eu/en/activities/edihs.

Under the EU's current digital governance umbrella, several other internal governance initiatives are worth flagging, due to their "first-of-a-kind" nature and their externalisation potential with extraterritorial reach. For instance, the GDPR[35] enshrines privacy, human rights, and data protection into EU law. By following a "privacy-by-design" model, it highlights the importance of adding enhanced data protections to the operations of businesses and companies, such as anonymising routinely collected data. To complement the GDPR, the new European Commission-proposed Data Act[36] from February 2022 pertains to new horizontal rules on who can use and access the data generated across all economic sectors in the EU, aiming to ensure fairness and competitiveness in the European data market. The European Commission has also unveiled in April 2021 the first-of-its-kind new proposal for a comprehensive regulatory framework on AI, the so-called AI Act.[37] It is the first ever legal-ethical attempt to enact a horizontal regulation of AI systems in use, based on a "risk-based approach", according to which risks deemed "unacceptable" would be prohibited, while "high-risk" AI systems would be authorised, but subject to a set of obligations and requirements to gain EU market access.

The above are only some examples of digital regulatory schemes, noteworthy being the fact that their impact will not stop at the EU's borders. This implies that there is not only value in advancing internal digital governance frameworks for the benefit of EU citizens and the European digital transition, but that to do so would equally have a broader global impact in terms of the so-called "Brussels effect".[38] Accordingly, the EU has the unique ability to promulgate rules that shape the global (digital) economy, business environments, and e-commerce via its market and regulatory powers, by elevating standards worldwide in various domains, from competition regulations to new international standards for regulating AI and online hate speech to data protection, only to name a few. Yet, this extraterritorial impact alone, via regulatory standards-setting and market forces, does not guarantee the EU's success in navigating the digital decade.

Conversely, the EU should focus on multilateralism and more collaborative approaches with like-minded partners to bring other governments along with its perspectives on digital governance, and to promote the rules-based international order, open internet, and access to free markets. In a bid to promote global data governance standards and indicative of the above externalisation trend, the February 2022 Joint Declaration on privacy and the protection of personal data[39] is an example of how the EU, together with partners such as Australia, Comoros, India, Japan, Mauritius, New Zealand, Singapore, South Korea, Sri Lanka, the Philippines, Thailand, and Taiwan can cooperate on privacy and the protection of personal data. The goal is to harness the opportunities presented by the digital economy and cross-border commercial exchanges, while interlinking trusted technology and security to privacy regulatory regimes, ensuring a human-centric approach to the secure free flow of data and respecting individuals' rights to privacy and high personal data protection as a core value and fundamental freedom.

35 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), accessed 18 November 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

36 European Commission, 'Data Act: Commission Proposes Measures for a Fair and Innovative Data Economy' (Press release), 23 February 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

37 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative act, COM/2021/206 final, accessed 18 November 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

38 Anu Bradford, The Brussels Effect: How the European Union Rules the World (New York, NY: Oxford University Press, 2020).

39 European External Action Service, 'Joint Declaration on Privacy and the Protection of Personal Data', 23 February 2022, https://www.eeas.europa.eu/eeas/joint-declaration-european-union-australia-comoros-india-japan-mauritius-new-zealand-republic_en.

Emphasis is put on strengthening trust in the digital environment and data free flows by addressing emerging challenges for privacy and the protection of personal data. The Joint Declaration is also indicative of the fact that the signatories share a common vision of a human-centric approach to the digital transformation, prioritising the effective protection of personal data as a key enabler for cross-border cooperation. Worth flagging are a number of core principles at the heart of high data protection and privacy standards, namely lawfulness, fairness, transparency, purpose limitation, data minimisation, limited data retention, data security and accountability. A recent bilateral EU engagement, the EU-India Trade and Technology Council[40] from April 2022, aims for instance to advance strategic coordination mechanisms that "will allow both partners to tackle challenges at the nexus of trade, trusted technology and security", emphasis being given to digital trade among others.

Indeed, in the next few years, the EU's success as a normative and regulatory superpower will be defined by how it deals with the major challenges posed by emerging and disruptive technologies, how it deals with data, AI, cybersecurity, and in general the digital transformation. The coherence between EDTs, international (digital) norms promotion activities, and foreign policy ambitions will be crucial for the EU in a global context shaped by rapid innovation and geopolitical rivalry also played out in the digital sphere. For the EU, also mastering digital geopolitics is key, especially in terms of toughening up its digital foreign policy engagement with strategic partners and in key regions.

In this respect, the 2021 Indo-Pacific Strategy recognises the need for enhanced bilateral and multilateral cooperation in the Indo-Pacific region, reinforcing collaborations with regional organisations such as the Association of Southeast Asian Nations (ASEAN), as well as fostering reliable and long-standing relations will all its like-minded partners in the region (p. 4). In fact, the word "multilateral" is mentioned no less than 18 times in the 17-page long document. The EU's external engagement goals are structured around digital economy goals. These include, among others, working closely with partners on international standards-setting and other digital regulatory priorities, besides initiating regulatory cooperation in areas supporting the digital transitions across Europe and in the Indo-Pacific region (p. 6). When it comes to digital governance priorities in the region, the EU's goals encompass: expanding the network of digital partnerships with Indo-Pacific like-minded governments and regional fora, including exploring the possibility of new Digital Partnership Agreements as underpinned by the Communication 2030 Digital Compass: The European Way for the Digital Decade (p. 10); seeking mutually beneficial research and innovation schemes with like-minded partners under the Horizon Europe[41] programme – the EU's key scientific research initiative (p. 11); supporting educational and academic exchanges between the Indo-Pacific region and Europe (p. 11); and promoting all dimension of (digital) connectivity to better connect Europe to its partners in the region, also in line with the 2021 EU Declaration on the European Data Gateways[42] (p. 12).

40 European Commission, 'EU-India: Joint Press Release on Launching the Trade and Technology Council' (Press release), 25 April 2022, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2643.
41 European Commission, 'Horizon Europe', accessed 18 November 2022, https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.
42 European Commission, 'Digital Day 2021: Europe to Reinforce Internet Connectivity with Global Partners', accessed 18 November 2022, https://digital-strategy.ec.europa.eu/en/news/digital-day-2021-europe-reinforce-internet-connectivity-global-partners.

Significantly, the EU's multilateral approach is an essential building block to advance mutually beneficial governance and technical cooperation with like-minded countries in strategic digital domains such as secure connectivity infrastructures; resilience of supply chains; the digital transformation of the public and private sectors; the support of science, research, technology, and investment in innovation; the development of standards for EDTs like AI in line with democratic principles and fundamental rights; and facilitating investments in the digital marketplace and a stable digital trading environment.

Nevertheless, the multilateral approach should be supplemented by bilateral agreements. The EU is not a party to any of the agreements being developed to promote multilateral digital governance in the Indo-Pacific region – or rather, in the Asia-Pacific (e.g., CBPR, CPTPP, DEPA) and East Asia (e.g., RCEP). These agreements, however, are either fairly shallow (e.g., CBPR, RCEP) or have no credible enforcement mechanisms (e.g., CPTPP, DEPA). Thus, there is a window of opportunity for the EU to promote its preferred approaches to digital governance via bilateral agreements. Most notably, digital partnership agreements such as that signed with Japan, South Korea and Singapore are useful tools to promote mutually agreeable digital governance frameworks.

In this respect, the Digital Partnership Agreement already in place with Japan and South Korea serves to exemplify how the EU can make use of bilateral instruments to boost cooperation in the digital domain and expand the influence of its preferred approaches to digital governance. The agreement with Japan covers the four components of the Digital Compass: skills, public services, infrastructures, and business.[43] Of particular interest to Japan, and the Indo-Pacific region more broadly, are the resilience of global supply chains, secure 5G, secure connectivity, and digital trade. These are, after all, the areas that countries in the Indo-Pacific are prioritising, including via agreements such as CPTPP and DEPA. They are also priority areas for IPEF, to which over a dozen Indo-Pacific countries have signed up – including Japan, Singapore, and South Korea, the three countries that the EU has prioritised in terms of digital partnership agreements.

According to the Digital Partnership Agreement with Japan, the EU and its partner will reach their goals via research and development in the area of technology; implementing concrete projects in cutting-edge areas such as AI; sharing best practices including in the areas of regulatory cooperation, rules, and standards; establishing mechanisms for collaboration in international organizations; taking a similar approach to digital transformation based on an open internet; and share digital and trade principles to foster digital trade.[44] As the United Nations Conference on Trade and Development (UNCTAD) has pointed out, Japan has a similar approach to the EU's when it comes to digital governance. Thus, it makes sense for both countries to prioritise these areas, including the principle of an open internet and the internationalisation of their preferred regulations, rules, and standards.

The expectation is that the Digital Partnership Agreement with South Korea will be similar. After all, South Korea is at a similar stage of development of digitalisation and the digital economy as Japan, has a similar approach to digital governance to the EU's and Japan's as per UNCTAD's assessment, and seeks cooperation in multilateral organizations to advance its preferred principles.

43 'Japan-EU Digital Partnership – Factsheet'.
44 Ibid.

Furthermore, the EU presented its vision for a digital partnership with South Korea at the same time as it was finalising the partnership with Japan.45 In other words, discussions with both partners have moved in parallel, which further underscores that they are bound to be similar. Even though UNCTAD's assessment was that Singapore's approach to digital governance is closer to the US's than the EU's, this did not stop the two partners agreeing to a digital partnership in December 2022.

What is more, data adequacy recognition of Japan, New Zealand, and South Korea by the European Commission is a powerful tool to promote the EU's preferred digital governance principles.[45] In this respect, the Brussels effect seems to work insofar as businesses and their governments share an interest in gaining access to the EU's single market, and therefore seek this "seal of approval" from the European Commission. Similarly, the EU's Digital Economy dialogues with ASEAN, China, India, Japan, South Korea, and Taiwan can serve to promote the Union's preferred digital governance approaches and norms. EU partners see value in these dialogues since they allow them to exchange opinions and views with EU officials and experts. The keyword here is "exchange". In recent years, Indo-Pacific partners have become more willing to assert their own positions, including in the areas of the digital economy and digital governance. Thus, they are willing to listen to and discuss with third parties, including the EU. And due to the Brussels effect, they may follow EU rules, as the EU's data adequacy decisions show. But they also want to express their own views and to engage in a dialogue, particularly in areas in which they are amongst the most advanced in the world, such as China, Japan, Singapore, or South Korea, when it comes to the digital economy.

Conversely, an area of concern for the EU should be digital connectivity. The EU's Indo-Pacific Strategy highlights it as an area of work in the region (p. 10). However, it is an area in which the EU's footprint is minimal. The ASEAN Digital Masterplan 2025 arguably has the greatest potential to lay out the blueprint for digital connectivity across the Indo-Pacific.[46] Agreements such as CPTPP, DEPA, or RCEP, or even the US's IPEF, may also help. And Chinese, Japanese, and South Korean firms have been supporting digital connectivity infrastructure building across the Indo-Pacific, particularly in South and Southeast Asia. In contrast, the EU and European firms are secondary actors at best in this area. The EU-India Connectivity Partnership,[47] the EU-Japan Partnership on Sustainable Connectivity and Quality Infrastructure,[48] the ASEAN-EU Joint Ministerial Statement on Connectivity, [49] and EU-South Korea discussions about a connectivity partnership are steps in the right direction, particularly if they are linked to the Union's Global Gateway. However, neither the partnership with India nor the one with Japan have resulted in any project. This is actually creating political frictions, affecting the credibility of the EU. It is an area in which the Union needs to step up and start to deliver sooner rather than later.

45 European Commission, 'Adequacy Decisions: How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection', accessed 18 November 2022, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
46 The Association of Southeast Asian Nations (ASEAN), 'ASEAN Digital Masterplan 2025', accessed 18 November 2022, https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf.
47 Council of the European Union, 'EU-India Connectivity Partnership [8 May 2021]', accessed 18 November 2022, https://www.consilium.europa.eu/media/49508/eu-india-connectivity-partnership-8-may-2.pdf.
48 EU-Japan Partnership on Sustainable Connectivity and Quality Infrastructure was signed between the EU and Japan, European External Action Service, September 2019, accessed 18 November 2022, https://www.eeas.europa.eu/sites/default/files/the_partnership_on_sustainable_connectivity_and_quality_infrastructure_between_the_european_union_and_japan.pdf.
49 Ministry of Foreign Affairs Singapore, 'ASEAN-EU Joint Ministerial Statement on Connectivity', 1 December 2020, https://www.mfa.gov.sg/Overseas-Mission/Ministry-of-Foreign-Affairs---Permanent-Mission-of-the-Republic-of-Singapore/Latest-News-in-ASEAN/2020/12/ASEAN-EU-Joint-Ministerial-Statement-on-Connectivity.

THE EU AND CYBERSECURITY IN THE INDO-PACIFIC

Rapid developments in the field of digital technologies are already changing the threat landscape and (cyber) operational environment, involving multiple state and non-state actors across the cyber-physical domains. EDTs such as AI[50] are progressively deployed to enhance various functions related to cybersecurity, cybersurveillance, and cyber defence, to protect communications and information platforms, for data analytics, and to secure the resilience of critical infrastructures. Algorithmic-driven attacks and responses are becoming faster, more precise, and more disruptive. International cooperation on norms and regulations is thus necessary for promoting responsible state behaviour in cyberspace via voluntary nonbinding norms, rules, and principles, while governance red lines need to be drawn to determine proportional responses to evolving cyber threats. These include, among others, setting clear thresholds for the attribution of legal and illegal cyberattacks, in addition to applying appropriate international sanctions for malicious cyber operations.

Against this backdrop and a proliferation of cyber and hybrid threats below the threshold of military escalation, the EU, and particularly the European Commission, holds significant agenda-setting powers and competencies with regard to the cybersecurity policy field. Its digital single market strategy derives its legal basis from Single Market Treaty provisions, and within this context numerous legislative and policy initiatives have been launched since 2013. Out of those, major pieces of regulation specifically concern cybersecurity sub-sections including critical infrastructure protection, public-private partnership for cybersecurity, illegal online content, and disinformation, as well as enhancing the powers of the EU's key cybersecurity agency the European Union Agency for Cybersecurity (ENISA). This governance structure sits alongside national cybersecurity policies, setting the main parameters for Union-wide cybersecurity management and governance structures.

While EU member states remain responsible for national (cyber)security and defence, the impact, scale, and transnational nature of cyber and hybrid threats have made a powerful case for more EU-level coordinated action and multilateral cooperation with key partners. The Cybersecurity Strategy of the European Union - An Open, Safe and Secure Cyberspace[51] from February 2013 was the first comprehensive and programmatic policy document to address cyberspace-related security issues. The strategy is also credited to first enshrining European cyber defence at the EU-level and as an emerging policy area dealing with the military dimension of the EU's cybersecurity. The document proposed a holistic three-pillars-of-action approach, including network and information security, law enforcement, and defence. The defence part of the strategy was reinforced by the adoption of a "Cyber Defence Policy Framework"[52] by the European Council in November 2014, highlighting five priority areas: supporting the development of cyber defence capabilities related to the EU's Common Security and Defence Policy (CSDP) together with EU member states; enhancing the protection of CSDP communication networks used by EU entities; promotion of civil-military cooperation and synergies with wider EU cyber policies and relevant EU institutions and agencies, as well as with the private sector; improving training, education, and exercise opportunities; and finally enhancing cooperation with key international partners,

50 Raluca Csernatoni and Katerina Mavrona, 'The Artificial Intelligence and Cybersecurity Nexus: Taking Stock of the European Union's Approach,' Carnegie Europe Article, 15 September 2022, https://carnegieeurope.eu/2022/09/15/artificial-intelligence-and-cybersecurity-nexus-taking-stock-of-european-union-s-approach-pub-87886.
51 European Commission, 'The EU's Cybersecurity Strategy in the Digital Decade'.
52 EU Cyber Direct – EU Cyber Diplomacy Initiatives, 'EU Cyber Defence Policy Framework', accessed 18 November 2022, https://eucyberdirect.eu/atlas/sources/eu-cyber-defence-policy-framework.

including NATO and other major stakeholders. In November 2022, the EU published The EU Policy on Cyber Defence,[53] setting out to cover a wide range of initiatives that will help the EU and its member states to be able to better detect, deter, and defend against malicious cyber-attacks. Noteworthy is the fact that the policy emphasised stronger cooperation between the military and civilian actors for a stronger EU cyber defence.

Noteworthy as well is the fact that the 2016 EU Global Strategy considered "cyber" as one of the key components of the EU's foreign, security, and defence policy. This was followed by the 2017 Joint Communication by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy on "Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU",[54] flagging the need for EU cyber defence to better respond to hybrid threats. In September 2017, the European Commission and the European External Action Service (EEAS) also updated the 2013 EU Cybersecurity Strategy with the objective to promote an "open, safe and secure cyberspace" and with the intention to improve the protection of Europe's critical infrastructure, and importantly, to boost the EU's digital autonomy in relation to other regions of the world. Furthermore, the European Commission, the European Parliament and the Council issued a joint communication titled "Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats",[55] also stressing the need for deeper European and cross-border coordination in cyber resilience and deterrence, as well as stepping up on cybersecurity capabilities. In this respect, cyber deterrence has entered more and more EU cyber governance considerations.

Prompted by the WannaCry and NotPetya attacks and their aftermath in economic consequences, in 2017 the EEAS and the Commission set in motion a process of developing a framework for a Joint Diplomatic Response to Cyber Operations, the outward facing Cyber Diplomacy Toolbox.[56] The EU has been using its toolbox to prevent, discourage, deter, and respond to malicious cyber activities, thus clearly signalling the added value of a joint EU diplomatic response to malicious cyber activities via international engagement, by influencing the behaviour of potential aggressors in cyberspace, and thus reinforcing the security of the EU and its member states. The toolbox implements guidelines envisaging a response spectrum ranging from confidence-building measures (CBMs), partners' capacity-building, and diplomatic engagement to using stronger individual or cooperative responses in order to protect the open and safe cyberspace. The toolbox was updated in 2019 with the council decision concerning restrictive measures against cyber-attacks threatening the Union or its member states,[57] introducing a dissociation of sanctions and targeted restrictive measures from definitive attribution of malicious cyber activities to a third state.

53 European Commission, 'Questions and Answers: The EU Policy on Cyber Defence', 10 November 2022, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6643.
54 European Commission, 'Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU' (JOIN[2017]450 final), 13 September 2017, ,https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en.
55 European Commission, 'Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats' (JOIN[2018]16 final), 13 June 2018, https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016.
56 'EU Cyber Diplomacy Toolbox', accessed 18 November 2022, https://www.cyber-diplomacy-toolbox.com/.
57 'Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States', ST/7302/2019/INIT, accessed 18 November 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0796&from=EN.

The EU's latest Cybersecurity Strategy for the Digital Decade (2020) builds on the above developments and highlights cybersecurity as a precondition for achieving the aims of resilience, technological autonomy, and leadership (p. 5). It also maps a sober threat landscape compounded by "geopolitical tensions over the global and open Internet and over control of technologies across the whole supply chain" (p. 1). These tensions are reflected in the increasing number of nation states erecting digital borders jeopardising the global and open cyberspace, as well as the rule of law. It comes as no surprise that the 2020 Cybersecurity Strategy also identifies key technologies like AI, encryptions, quantum computing, and future generation networks as essential to cybersecurity.

While the strategy does not make any reference to the Indo-Pacific region, it signals the increasing deterioration of effective multilateral debates on international security in cyberspace (p. 20) by also underlying the EU's efforts to promote CBMs between states, including sharing best practices at regional and multilateral levels. The stated intention is to contribute to cross-regional cooperation on cybersecurity, cyber resilience, and mutual assistance in cases of cyber crises. Thus, the end goal is for the EU to continue working with international like-minded partners to better understand the threat landscape and to develop a cooperation mechanism in order "to promote a political model and vision of cyberspace grounded in the rule of law, human rights, fundamental freedoms and democratic values" (p. 19).

Stronger international cooperation with like-minded partners are also prioritised in relation to shaping international standards in the areas of emerging technologies "to ensure that the Internet remains global and open, and that EDTs are human-centric, privacy-focused, and that their use is lawful, safe and ethical" (p. 20). In this respect, the objective is for the EU to strengthen and expand its cyber dialogues with third countries to promote its values and vision for cyberspace, sharing best practices, and seeking to cooperate more effectively. The strategy also mentions the fact that the EU should establish structured exchanges with regional organisations such as the ASEAN Regional Forum.

The EU's Cybersecurity Strategy should indeed be the basis for its policy towards the Indo-Pacific in this area. To begin with, the strategy serves Indo-Pacific partners, both existing and potential, to understand how the EU seeks to address cyberattacks, espionage, and disinformation. These are the key cybersecurity threats that the EU seeks to confront, and they are shared by Indo-Pacific partners. In particular, malicious cyber activities by China, North Korea, and Russia affect both the EU and its Indo-Pacific partners. The toolkit laid out by the EU in its Cybersecurity Strategy should be the basis of its approach towards cooperation in the region. Yet, the EU should be aware that Indo-Pacific partners will variously cooperate with the EU itself, its members states, and NATO, depending on the issue area. In this respect, South Korea's membership in NATO's Cooperative Cyber Defence Centre of Excellence and Australia's and Japan's role as contributing participants illustrate that Indo-Pacific countries understand the potential for cooperation with various like-minded actors in Europe and in the context of the transatlantic alliance.

There is a question as to whether the EU's emphasis on making use of existing standards and cooperation mechanisms, namely the Council of Europe's Budapest Convention, can assist or hinder the Union's cybersecurity role in the Indo-Pacific. This is stressed in the Indo-Pacific Strategy (p. 14). Australia, Japan, the Philippines, and Sri Lanka are the only Indo-Pacific countries which are parties to a convention already signed in 2001.[58] This signals the failure of its parties to internationalise the convention, which after all was drawn by a European organisation. Promotion of a European convention could be interpreted by countries in the Indo-Pacific as an attempt to universalise standards that were not developed in consultation with them.

In terms of norm setting to strengthen cybersecurity, digital partnership agreements such as those signed with Japan, South Korea and Singapore, or the ASEAN-EU Statement on Cybersecurity Cooperation, even if too broad, can serve as the basis to promote norm setting. Since these agreements are negotiated with partners, they are not perceived as the imposition of European norms, as is the case with the Budapest Convention, for example. Likewise, the EU's Cyber Diplomacy Network outline in the Indo-Pacific Strategy (p. 14) can also support norm setting. This would be a more time-consuming and longer process, but it has the advantage of making Indo-Pacific partners feel included and take ownership of their decisions.

Cyber-resilience is another area highlighted by the EU's Indo-Pacific Strategy in relation to cybersecurity (p. 14). In this respect, capacity building arguably is one of the most effective tools that the EU may have to boost cooperation with Indo-Pacific partners – particularly in South and Southeast Asia. This would have the added benefit of supporting the promotion of EU norms. The role of EU and EU member states policies and military cyber units in boosting resilience should be emphasised, particularly in cooperation with third parties such as Australia, Japan, Singapore, South Korea, or the US. Furthermore, the EU has two other important tools at its disposal when it comes to capacity building. One of them is Enhancing Security Cooperation in and with Asia (ESIWA), with its focus on cybersecurity as one of its key pillars.[59] The other is Horizon Europe, which can promote joint research and innovation with partners. Both of them are highlighted in the EU's Indo-Pacific Strategy (p. 14 and 11, respectively). They would be welcomed by partners in the region, given their focus on diversifying their links to reduce dependence on one or a small number of partners (e.g., China or the US).

58 Council of Europe, 'The Budapest Convention (ETS No. 185) and its Protocols', accessed 18 November 2022, https://www.coe.int/en/web/cybercrime/the-budapest-convention.
59 GIZ, 'Enhancing Security Cooperation in and with Asia', accessed 18 November 2022, https://www.giz.de/en/worldwide/87412.html.

CONCLUSION AND RECOMMENDATIONS

Digital governance in the Indo-Pacific can only be defined as fragmented as of 2022. Our expectation is that this will remain the case going into 2030. To begin with, it remains to be seen whether an Indo-Pacific-wide digital governance framework will emerge. IPEF, or future US-led initiatives, arguably are the most likely to result in an Indo-Pacific-wide framework. But there are two caveats. The first is that US-led initiatives are meant to exclude China. Thus, they cannot really be said to cover the whole of the Indo-Pacific region. The second is that, absent a promise of market access, US initiatives are likely to remain shallow and with poor enforcement. Thus, US-led Indo-Pacific initiatives will be part of a network of agreements and other initiatives covering different parts of the region, rather than the only approach to digital governance.

We therefore should expect that Asia-Pacific (e.g., CBPR, CPTPP, DEPA) and East Asia agreements (e.g., RCEP) will continue to coexist with the US-led Indo-Pacific initiative. This will create a set of overlapping rules. Even though this may seem contradictory and even detrimental to digital governance in the region, the lack of effective enforcement mechanisms means that it is a realistic scenario until 2030. After all, several Indo-Pacific countries are members of CPTPP and RCEP – and several RCEP members are seeking to also join CPTPP in the not-too-distant future. Differently from the case of the EU, there is no single, overarching framework covering digital governance in the Asia-Pacific or East Asia. This is why different agreements will continue to coexist.

Therefore, we should not expect the EU's stated goal of promoting multilateralism in the region to be achieved in the area of digital governance. Most Indo-Pacific countries remain uninterested in, when not opposed to, the Budapest Convention, which they see as a European rather than multilateral agreement. This has been the case for over two decades, and it is not going to change before 2030. Instead, some countries such as Japan or South Korea are likely to have similar approaches to digital governance as the EU. Others will have an approach similar to the US, such as Australia and Singapore. And others will share China's suspicion of openness in this area, including India or Vietnam. This multitude of approaches will be possible thanks to the absence of an Indo-Pacific-wide agreement with effective enforcement mechanisms.

It is more likely that the EU will be able to serve its own interests and goals in the Indo-Pacific region via bilateral mechanisms, such as adequacy decisions, trade and technology cooperation mechanisms such the Trade and Technology Council format, digital dialogues or digital partnership agreements. The Brussels effect, in particular, is a strong pull factor for Indo-Pacific partners to implement standards similar to those of the EU. It is thus likely that more Indo-Pacific countries will seek adequacy recognition from the European Commission. However, we should not expect this process to become universal. It is telling that at the time of writing only Japan, New Zealand, and South Korea have adequacy recognition – these are the three Indo-Pacific countries that UNCTAD recognises as having a similar approach to digital data governance as the EU.

When it comes to cybersecurity, we can expect greater cooperation between Indo-Pacific partners such as Australia, Japan, New Zealand, Singapore, or South Korea and Europe. After all, the risks are similar and all of them are seeking to expand their network of links with like-minded partners. Yet, we can expect that between now and 2030 links will become stronger not only with the EU, but also with individual member states and with NATO. This is the preferred approach of Indo-Pacific partners, who do not want to limit their contact network.

Considering the above scenarios, we propose seven recommendations to the EU moving forward in order to strengthen its position in the digital governance of the Indo-Pacific.

For the EU to become a stronger digital and cybersecurity actor in the region, it should **take a holistic and cross-sectoral approach to digital governance and cybersecurity in the short and medium term**, by involving different agencies and bodies led by Directorate-General Connect and Directorate-General Trade. In this respect, the EU should get involved in a wide range of issues including supply chain resilience, critical infrastructure, data governance, and digital trade. It is further recommended that the EU work closer together with the largest number of like-minded partners as possible, but especially Australia, Japan, New Zealand, Singapore, and South Korea. Another important point is the need to embrace the diversity of the Indo-Pacific region, including less-developed partners such as Indonesia, Malaysia, the Philippines, and Vietnam.

Looking **towards 2030, the EU should indeed promote multilateral engagement in the region,** not only because it is the preferred strategic approach of the Union but also since, at least in the theory, it is the preferred approach of some of the EU's Indo-Pacific like-minded partners. Accordingly, the EU should emphasise multilateralism including via international organisations, which most Indo-Pacific countries continue to support, as well as the Budapest Convention for countries interested in the latter.

Moreover, while EU-led multilateral cooperation should be encouraged, the bloc will need to **prioritise bilateralism over multilateralism, when necessary,** due to the fact that digital governance in the Indo-Pacific region is very unlikely to become multilateral for the foreseeable future. To date, partners in the region feel comfortable in bilateral settings in which they can have meaningful exchanges, including in the cases of Japan, Singapore, and South Korea, as well as potentially others with which bilateral cooperation is at an earlier stage, such as India, Indonesia, Malaysia, or the Philippines.

One constructive and pragmatic area of both bilateral and multilateral engagement is capacity building in the region. Accordingly, **the EU should support capacity building in the Indo-Pacific region, bilaterally or together** with third parties, such as Japan, Singapore, or South Korea. Furthermore, there is a demand in South and Southeast Asia for this type of productive cooperation, focusing on areas such as critical infrastructure building, data governance framework development, digital trade facilitation, or research and development projects.

Due consideration should be given by the EU to prioritising cooperation with key partners, particularly Japan, Singapore, and South Korea, as a way to boost the presence of the EU in the region and promote the Union's norms via partners with similar approaches. Emphasis should be put on norms and standards promotion in the region, considering the fragmented nature of digital governance and cybersecurity in the region, the different approaches to digital governance by regional countries, and the EU's relatively recent presence in digital and cyber discussions in the Indo-Pacific.

In addition to norms promotion, **the EU should make strategic use of digital trade and digital services facilitation,** which remain powerful tools for the Union to shape policy in the region given the size of its market, is appealing to governments in the region. Most importantly, the end goal should be to ensure predictability and legal certainty for businesses, a secure online environment for consumers, and the removal of barriers, particularly as other countries refuse to contemplate a similar approach.

Finally, **the EU should be prepared to strategically explore the possibility of collaborating with or even joining regional agreements, most notably DEPA and/or CPTPP**, since they have the potential to help set standards in the region. Such collaborations will give voice to the Union in regional digital governance dynamics, particularly since multilateralism is unlikely to be successful for the foreseeable future, since regional agreements are growing in terms of membership, and other agreements such as IPEF are only moving ahead more slowly.

Recommendations – a summary

1. Take a holistic approach to digital governance and cybersecurity, involving different agencies and bodies led by DG Connect and DG Trade.
2. Promote multilateral approaches with like-minded Indo-Pacific partners, including via international organisations and in support of the Budapest Convention when possible.
3. Prioritise bilateralism and minilateralism over multilateralism, when necessary, since digital governance in the region is very unlikely to become multilateral for the foreseeable future.
4. Support capacity building in the region, bilaterally or together with third parties such as Japan, Singapore, or South Korea.
5. Prioritise cooperation with key partners, particularly Japan, Singapore, and South Korea, as a way to boost the presence of the EU in the region.
6. Make strategic use of digital trade facilitation, which remains a powerful tool for the Union to shape policy in the region given the size of its market.
7. Explore the possibility of collaborating with or even joining regional agreements, most notably DEPA and/or CPTPP to help set standards in the region.

ABOUT THE AUTHORS

Raluca Csernatoni is Guest Professor on European Security with the Brussels School of Governance and its Centre for Security, Diplomacy and Strategy, at Vrije Universiteit Brussels, Belgium. Csernatoni is currently a research fellow at Carnegie Europe, where she specialises in European security and defence, with a focus on emerging and disruptive technologies. She is also Team Leader and Expert on new technologies for the EU Cyber Direct – EU Cyber Diplomacy Initiative project. Csernatoni is presently co-leader of the "Governance of Emerging Technology" Research Group with the Centre on Security and Crisis Governance, at the Royal Military College Saint-Jean, Canada. She is also Visiting Faculty on Technology, Security, and High-tech Warfare with the Department of International Relations of Central European University in Vienna, Austria.

Ramon Pacheco Pardo is KF-VUB Korea Chair at the Centre for Security, Diplomacy and Strategy of the Brussels School of Governance and Professor of International Relations at King's College London. He is also a committee member at CSCAP EU, adjunct fellow (non-resident) with the Korea Chair at Center for Strategic and International Studies and non-resident fellow with Sejong Institute. Pacheco Pardo currently supports the implementation of ESIWA in South Korea and the EU-ROK Policy Dialogue Support Facility. He has testified before the European Parliament and advised the Organisation for Economic Cooperation and Development, the EEAS, the South Korean Ministry of Foreign Affairs and the UK's Cabinet and Foreign, Commonwealth & Development offices, in matters related to the Indo-Pacific, the Korean Peninsula and Europe-Asia relations. His latest book is Shrimp to Whale: South Korea from the Forgotten War to K-Pop (Hurst and Oxford University Press).

Funded by the European Union

The Indo-Pacific Futures Platform

The Centre for Security, Diplomacy and Strategy (CSDS) seeks to contribute to a better understanding of the key contemporary security and diplomatic challenges of the 21st century – and their impact on Europe – while reaching out to the policy community that will ultimately need to handle such challenges. Our expertise in security studies will seek to establish comprehensive theoretical and policy coverage of strategic competition and its impact on Europe, whilst paying particular attention to the Transatlantic relationship and the wider Indo-Pacific region. Diplomacy as a field of study will be treated broadly and comparatively to encompass traditional statecraft and foreign policy analysis, as well as public, economic and cultural diplomacy.
www.brussels-school.be/research/security-diplomacy-and-strategy

VUB BRUSSELS SCHOOL OF GOVERNANCE

The Brussels School of Governance is an alliance between the Institute for European Studies (Vrije Universiteit Brussel) and Vesalius College.

Visitor's address:
Pleinlaan 5, 1050 Brussels, Belgium
Mailing address:
Pleinlaan 2, 1050 Brussels, Belgium

info_bsog@vub.be

www.brussels-school.be