



MAY 2020

Digital connectivity going global The case for digital ODA

Support for digital infrastructure, literacy and the e-economy is vital for the development of countries neighbouring Europe. A focus on digital Official Development Assistance (ODA) as a cornerstone in **Europe's digital connectivity agenda** can help deliver inclusive and sustainable growth in Europe's periphery, while also serving Europe's economic and strategic interests. Only with greater presence of European companies in the e-economy can the European Union (EU), with partners, push back on the negative effects of China's Digital Silk Road, which is spreading authoritarian norms in the field of cyber security and internet governance, including high-tech surveillance. With an eye to practical implementation, this Clingendael Policy Brief adds conceptual clarity to what digital ODA is (or can be) and discusses where the EU stands today. It offers opportunities for best-practice learning from Asian players that have more experience in this field. Clearly, digital ODA is no longer just a technical but also a (geo)political issue.

Introduction

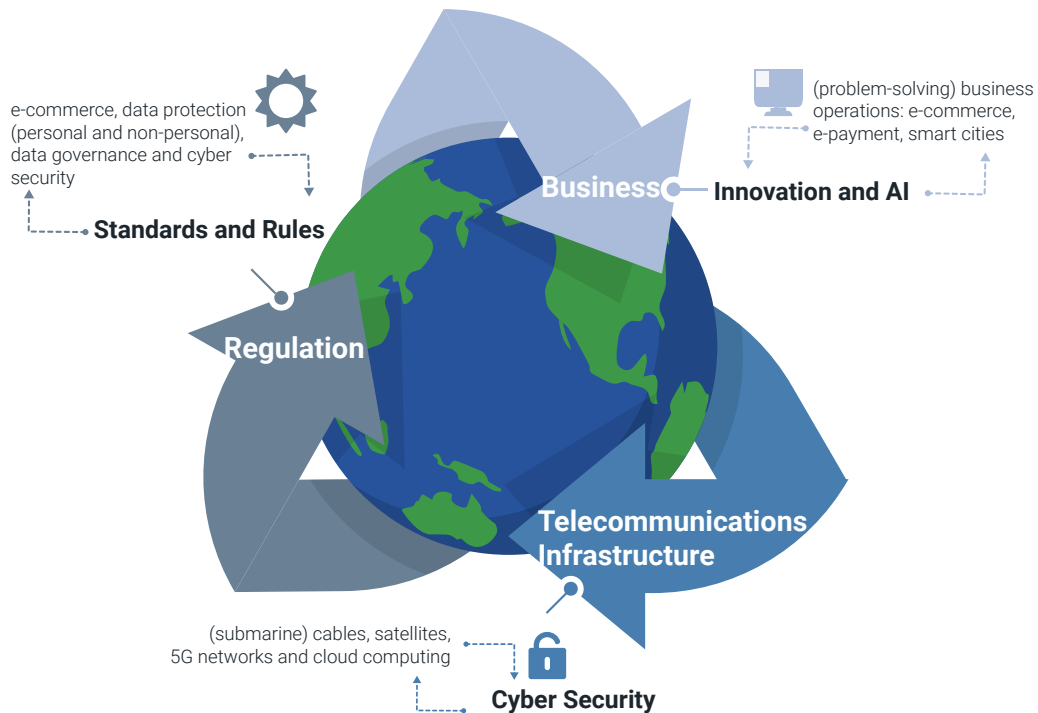
Digital connectivity will feature prominently in the EU–Japan summit this year, and in the EU–Africa summit scheduled for November 2020. On both occasions, digital Official Development Assistance (ODA) deserves a more prominent place on the agenda than seen so far. For [Japan](#), this means implementing coordinated digital development initiatives and aiming for greater contributions to the e-economy and e-government, and for [African](#) governments, the European Union (EU) should identify real needs that inform targeted, request-based action on digital ODA.

While acting on long-term challenges, digital ODA addresses several [key priorities](#) identified by the European

Commission. These priorities include making the EU fit for the digital age, reinforcing multilateralism, contributing to the Sustainable Development Goals (SDGs), and reinventing the EU's partnership with Africa. An updated EU digital ODA agenda also responds to [global trends](#) such as the impact of the fourth industrial revolution in Europe and its backyard, life in a post-COVID-19 world, international migration and climate change, as well as [geostrategic challenges](#) like the US–China technology conflict and China's Digital Silk Road.

This Clingendael Policy Brief will offer [ideas and suggestions for how to strengthen Europe's agenda on digital ODA](#) – first, by adding conceptual clarity and focus, and second, through best-practice learning from Asian players. As such, it fills a gap

Figure 1



Source: adjusted from Okano-Heijmans (2019)

left by the September 2018 [EU Connectivity Strategy](#), which dedicates less than half of its 13 pages to digital connectivity. It will outline key challenges and introduce several relevant initiatives by the EU, before asking what lessons may be learned from EU partners in East Asia such as Japan, South Korea and Singapore, which have long been actively involved in digital ODA-like activities, and how and why closer cooperation might be in each other's interest.

Digital ODA: what and why?

In essence, digital ODA entails technical assistance to developing countries and emerging economies, helping them to address the digital challenge that developed countries also face. Digital ODA should be implemented in each of [digital connectivity's three strands](#) – namely, telecommunications infrastructure, regulation and business – and aim for both practical and strategic objectives (see Figure 1). In the regulatory field, the digital ODA agenda should focus primarily on digital capacity-building –

that is, assisting third countries on how to establish data-protection structures and prevent cyber-crime, and cross-border e-commerce and data-transfer rules.

In so doing, the EU can also promote an inclusive, human-centred and open information and communication technology (ICT) environment. Digital ODA in the business dimension could help to ensure that the fourth industrial revolution and the e-economy foster inclusive growth, also in these countries. It will enable them to keep control over their own data for their domestic businesses' development, rather than allowing foreign companies to gather local data and use it for their own benefit. Finally, on the telecommunications infrastructure side, digital ODA can play a role in helping to design, build and secure telecommunication and data infrastructure – and thereby spread European standards, including on cyber security. After all, as per the [EU Connectivity Strategy](#), 'high-capacity network links are critical to support the digital economy [...and...] universal and affordable access to the internet is a proven enabler of socio-economic development'.

Three recent EU documents show that the EU and its member states are stepping up their act. First is the digital strategy ‘[Shaping Europe’s Digital Future](#)’ of February 2020, which also addresses the international dimension – or Europe’s role as a global player. Second is the September 2019 [EU–Japan Partnership on Sustainable Connectivity and Quality Infrastructure](#), where, thematically, digital connectivity stands out as the preferred field of cooperation. And third, the April 2020 communication ‘[Towards a Comprehensive Strategy with Africa](#)’ also has a significant digital element. This follows the creation in December 2018 of the [European Union–African Union Digital Economy Task Force \(EU–AU DETF\)](#), which in June 2019 recommended actions towards (1) access to affordable broadband connectivity and digital infrastructure; (2) digital skills; (3) digital entrepreneurship; and (4) e-services: e-government, smart cities, e-commerce and e-health.

Success in digital ODA requires that action follows these documents. This necessitates digital ODA being properly budgeted, staffed and coordinated, which is not the case today. Programmes also need to target emerging economies rather than only the traditional developing countries for ODA (like the digital ODA strategy of the Netherlands) or just Asian countries (as per the EU’s connectivity strategy). Finally, digital ODA stands to benefit from better coordination, for example with partners in Asia. This Clingendael Policy Brief aims to contribute to this latter point.

International challenges pushing digital ODA

In spring 2020, the self-proclaimed ‘geopolitical European Commission’ led by Ursula von der Leyen sees itself confronted by three global challenges that should stimulate the broadening of digital ODA: the COVID-19 crisis; the US–China tech rivalry; and China’s engagement of African countries in the framework of the Digital Silk Road.

COVID-19 has focused all governments’ attention on SDG3: health. As global supply chains are more integrated than ever, and technology a more significant part of everybody’s daily life, COVID-19 highlights the need for closer cooperation on detecting, monitoring and preventing epidemics, including with digital tools. However, just when the EU proposed a [pan-European coordinated approach for a mobile contact-tracing app](#) that could have also been beneficial in developing countries, two US tech giants – Apple and Google – introduced their own solution. The European Commission has now begun talks with Apple about an app that would abide by EU data standards.

New technologies can make significant contributions to [realising the Sustainable Development Goals](#). Some of the core development sectors, such as agriculture, education and healthcare (SDGs 2, 3 and 6), will undoubtedly benefit from digital technologies – such as by connecting rural farmers to market information, remote learning and communicable disease management – and they can also be applied in a cross-sectoral fashion. International cooperation is needed to achieve the full social and economic potential of digital technology.

Geostrategic challenges for European and Asian partners

This brings us to the second long-term trend that should inform European digital ODA: the [US–China tech conflict](#). As developing countries become a playground of US–China rivalry, this leaves the EU and its member states – and partners – with a role and responsibility to show that there is a ‘third way’, beyond what China and the US propose. Digital ODA can contribute to [securing liberal norms](#) such as openness, data privacy and transparency, rather than allowing an all-too-strong state or dependence on giant technology companies. After all, long-term support of third countries’ governments can only be achieved through persuasion, not force.

China is another key player in digital connectivity. Its Digital Silk Road (DSR), which is part of its broader Belt and Road Initiative, aims at promoting and facilitating the digital economy, including cross-border e-commerce and digital payment, in developing countries and emerging economies.¹ However, China's strong footprint on the ground also contributes to the [spread of authoritarian norms](#) in the field of cyber security and internet governance, including high-tech surveillance. China has already used Chinese-built information technology (IT) infrastructure to spy on governments and international institutions in Africa and is exporting its high-tech surveillance (such as mass facial recognition), for example to Zimbabwe. This is leading to accusations of an ['authoritarian future for the internet'](#) if China is in control of core IT infrastructure. Hence, there is a strong incentive for the EU and its member states to step up their game in Africa.

Digital ODA in Europe's backyard

In the last decade, the EU has been trying to improve its cyber capacity-building capabilities in developing countries, by strengthening the functioning and accountability of these countries' institutions to enhance their effective response to cyber-crime and a country's cyber resilience. This has become a core element of the EU's international cooperation policy to spread the EU's vision for a free, open, peaceful, secure and interoperable cyberspace. Simultaneously, the EU also began to promote the [mainstreaming of digital technologies and services into EU development policy as 'Digital for Development' \(D4D\)](#). One core objective is building affordable and secure broadband connectivity, promoting digital literacy and digital entrepreneurship, paired with

sustainable development, through ['a series of concrete and demand-driven actions'](#) between 2017 and 2020.

Regulation

Some D4D projects intend to improve regulation and cyber-security norms and regulations. Examples are [Cyber4Dev](#) (2018 and 2021) to promote cyber resilience and cyber security, with projects in Kenya, the Democratic Republic of Congo (DRC), Rwanda and Mauritius. The [West African Response on Cyber Security and Fight Against Cybercrime \(OCWAR-C\)](#) aims at enhancing security and combating cyber-crime in the Economic Community of West African States (ECOWAS) region, and two joint EU and Council of Europe projects – [CyberSouth](#) in Northern Africa and the [Global Action on Cyber-Crime Extended \(GLACY\)+](#) – focus on strengthening legal and policing institutions to combat cyber-crime. Meanwhile, the EU's Policy and Regulation Initiative for Digital Africa (PRIDA) with the African Union aims at harmonising the legal and regulatory framework for the use of ICT for social and economic development in Africa. The [EU budget](#) for these projects is a mere € 42 million for the period 2018–2021.

Telecommunications infrastructure

Other EU projects focus on developing or improving IT infrastructure. At a [D4D multi-stakeholder event](#) in March 2019, Carla Montesi of the European Commission's Directorate-General for Development and Cooperation reiterated that the EU intends to 'accelerate inclusive, sustainable development in EU partner countries around the world, with an immediate focus on Africa'. Priority would be on (1) the development of optical fibre backbones from the Sahara to the Central African Republic (CAR); (2) digital skills; (3) digital entrepreneurship, including financial inclusion; and (4) digital enablers from e-health to e-government, such as AfricaConnect3. The European Investment Bank (EIB) has also been involved in improving telecommunications infrastructure and connectivity in Africa through the EU–Africa Infrastructure Trust Fund. Between 2015 and 2020, the EIB sponsored projects worth about € 120 million, such as the expansion of

1 Majcherczyk, M. and Shuqiang, B. (2019), 'Digital Silk Road: The Role of Cross-Border E-Commerce in Facilitating Trade', *Journal of the WTO and China*, 9(2), pp. 106–128.

telecommunications infrastructure in Kenya, the construction of solar-powered mobile towers in sub-Saharan Africa (especially the DRC), and the expansion of high-speed internet access in cities across Angola. In comparison, [China's annual ODA spending for ICT in Africa](#) in 2014 alone was about € 350 million, which rose to over € 1 billion with the start of the Digital Silk Road.

Business

Improving IT infrastructure or building payment systems that further the financial inclusion of large segments of the population enhances business opportunities for African companies. These actions can also be interesting channels of investment for European companies. However, European governments and companies are confronted by two challenges. The first is that China often conflates its international cooperation (mostly loans with few strings attached) with its commercial interests, while the EU separates them. The EU's second challenge concerns its fragmented telecommunications sector.² The [global market for telecommunications equipment](#) is dominated by Chinese, US and Japanese companies, with Ericsson and Nokia ranking fifth and sixth globally in 2018. This gives [China an advantage in Africa](#), where the EU is already far outspent by China's Digital Silk Road projects. Companies like Huawei, ZTE or China Telecom are already dominant players, building data centres, smart cities, 4G and soon 5G networks in more than a dozen countries throughout Africa. In 2014 alone, [Chinese investment in Africa](#) amounted to US\$ 37 billion, with US\$ 7 billion as ODA. While furthering much-needed economic development in these countries, this is also [spreading illiberal Chinese high-tech standards and winning China partners to help advance its vision of more autocratic internet governance](#).

While these examples of EU regulatory, telecommunications-infrastructure and business development initiatives in Africa are well-intended first steps for digital ODA

2 Only the German Telekom, Spanish Telefonica and French Orange are among the global top 20 telecommunication market leaders.

with a European face, they suffer from the diversity of implementing EU bodies, insufficient funding and staff, and a lack of permanent institutions. While this was less of an issue when Europe was the dominant development actor in Africa, China's growing influence means that coordinated action within Europe and its partner countries has never been more critical.

Digital ODA in Asia

The first reason why it makes sense to compare the digital challenges and assistance activities in East Asia with those of Europe in Africa is a similar need to bridge the North-South digital divides in both regions.³ The second reason is the growing economic, technical and norm-shaping influence of China in both regions. China's Digital Silk Road aims, among other things, at government control of IT infrastructure and has low regard for a free and open internet. Looking at some of the actions and programmes of Japan, Singapore, South Korea and India can therefore inform the discussions about digital ODA in Europe.

Japan

Japan's core focus in digital development has long been on improving the cyber capacity of less cyber-mature countries, with a strong focus on South-East Asia. Japan's Strategy for Cyber Security aims at (1) sharing its expertise and coordination of policies, (2) assisting in incident response and (3) capacity-building, and encourages Japanese companies and other stakeholders to contribute to the security of cyberspace and the security environment in other countries. Japan takes a strategic view on cyber capacity-building, as it considers the protection of Japan a core incentive for strengthening and improving cyber capacities in developing countries, given that attacks on their IT infrastructure

3 The digital divides refer to economic and social inequalities among populations because of differences in access to, use of, or knowledge of ICT; see ASPI International Cyber Policy Centre (ICPC) (2017), *Cyber Maturity in the Asia-Pacific Region, 2017*, Australian Strategic Policy Institute.

can undermine Japan's cyber security. The second core incentive for Japan is norm-setting in the recipient countries, or strengthening an understanding, awareness and support for an open and free internet and the rule of law in cyberspace. Japan's latest success is the opening of the [ASEAN-Japan Cybersecurity Capacity-Building Centre \(AJCCBC\)](#) in Bangkok in September 2018, whose core objective is improving the skills of security-related agencies in ten Association of South-East Asian (ASEAN) countries and establishing an ASEAN-CERT (Computer Emergency Response Team). The EU could adopt a similar frequency of ministerial-level meetings and permanent institutions for capacity-building on the ground.

Singapore

Singapore is undoubtedly one of the most active players in cyber security and cyber capacity-building in South-East Asia and for ASEAN members in particular. In 2016, Singapore brought telecommunications and other relevant ministers together for the first [ASEAN Ministerial Conference on Cybersecurity \(AMCC\)](#), aiming at (1) tighter regional cyber security cooperation and (2) the use of digital technologies for economic progress and improvement of living standards across the region. To make such cooperation more permanent and to enable practical and technical cooperation, Singapore suggested the establishment of an [ASEAN Cyber Capacity Programme \(ACCP\)](#) to help ASEAN nations improve their IT infrastructure to counter cyber threats, through cyber capacity-building and confidence-building measures. One result was the opening of the [ASEAN-Singapore Cybersecurity Centre of Excellence \(ASCCE\)](#) in Singapore in October 2019. The permanence of inter-regional institutions and a training centre could guide EU activities in Africa.

South Korea

South Korea's digital ODA is active in Asia and Africa. In Asia, South Korea's Overseas Infrastructure Development Support Corporation (KIND) supports Korean companies to advance into the region's infrastructure development projects through continuous monitoring and support

– bilaterally and through the [ASEAN Global Infrastructure Fund](#). KIND also aims at improving 5G networks in ASEAN countries and India through the 2019 5G+ 'Strategy for the Realisation of Innovation and Growth' initiative. In Africa, South Korea cooperates in multiple bilateral and multilateral initiatives on cyber issues. For example, the [Korea Internet and Security Agency \(KISA\)](#) provides Tanzania with the expertise to monitor the security of its IT infrastructures; and the [Cybersecurity Alliance for Mutual Progress \(CAMP\)](#) cooperates with organisations from 37 countries 'with the purposes of achieving sustainable benefits and serving as a platform where members prepare themselves with collective actions to keep cyberspace safe'.

India

India's potential for digital ODA stems largely from its domestic experience with the use of digital tools to spur development. India had remarkable success with its efforts to enhance [digital financial inclusion](#) through digital payment systems. The question now is whether this success can be exported to other developing countries, either by India as a development player on its own, or in a trilateral format with European partners. Trilateral cooperation with Indian companies with a proven track record could facilitate improved access to countries, particularly in Africa. Cooperation may be sought with India's [Centre for Digital Financial Inclusion \(CDFI\)](#), which promotes the use of technology to support its welfare programmes and financial mainstreaming for the poor, with a valuable track record on digitising benefits' delivery, from implementing data-driven frameworks from governance to farm services, and promoting basic financial literacy using digital communication tools. For now, it operates only within India, but its experiences could be of benefit to individuals in many other developing countries.⁴

4 Author's interview with CDFI director Krishnan Dharmarajan on 17 January 2020, Bangalore.

Conclusion: digital ODA in the post-coronavirus world

As digital and communications technology has revolutionised societies, economies and everyday life, digital technologies have gradually become part of 'technical' development policies in Europe and Asia. However, in recent years, digital technologies exported by large IT companies steered by Beijing have also weakened inclusive growth, while strengthening authoritarian systems. Partner countries in Asia have taken the lead in broadening digital ODA from merely technical and infrastructure to a norm-setting and regulatory agenda, offering developing countries a diversification, preventing an (over)reliance on China and strengthening their resilience. Europe now needs to step up its efforts as well.

Among digital connectivity's three strands, Japan, South Korea and Singapore have been mainly focusing on the improvement of telecommunications infrastructure and standard- and norm-setting through open and transparent regulations. One lesson from these countries is the importance of [permanent capacity-building centres](#), which improve not only technical competencies but also disseminate norms that secure the continued open and free access to information for all citizens. All three countries have also developed a partnership mechanism through [regular ministerial meetings](#) with ASEAN, which make sure that the less cyber-secure and therefore more vulnerable countries are treated as equal partners.

The lesson from India is that digital development efforts should not focus only on the defensive side (mitigating security challenges) but also help to create opportunities offered by the e-economy. This would enable developing countries to develop and implement solutions to achieve

[digital financial inclusion](#) or [data-driven networks](#) that are uniquely suited to their specific needs and spur socio-economic development. Countries in Europe's neighbourhood could benefit from India's experience, but India is unlikely to export its efforts because of limited government capacity. Trilateral cooperation between the EU and India – and Japan – in third countries on digital ODA could help to leapfrog stages of development, and, most importantly, [the dissemination of standards and norms](#). This is particularly important, as India's data privacy policy contains both EU and Chinese elements.






When it comes to the business component of digital connectivity and digital ODA, Japan, South Korea, Singapore and EU member states have a hard time competing with China in Africa. If Europe wants to develop a footprint in Africa's 5G and telecommunications market, it is crucial to combine the forces of major European telecommunication companies and intensify cooperation with Asian partner countries. The [EU's connectivity partnership with Japan](#) is an excellent first step to broaden the regional focus to Europe's neighbourhood, including Africa, rather than on Asia alone. In conclusion, the EU and its Asian partners should [deepen mutual learning](#) about their respective digital development strategies in their backyards, but, equally important, they should [combine their forces](#) in Asia and Africa to increase effectiveness.

Even if Covid-19 focuses attention in the short and medium term to economic recovery within the EU, China's unwavering action shows that the strategic challenge of digital development cannot be pushed out to the long term. Digital ODA must be taken for what it is: a cross-cutting issue rather than one of the traditional development domains, a geopolitical as well as technical issue, and a concern that requires a dedicated budget and people.

About the Clingendael Institute



Clingendael – the Netherlands Institute of International Relations – is a leading think tank and academy on international affairs. Through our analyses, training and public debate we aim to inspire and equip governments, businesses, and civil society in order to contribute to a secure, sustainable and just world.

www.clingendael.org
info@clingendael.org
+31 70 324 53 84



 @clingendaelorg
 The Clingendael Institute
 The Clingendael Institute
 clingendael_institute
 Newsletter

About the authors

Maaïke Okano-Heijmans is a Senior Research Fellow at the Netherlands Institute of International Relations ‘Clingendael’ in The Hague. She is also a visiting lecturer at the University of Leiden.

 mokano-heijmans@clingendael.org
 @MaaïkeOh

Wilhelm Vosse is Professor of Political Science and International Relations at the International Christian University (ICU) in Tokyo. In 2019/20 he is a Visiting Professor at The University of Warwick, UK.

 vosse@icu.ac.jp
 @vosse

DISCLAIMER: Research for and production of this report was conducted within the PROGRESS research framework agreement. Responsibility for its contents and for the opinions expressed rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defence.