



JULY 2019

## How to strengthen Europe's agenda on digital connectivity

Connectivity is high on the EU's agenda, but its digital dimension remains underdeveloped. The short paragraph on digital in the EU connectivity strategy is telling. The EU's distinct approach to digital connectivity – with a focus on the internal market, rule-making and development – differs from similar strategies, particularly China and its Digital Silk Road. Needed, now, is a comprehensive strategic vision that spurs action on all three practical elements of digital connectivity – namely, telecommunications infrastructure, business and regulation – and gives strategic guidance in the political and even securitized sense, and not only from a market perspective.

As the US–China trade war evolves into a more permanent conflict at the nexus of trade, technology and data, Europe needs to act on the challenges of digital connectivity. An edge in innovation and Artificial Intelligence (AI) is crucial, as digitization transforms the global economy. Moreover, dominance in the fields of data and technology is vital for military dominance, and the United States has shown no restraint in demanding support from its allies to maintain its leading position. The call to ban Huawei from providing 5G infrastructure is the most well-known such example. But the United States' push for a new export control regime for emerging technologies illustrates that the US–China conflict is impacting the EU and its member states and their relations with the United States and China in other fields as well. The EU needs to act if it is to remain a relevant player in the global reconfiguration of power and sources of power.

The EU's 'Europe–Asia Connectivity Strategy', adopted in October 2018,<sup>1</sup> should help the EU and its member states on their way, but falls short of providing the necessary strategic guidance in the digital field. Essentially a value proposition for sustainable, comprehensive and rules-based connectivity, the strategy largely focuses on the field of transport. This focus may have seemed natural considering the boom in Chinese investments and loans for infrastructure development in Europe recent years, but today, as the fourth industrial revolution<sup>2</sup> sparks a more conflictual international environment, European stakeholders are left ill-equipped to deal with growing challenges in the field of digital connectivity.

1 [Connecting Europe and Asia: Building blocks for an EU strategy](#), 19 September 2018, p. 5.

2 The Fourth Industrial Revolution is characterised by 'a fusion of technologies that blurs the lines dividing the physical, digital and biological spheres'. See Klaus Schwab, [The Fourth Industrial Revolution: what it means and how to respond](#), World Economic Forum, 14 January 2016.

## What is digital connectivity?

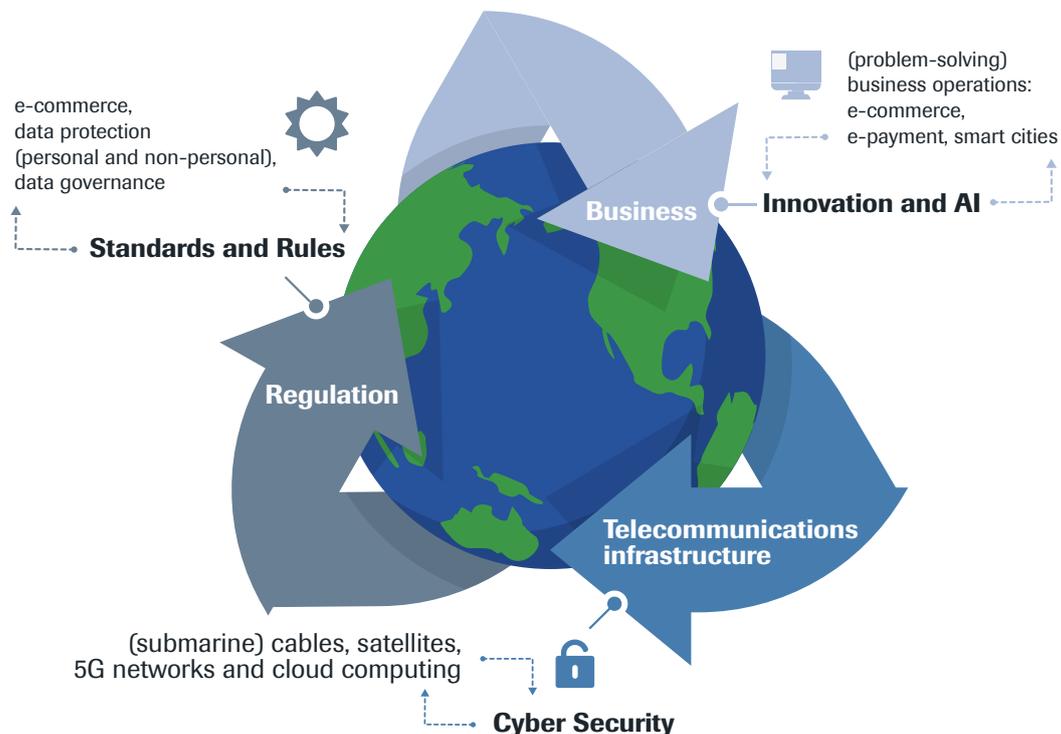
As concerns connectivity, the primary need for European capitals, businesses and consumers today is for strategic guidance and practical assistance in the digital field. This means equipping stakeholders to reap the opportunities that digitalization offers for any economy, and to guide them through the emerging stand-off that arises because of countries' varying normative interpretations and practical applications of digital and data.

As illustrated in Figure 1 below, digital connectivity in the practical sense involves three core elements: telecommunications infrastructure; business operations; and (international) regulation. Telecommunications infrastructure refers to the hardware and software of the physical networks that are necessary for the digital economy to function – that is, its (submarine) telecommunications cables and satellites, as well as 5G and cloud computing. Business operations 'fill' the digital economy, with, for example, e-commerce and e-payments.

Taken together, these activities could contribute to the development of so-called 'smart cities' where data can be collected to analyse and effectively tackle public challenges, ranging from transportation and traffic to waste management, schools and even crime detection. Finally, digital connectivity has an institutional dimension that supports the digital economy, aiming to make it transparent, rules-based and fair. Today, this includes negotiations on (international) regulation for e-commerce and taxation, as well as for the protection of (non-)personal data.

Importantly, each of these three practical elements has an underlying strategic dimension. At this level, digital connectivity refers to cyber security – in particular, the strategic/security consequences of the rollout of 5G telecommunications infrastructure; positioning in the global race for supremacy in innovation and AI; and standards and rule-setting in data governance in the digital age.

**Figure 1 Digital connectivity: practical and strategic elements (author's compilation)**



## The EU's digital agenda

The EU connectivity strategy illustrates the Union's focus on (domestic) regulation and access in the digital field. The strategy's short paragraph on digital emphasizes the importance of high-capacity network links that are critical for supporting the digital economy (access) and the regulatory environment. As such, it largely reflects the basics of the EU's Digital Single Market (DSM) strategy, adopted in 2015, even if the DSM as such is not referenced in the strategy. Also evident from the EU's connectivity strategy is the emphasis on digital networks and the Digital4Development framework. While the strategy also states the importance of 'a coherent regulatory approach', the multilateral agenda for digital/data regulation is – somewhat surprisingly – left unmentioned.

To understand better the core of the EU's digital agenda thus requires a closer look at the DSM, which is overseen by the Directorate-General for Communications Networks, Content and Technology (DG CONNECT). The DSM strategy is built on three pillars: access; environment; and economy and society.<sup>3</sup> Access is about enabling consumers and businesses to access and engage with digital goods and services across Europe, thereby narrowing the so-called 'digital divide' (the ever-growing gap between members of society without computer or internet access and those with access). Environment is about creating the right conditions and a level playing field for digital networks and innovative services to flourish. Ultimately, better access and regulatory intervention serve to maximize the growth potential of the EU digital economy. After all, a seamless EU market helps to nurture European champions by allowing companies to scale up at home and subsequently be successful on the global stage.

---

3 See the European Commission's website on [Shaping the Digital Single Market](#).

While the DSM is essentially the EU's internal digital agenda, the Digital4Development framework is its external element, overseen by the Directorate-General for Development (DG DEVCO).<sup>4</sup> This is about integrating digital technologies into EU development policy, thus contributing to the Sustainable Development Goals (SDGs). Effective implementation has lagged, however, partly because of a lack of budget and staffing to implement the strategy effectively in third countries. New funds will become available only in 2021.<sup>5</sup>

Essentially, the DSM and Digital4Development form the EU's approach to the infrastructure and (domestic-internal) regulatory elements of digital connectivity. Practical in nature and crafted with domestic objectives in mind, however, they do not incorporate strategic-level thinking on two key issues. With regard to security, this entails cyber-security elements of telecommunications infrastructure development; and on the business side, this refers to the added value of having European companies that operate successfully in the global digital economy.

Parallel with these digital connectivity initiatives, Europe has invested much in regulation on personal data protection, which is now having surprisingly large effects beyond its borders. The EU's General Data Protection Regulations (GDPR), in particular, are spurring action by others in this field. Countries as varied as members of the Association of South-East Asian Nations (ASEAN) and Nigeria, for example, are wanting to learn from Europe's approach. Meanwhile, other governance frameworks are being developed to regulate the free flow of personal data. The Asia-Pacific Economic

---

4 See Staff Working Document on ['Digital4Development: mainstreaming digital technologies and services into EU Development Policy'](#), 2017, p. 157.

5 The European Commission has proposed promoting digital connectivity with Asian and other countries through the Connecting Europe Facility for the period of 2021–2027. See Communication, ['A modern budget for a Union that protects, empowers and defends'](#), COM(2018)321.

Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system is one such example.<sup>6</sup> A challenge for the future will be to prevent a modern version of Jagdish Bhagwati's famous 'spaghetti bowl effect', which points to the risk of too many crisscrossing agreements (then, in free trade) hampering freer and more open global trades.

Clearly, this challenge also applies to the flow of non-personal data across borders, for which the EU adopted a new regulation in May 2019.<sup>7</sup> Referred to as the emergence of a 'splinternet', the risk now is of a fragmented internet because of different national regulations that confine valuable reservoirs of information within national borders. However, countries with restrictive data transfer regulations that associate data governance with political and social control – such as China, Russia and India – will see little benefit in cooperation. And for European companies, Chinese or Russian regulations are clearly problematic, as they infringe on intellectual property.

Recognizing that each country's domestic data governance needs to be global in scope and interoperable given the globally distributed nature of the internet,<sup>8</sup> the EU thus joined Japan's push for a concept known as Data Free Flow with Trust (DFFT). This initiative aims to create a set of international rules enabling the free movement of data across borders with trust. For instance, a (government) guarantee of strong cyber-security measures and intellectual property safeguards could facilitate freer movement of important industrial data, such as those of health and vehicles.

Summing up, while the EU is pushing for improved digital infrastructure and is clearly active in the regulatory field, business operations and strategic thinking on digital connectivity outside EU borders remain underdeveloped. Also, in the Asia-Europe Meeting (ASEM), where the EU pushed forwards the multilateral debate on sustainable connectivity, the digital element remains underdeveloped. The ASEM Connectivity Inventory, which was launched just days after the EU's connectivity strategy, showed that only eight of 112 ASEM events during the period 2013–2018 focused on information and communication technologies (ICT) and digital technologies, and only one on digital connectivity.<sup>9</sup> For its part, the ASEM Sustainable Connectivity Portal, which was also published in October 2018, includes just one digital indicator: connection speed.<sup>10</sup>

## Broadening the European approach

Turning back to digital connectivity's practical and strategic elements, as illustrated in Figure 1, it becomes clear that the key challenge for the EU and its member states today is to broaden their approach and their action. At present the EU primarily focuses on the element of regulation – and within that, EU internal regulation – while lagging behind in much-needed investments in innovation and AI to develop (problem-solving) digital business.<sup>11</sup> Also, until recently, little attention has been given to the strategic dimension of digital connectivity's hard infrastructure. This is illustrated by failure initially to discuss the security of next-generation telecommunications infrastructure, and the

6 For a useful comparison between GDPR and CBPR, see María Vasquez Callo-Müller, *GDPR and CBPR: Reconciling personal data protection and trade*, APEC Policy Support Unit, Policy Brief no. 23, October 2018.

7 See [Free flow of non-personal data](#), 7 June 2019.

8 Nigel Cory, Robert D. Atkinson and Daniel Castro, *Principles and policies for 'data free flow with trust'*, Information Technology & Innovation Foundation (ITIF), 27 May 2019.

9 This event concerns the [ASEM high-level forum](#), which was held in China in June 2017: [ASEM Connectivity Inventory](#).

10 [ASEM Sustainable Connectivity Portal](#).

11 The EU is catching up, however, looking for a way to embrace the opportunities offered by AI in a way that is human-centred, ethical, secure and true to the EU's core values. See, for example, the report by the EU's Joint Research Centre: [Artificial Intelligence: A European perspective](#), 2018.

role of China's equipment provider Huawei within this. Owing to intense pressure from Washington – which is calling on EU member states to ban Huawei from providing their 5G infrastructure – a common EU approach to the security of 5G is now being prepared.<sup>12</sup> Clearly, the EU's focus on internal regulation and digital access, has left unaddressed some of the key digital challenges facing European stakeholders today – that is, the business element of digital connectivity, as well as the strategic dimensions of business and telecommunications infrastructure.

The EU and its member states must also act on the normative digital divide that exists, particularly with China and to a lesser extent with the United States. After all, data, for China, constitute a valuable enabler of the high-tech surveillance state. This contrasts with Europe, which considers a role for the state in protecting and regulating data, but not controlling it. The United States goes one step further by championing a free-trade approach, focusing on data as something to be commercialized.<sup>13</sup>

The growing presence of Chinese technology champions such as Huawei, Alibaba, ZTE and Tencent – supported by the Chinese state – will further China's vision for state-led internet governance and may facilitate its espionage and security services and even export these to third countries. Many in ASEAN reportedly now admire China for its technologies over the United States or Japan – including China's digital menu boards and e-payment services in restaurants.<sup>14</sup> Tellingly, all of ASEAN's 'unicorn companies'<sup>15</sup> are backed by equity from Chinese technology giants, such as Didi Chuxing Technology Co.'s investment in Singapore's ride-hailing

service company Grab (which purchased Uber's South-East Asian business in 2018).

Furthering the European value proposition requires that European infrastructure and e-business players are present on the ground. Also, financial tools are needed to coordinate strategically with like-minded countries such as Japan and the United States – both at the government level, as well as in infrastructure finance and in public-private partnerships that further problem-solving digital businesses. Only by cooperating with others do the EU and its member states have a chance of success in offering business- and value propositions that rival the operations and influence of China's (state-backed) tech giants in third countries.

## China's Digital Silk Road

Compared to the EU's regulatory approach, key elements of the digital-connectivity strategy of others – especially China, with its Digital Silk Road (DSR) – are both at a higher level of strategic action and are business-oriented at the same time. The DSR is about hard infrastructure – that is, constructing and expanding existing telecommunications networks. This includes ICT infrastructure such as fibre-optic (submarine) cables – notably by Huawei Marine – and 5G networks and cloud computing – notably by Huawei and Alibaba Cloud. Offering network security for China's Belt and Road Initiative (BRI) investment recipients is an important element of the BRI now, and this role is expected to grow in the future as advanced infrastructure networks advance.<sup>16</sup>

The DSR is also about business operations: promoting exchanges via the establishment of digital marketplaces. Known examples in e-commerce include China's Alibaba; in the car-sharing industry, China's Tencent and Didi Chuxing, but also Singapore's Grab and Indonesia's Go-Jek; and in the e-payment

12 Details available on the European Commission's website, see [here](#).

13 Control Risk, [RiskMap2019: Top five risks for 2019](#).

14 Hirobumi Kayama, Special Adviser to Japan's Ministry of Economy, Trade and Industry, at the event 'China's Digital Silk Road', Washington, DC: CSIS, 5 February 2019. Transcript available [online](#).

15 A 'unicorn' is a privately held start-up company whose value is estimated at more than 1 billion US dollars.

16 Kieran Green, [Securing the Digital Silk Road](#), Washington, DC: Center for Advanced China Research, 11 February 2019.

market, notably Alipay. Both elements come together in smart city projects, which some distinguish as a third element of the DSR.<sup>17</sup> China's edge in AI and innovation is important, as dominance in the fields of data and technology is also a key to military dominance.

China's push into the global digital economy has been largely driven by its national technology champions Huawei, Alibaba and Tencent. These companies have been able to deliver high-quality products at low cost, partially because of Chinese government support, even if Beijing's role in supporting the DSR has been more low-key than other BRI components.<sup>18</sup>

Notably, while e-governance and e-business regulations appear to be largely missing in China's DSR, this soft element does feature in the digital strategies of Japan and the United States, which otherwise resemble China's approach. The United States and Japan, for example, are both moving on digital – individually and in synergy – including in their Free and Open Indo-Pacific policies. Alongside this regulatory push, both seek a share of the digital economy in third countries, by nurturing and maintaining, as well as investing in digital companies. Moreover, as China catches up in several high-technology fields, the United States is demanding support from its allies to maintain its leading position. The Huawei ban may have been the first – and, to date, the most well-known – such example, but the US push for a new export control regime for emerging technologies illustrates that more is yet to come.<sup>19</sup>

## Why Europe needs to act

Importantly, China's more strategic and practical – rather than regulatory – approach to the digital field is of significance to Europe and beyond.<sup>20</sup> First, European and other foreign firms are challenged to operate cost-effectively. In South-East Asia, for example, the digital economy has grown rapidly and is emerging as a new growth engine, catalysed by investments from external tech giants (largely from China, but also from Japan) and regional unicorns. Chinese companies increasingly rival – and outdo – other major players in their ability to expand their presence abroad rapidly, thanks to their innovative edge and government support.

Yet the consequences for the EU and its member states go beyond business operations to include also the normative and security spheres. There are, after all, risks about the hardware and software needed for the shift to a digital economy. Investments in network-security infrastructure abroad become a tool to further China's – restrictive – vision for internet governance. China's system runs counter to principles of free and accountable governance, and is successful already in Vietnam, for example.<sup>21</sup>

Moreover, the integration of Chinese security software into critical infrastructure could serve as a boon to China's espionage and security services. As regular software updates – rather than a one-off hardware installation – are needed, installing security checks is a bigger challenge than in earlier-generation technology. Although more infrastructure is needed to support digital activities, robust regulations are needed on key issues such as data privacy and cyber security.

---

17 Speech by Kayama, see footnote 14.

18 Green, *Securing the Digital Silk Road*.

19 See Martin Chorzempa, [\*The Trump administration's rush to curb technology leakage is in danger of backfiring\*](#), Washington, DC: Peterson Institute for International Economics, 8 January 2019; and Brigitte Dekker and Maaike Okano-Heijmans, *The US-China trade-tech stand-off and the need for European action on export control*, Clingendael Policy Brief (forthcoming 2019).

---

20 This builds on Green, *Securing the Digital Silk Road*.

21 Brian Harding, [\*China's Digital Silk Road and Southeast Asia\*](#), Washington, DC: Center for Strategic and International Studies (CSIS), 15 February 2018.

## Next steps

The EU has not been sitting still with regard to digital connectivity. A common EU approach to the security of 5G is in the making. On data privacy and security, the EU has acted to protect European consumers and individuals, particularly within the Union. In addition, at the World Trade Organization, the G20 and other forums, the EU is moving in cooperation with Japan and others to further a global framework that addresses cross-border internet policy, governed by the concept of data free flow with trust.

Missing, however, is a comprehensive strategic vision that spurs action on all three practical elements of digital connectivity and gives strategic guidance in the political and even securitized sense, not only from a market perspective. For European players to remain at the forefront of the fourth industrial revolution, problem-solving business operations of digital companies should be nourished and retained during the scale-up. This requires investments in innovation and technology – including in public-private partnerships – that nurture and maintain start-ups and ‘unicorns’. Awareness of the need for greater investments in and a strategic vision on AI is growing in the EU and must now be followed by action. European governments and companies can learn from digital advances elsewhere – especially in South-East Asian countries, which are leapfrogging ahead in the field and are inspired by China rather than by European, US or Japanese technologies.<sup>22</sup>

Platforms are needed for the EU and its member states to discuss digital connectivity with stakeholders elsewhere, just as the EU-China Connectivity Platform facilitates dialogue on transport connectivity with China and the Asia-Europe Foundation (ASEF) furthers human connectivity between European and Asian countries. There is ample room for the EU to engage with others on its best practices with the Digital Single Market, including through its Digital4Development framework, but

resources are needed for action outside the EU. Opportunities for best practice exchange and greater synergies are also evident in the field of cyber security – including 5G. After all, countries in South-East Asia and Africa are facing similar challenges to those that EU member states are currently facing – of having to balance cost and risk.

Now is the time to act on digital connectivity’s practical as well as strategic elements of hard infrastructure and business operations. This requires that European stakeholders do their groundwork – by way of investments in innovation, technology and public-private partnerships, as well as an allocation of funds – and thus reap the potential of strategic cooperation and coordination with partners elsewhere.

---

22 Speech by Kayama, see footnote 14.

### 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](http://www.clingendael.org)  
[info@clingendael.org](mailto:info@clingendael.org)  
+31 70 324 53 84

 @clingendaelorg  
 The Clingendael Institute  
 The Clingendael Institute

### About the author

**Maaïke Okano-Heijmans** is a Senior Research Fellow at the Netherlands Institute of International Relations 'Clingendael' in The Hague. She is a Scientific Coordinator of the Asia-Pacific Research and Advice Network (#APRAN) for the European Commission and the European External Action Service.

E [mokano-heijmans@clingendael.org](mailto:mokano-heijmans@clingendael.org)  
T @MaaïkeOh