

## BRIEF

CHINA'S DIGITAL SILK ROAD:  
OUTLINES AND IMPLICATIONS FOR  
EUROPE

| MARIA |

China's Belt and Road Initiative (BRI), launched in 2013, is a large-scale initiative encompassing infrastructure projects, trade and financial agreements, and cultural and defence cooperation with over 140 countries worldwide. The Chinese government devised the Digital Silk Road (DSR) as part of the BRI. In March 2015, China's National Development and Reform Commission (NDRC), the Ministry of Foreign Affairs, and the Ministry of Commerce released a white paper stating the need for "an Information Silk Road" to create cross-border optical cables and improve the satellite information passageways to foster data cooperation.<sup>1</sup> This addition to the BRI reflects China's ambition to advance its position in internet infrastructure and information technology.

Chinese President Xi Jinping, at the Belt and Road Forum (BRF) for International Cooperation in Beijing on 14 May 2017, proclaimed that China should "intensify cooperation in frontier areas such as digital economy, artificial intelligence, nanotechnology, and quantum computing, and advance the development of big data, cloud computing and smart cities to turn them into a digital silk road of the 21st century."<sup>2</sup> Bringing the digital component into the BRI seamlessly advanced Beijing's ambition of taking a leadership position in the technology sector.

Drawing from China's Standards 2035 and Made in China 2025 at the domestic level, the DSR facilitates the spread of Chinese digital standards by integrating BRI partner countries. Beijing has reportedly invested \$8.43 billion in Angola, Nigeria, Zimbabwe, Ethiopia, and Zambia under the DSR framework.<sup>3</sup> Developing countries

prefer the Chinese model of cyber governance as their leadership is critical of the West. For instance, Zimbabwe, Djibouti, and Uganda see the internet as a gateway for companies, like Google and Facebook, to undermine their governments by espionage and influencing the population.<sup>4</sup> These factors underpin developing nations leaning towards Chinese investment.

Furthermore, developing countries see China as a valuable partner that meets their need for competitively priced digital products and services.<sup>5</sup> China also offers internet consultation services in some BRI partner nations, like Egypt

*The DSR fits the spectrum for advancing the Chinese version of global governance by generating demand for Chinese companies*

and Zimbabwe, by providing training centres and research programmes through which China can export its ideology.<sup>6</sup> Thus, the DSR fits the spectrum for advancing the Chinese version of global governance by generating demand for Chinese companies.

## GLOBAL FOOTPRINT

There are 6 000 tech enterprises registered on the BRI portal, and more than one-third of Chinese FDI is invested in the tech sector of BRI partner countries.<sup>7</sup> At least sixteen states — Egypt, Turkey, Bangladesh, Laos, South Korea, Kazakhstan, the Czech Republic, Serbia, Poland, Hungary, Estonia, England, Cuba, Peru, the United Arab Emirates, and Saudi Arabia — signed the memoranda of understanding (MoUs) on the DSR as of 2020.<sup>8</sup>

However, the DSR might include more than these sixteen countries. There remains ambiguity regarding which projects operate solely under the DSR and which are independent initiatives led by China. Although these factors make the DSR opaque, one-third of the BRI member countries continue their participation in it, even if they have not signed MoUs.<sup>9</sup> Chinese tech companies have concluded over 116 smart city partnerships, including 70 projects in BRI partner countries, whereas Europe tops the list with the most Chinese-built smart city projects.<sup>10</sup>

The DSR also allows China to harness data for its strategic gains and surveillance. The US intelligence agencies have warned that Huawei’s 5G projects could act as a backdoor for espionage by the Chinese government.<sup>24</sup> Confidential data on the IT network of the Chinese-built African Union (AU) headquarters was allegedly diverted to Shanghai every night between 2012 and 2017.<sup>25</sup> Thus, the infiltration of personal data and backdoor vulnerabilities indicate that the DSR might contribute to an erosion of democratic rights and jeopardise confidential data.

Regions	Countries	Projects and Cooperation Areas
<b>Africa</b>	Angola, Djibouti, Egypt, Ethiopia, Kenya, Nigeria, Zambia	- 2Africa connecting 16 African countries with Europe and the Middle East <sup>11</sup> - Surveillance Systems
<b>Latin America</b>	Cuba, Mexico, Peru	Huawei’s building of Latin America’s largest Wi-Fi network in Mexico <sup>12</sup>
<b>Asia</b>	Bangladesh, Laos, Myanmar, Pakistan, Singapore, South Korea, Türkiye	- China-Myanmar International (CMI) terrestrial cable connecting East, Southeast, and South Asia <sup>13</sup> - PEACE fibre optic network connecting China to Europe through Pakistan <sup>14</sup>
<b>Central Asia</b>	Kazakhstan, Kyrgyzstan, Turkmenistan, Uzbekistan,	- Smart cities in Kyrgyzstan and Tajikistan <sup>15</sup> - Construction of fibre-optic cable under the Caspian Sea in Turkmenistan <sup>16</sup>
<b>Europe</b>	The Czech Republic, England, Estonia, Hungary, Poland, Serbia	- Safe City project by Huawei in Serbia <sup>17</sup> - Huawei-planned smart city in Duisburg, Germany <sup>18</sup>
<b>Middle East</b>	Saudi Arabia, The United Arab Emirates	- Alibaba’s supporting the NEOM mart city in Saudi Arabia <sup>19</sup> - Huawei’s building 5G network in the UAE <sup>20</sup>

**Table 1. Overview of the DSR’s global footprint.**

Source: Council on Foreign Relations, author’s own selection.<sup>21</sup>

In addition to spreading across regions, it is imperative to recognise that the DSR goes beyond the technology infrastructure, which raises two critical concerns. First, the DSR gives China leverage to advance the digital authoritarian governance model, and second, it risks data privacy. Huawei’s smart city projects are primarily located in authoritarian middle-income nations in Asia and Africa.<sup>22</sup> In 18 out of 65 countries, Chinese firms, like CloudWalk and

## DE-RISKING

Albeit already labelled as a “systemic rival” by the European Union in 2019, China emerged as the EU’s biggest trading partner, top exporter country to the EU, and the bloc’s third biggest market in 2021.<sup>26</sup> The EU’s and China’s transition from open to conditional engagement became prominent when European Commission President Ursula von der Leyen used the term “de-risking” in March 2023. The notion can be interpreted as reducing economic interdependence on China, encouraging the EU to diversify its market, and strengthening supply chains.

The shift to a de-risking policy might have occurred for two main reasons. First, the spread of Chinese digital authoritarianism via the

### *China’s digital authoritarianism can be exported to developing nations via the DSR*

Yitu, reportedly build surveillance systems for the local governments.<sup>23</sup> Given China’s digital control at home, its digital authoritarianism can be exported to developing nations via the DSR, which they can use to suppress their populations.

DSR raised concerns about Chinese espionage and data security. Secondly, Russia's full-scale aggression against Ukraine in 2022 increased the risk of dis- and misinformation, as well as the need to avoid dependence on suppliers, particularly in energy.

While the de-risking policy aims to lessen the reliance on China, the EU depends heavily on China, enhancing its chances of participating in the DSR.

China supplies 19 out of 30 critically important raw materials to the EU.<sup>27</sup> Despite the attempts by Sweden's Ericsson and Finland's Nokia to compete with the Chinese tech companies in the 5G race, Huawei remains the top 5G patent holder.<sup>28</sup> Moreover, China's two top export products to the EU in 2022 were telecommunications equipment and automatic data processing machines.<sup>29</sup> Thus, European policymakers must be concerned about how the union can de-risk while mitigating its reliance on China.

To reduce reliance on China through the DSR projects, as well as independent ones, the EU must find alternatives by collaborating with trusted partners and diversifying supply chains.<sup>30</sup>

*To reduce reliance on China through the DSR projects, the EU must find alternatives by collaborating with trusted partners and diversifying supply chains*

The EU can expand its technological landscape and engage nations in the Global South and the Indo-Pacific. Simultaneously, the EU must develop regulatory mechanisms to prevent Chinese state agencies from misusing sensitive data. The Digital Services Act, Digital Markets Act, and Artificial Intelligence Act are vital frameworks — now is the time for the EU to enforce them to combat China's technological threats.

## ENDNOTES

- <sup>1</sup> Ministry of Foreign Affairs of the People's Republic of China, *Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road* (Ministry of Foreign Affairs, March 2015).
- <sup>2</sup> "Full text of President Xi's speech at opening of Belt and Road forum," *Xinhua*, 14 May 2017.
- <sup>3</sup> Ovigwe Eguegu, "The Digital Silk Road: Connecting Africa with New Norms of Digital Development," *Asia Policy* Vol. 17, No 3 (National Bureau of Asian Research, July 2022): 30–39.
- <sup>4</sup> Sally Adee, "The global internet is disintegrating. what comes next?" *BBC News*, 15 May 2019.
- <sup>5</sup> Xinchuchu Gao, "An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model," *The International Spectator/Italian Journal of International Affairs* Vol. 57, No. 3(May 2022): 15–30.
- <sup>6</sup> Enyu Zhang and Patrick James, "All Roads Lead to Beijing: Systemism, Power Transition Theory and the Belt and Road Initiative," *Chinese Political Science Review* Vol. 8, No. 1 (March 2022): 18–44.
- <sup>7</sup> Tyson Baker, "Withstanding the Storm: The Digital Silk Road, Covid-19 and Europe's Options" in Alessia Amighini (ed.), *China after Covid-19: Economic revival and challenges to the world* (Institute for International Political Studies, 2021), 1–183.
- <sup>8</sup> "Assessing China's Digital Silk Road Initiative: A Transformative Approach to Technology Financing or a Danger to Freedoms?" Council on Foreign Relations, 2020.
- <sup>9</sup> Chan Jia Hao, "China's Digital Silk Road: The integration of Myanmar," Rajaratnam School of International Studies (RSIS) via *Eurasia Review*, 30 April 2019.
- <sup>10</sup> James Kyng and Nian Liu, "From AI to facial recognition: How China is setting the rules in new tech," *Financial Times*, 7 October 2020.
- <sup>11</sup> Dipanjan Roy Chaudhury, "China reportedly investing \$ 8.43 bn in Africa as part of Digital Silk Road Initiative," *The Economic Times*, 15 October 2015.
- <sup>12</sup> Adrian Shahbaz, "Freedom on the Net 2018. The rise of digital authoritarianism," *Freedom House*, 2018.
- <sup>13</sup> Baker, "Withstanding the Storm."
- <sup>14</sup> Baker, "Withstanding the Storm."
- <sup>15</sup> Leyla Muzaparova, L. "The Digital Silk Road: Opportunities and challenges for Central Asia," *Rosa Luxemburg Stiftung*, 12 October 2021.
- <sup>16</sup> Muzaparova, "The Digital Silk Road."
- <sup>17</sup> Stefan Vladislavljev, "China's Digital Silk Road enters the Western Balkans," *BFPE English*, 22 June 2021.
- <sup>18</sup> Baker, "Withstanding the Storm."
- <sup>19</sup> Andrew Chack, "Analyzing the entrenchment of Beijing's digital influence in Saudi Arabia and the United Arab Emirates," *Georgetown Security Studies Review*, 14 April 2023.
- <sup>20</sup> Sophie Zinser, "China's digital silk road grows with 5g in the Middle East," *The Diplomat*, 16 December 2020.
- <sup>21</sup> "Assessing China's Digital Silk Road Initiative," Council on Foreign Relations.
- <sup>22</sup> Clayton T. Cheney, "The Digital Silk Road: Understanding China's technological rise and the Implications for global governance" in Joseph Chinyong Liow, Hong Liu, and Gong Xue (ed.) *Research handbook on the Belt and Road Initiative* (Edward Elgar Publishing Limited, 2021), 88–101.
- <sup>23</sup> Shahbaz, "Freedom on the Net 2018."
- <sup>24</sup> Noah Berman, Lindsay Maizland, and Andrew Chatzky, "Is China's Huawei a threat to U.S. National Security?" *Council on Foreign Relations*, 8 February 2023.
- <sup>25</sup> Tin Hinane El Kadi, "The promise and peril of the Digital Silk Road," *Chatham House*, 6 June 2019.
- <sup>26</sup> Maaïke Okano-Heijmans, "Europe's strategic dependencies on China: The digital domain," in Ivano di Carlo (ed.), *EU-China relations at a crossroads, Vol. II: Decoding complexity, mitigating risk* (European Policy Centre, 2023).
- <sup>27</sup> Okano-Heijmans, "Europe's strategic dependencies on China."
- <sup>28</sup> "Who is leading the race of innovating and commercializing the 5G standard, paving the way for a more connected world?" LexisNexis, 10 October 2023.
- <sup>29</sup> "China-EU - International Trade in goods statistics," Eurostat, last modified in February 2023.
- <sup>30</sup> Okano-Heijmans, "Europe's strategic dependencies on China."

This publication is part of the project „On Sinicization of technology, creation of critical dependence, cyber threats originating from Asia, and possibilities for cyber cooperation.“ The partner of the project is the Asian Studies department at the Tallinn University's School of Humanities. The project is supported by the Estonian Ministry of Foreign Affairs.

## ABOUT THE AUTHOR

### MARIA

Maria is pursuing an MA in international relations at Tallinn University with a specialisation in international security and conflict studies. She studied political science for her bachelor's degree in Pakistan and was awarded the Global UGRAD scholarship to study Government and International Affairs in the US. She has a keen interest in decolonial studies, resistance movements, and development projects.

*Disclaimer: The views and opinions contained in this paper are solely of its author(s) and do not necessarily represent the official position of the International Centre for Defence and Security or any other organisation.*



INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY  
63/4 NARVA RD., 10120 TALLINN, ESTONIA  
INFO@ICDS.EE

ISSN 2228-2076