Cuadernos Europeos de Deusto

Núm. Especial 05 (Octubre 2022)

DOI: https://doi.org/10.18543/ced052022

ESTUDIOS

EU - China relations and data governance policies: the role of civil societies in overcoming geopolitical challenges in cyberspace

Relaciones UE-China y políticas de gobernanza de datos: el papel de las sociedades civiles para superar los desafíos geopolíticos en el ciberespacio

Cem Nalbantoğlu

doi: https://doi.org/10.18543/ced.2555

Recibido el 18 de mayo de 2022 • Aceptado el 25 de julio de 2022 • Publicado en línea: octubre de 2022

EU - China relations and data governance policies: the role of civil societies in overcoming geopolitical challenges in cyberspace

Relaciones UE-China y políticas de gobernanza de datos: el papel de las sociedades civiles para superar los desafíos geopolíticos en el ciberespacio

Cem Nalbantoğlu
Ph.D. Candidate, Wuhan University, China
cemnalbantoglu@yandex.com

doi: https://doi.org/10.18543/ced.2555

Received on May 18, 2022
Accepted on July 25, 2022
E-published: October 2022

Summary: I. Introduction.—II. Data governance and geopolitics in cyberspace.—III. Approaches to data governance & policies in the EU and China.—IV. Civil society, cyberspace, and policymaking.—V. Policy recommendations.—VI. Conclusion.

Abstract: EU and China are the global powers that can affect and alter international relations at the political, economic, and societal levels. While the EU shapes the foreign policy in Europe, China has a critical role in Asian politics. In Asia-Europe interregionalism and interregional relations, the EU-China relations are essential in consolidating global and regional stability. However, in the current political conjuncture, the security issues in cyberspace challenge both actors. Hence, cybersecurity and digitalization policies are a potential conflict area in EU-China relations. As the impact of technological and digital developments increases on the global political economy, global powers are developing policies to breast the tape in technological development. The European Commission has set "A Europe fit for the digital age" as one of its priorities for the 2019-2024 term. Meanwhile, since 2015 China has been promoting the Digital Belt and Road Initiative to foster digital connectivity among the Belt and Road countries. However, big data analytics are important in developing new technologies, especially in digital connectivity, automation, and robotics. In this context, data governance has become a geopolitical concept in international relations. Consequently, differences between China's and the EU's approach to data – access, process, and collection – may result in geopolitical confrontations. In this paper, we argue that both actors should involve civil society in the policymaking process to address the dynamics of information technologies, cooperate on adapting a global approach and avoid geopolitical confrontations. Civil society organizations can help the actors understand the underlying risks in cybersecurity and form a non-conflicting approach in data governance frameworks. Furthermore, while investigating the EU and China's data governance models, we shed light upon the role of civil society

organizations in addressing the potential risks and opportunities in cyberspace. Finally, we conclude our paper with policy recommendations for China and the EU to cooperate in cyberspace by involving civil society organizations.

Keywords: China, EU, data governance, geopolitics.

Resumen: *La UE y China son las potencias globales que pueden afectar y alterar las relaciones internacionales a nivel político, económico y social. Mientras que la UE da forma a la política exterior en Europa, China tiene un papel fundamental en la política asiática. En el interregionalismo Asia-Europa y las relaciones interregionales, las relaciones UE-China son esenciales para consolidar la estabilidad global y regional. Sin embargo, en la coyuntura política actual los temas de seguridad en el ciberespacio desafían a ambos actores. Por lo tanto, las políticas de ciberseguridad y digitalización son un área de conflicto potencial en las relaciones UE-China. A medida que aumenta el impacto de los desarrollos tecnológicos y digitales en la economía política global, las potencias globales están desarrollando políticas que lideran el desarrollo tecnológico global. La Comisión Europea ha fijado «Una Europa apta para la era digital» como una de sus prioridades para el periodo 2019-2024. Mientras tanto, desde 2015, China ha estado promoviendo la Iniciativa de la Franja y la Ruta Digital para fomentar la conectividad digital entre los países de la Franja y la Ruta. Sin embargo, el análisis del big data es importante en el desarrollo de nuevas tecnologías, especialmente en conectividad digital, automatización y robótica. En este contexto, la gobernanza de datos se ha convertido en un concepto geopolítico en las relaciones internacionales. En consecuencia, las diferencias entre el enfoque de datos de China y la UE (acceso, procesamiento y recopilación) pueden dar lugar a confrontaciones geopolíticas. En este artículo argumentamos que ambas potencias deben involucrar a la sociedad civil en el proceso de formulación de políticas para abordar la dinámica de las tecnologías de la información, cooperar para adaptar un enfoque global y evitar confrontaciones geopolíticas. Las organizaciones de la sociedad civil pueden ayudar a ambas potencias a comprender los riesgos subyacentes en la ciberseguridad y formar un enfoque no conflictivo en los marcos de gobernanza de datos. Además, mientras investigamos los modelos de gobernanza de datos de la UE y China, arrojaremos luz sobre el papel de las organizaciones de la sociedad civil para abordar los riesgos y oportunidades potenciales en el ciberespacio. Finalmente, concluimos nuestro artículo con recomendaciones políticas para que China y la UE cooperen en el ciberespacio involucrando a las organizaciones de la sociedad civil.*

Palabras clave: *China, UE, gobernanza de datos, geopolítica.*

I. **Introduction**

Asian regionalism and Asia – Europe interregionalism have been popular subjects among the political scientists investigating the relationship between Asia and Europe from a geopolitical perspective. In Europe, European Union (EU) has been playing the lead role in European regionalism and shaping the politics in the region. On the Asian side, although it is home to various regional organizations such as the Association of Southeast Asian Nations (ASEAN) and Asia-Pacific Economic Cooperation (APEC), the region is far from a political unity. In this vein, there have been various attempts to define the challenges to Asian regionalism. Gilson advocates that in Asia – Europe relations, East Asian countries, particularly China, South Korea, and Japan, weigh heavier given their political and economic capacity; hence a geopolitical analysis should focus on East Asia rather than Asia as a region continent in a political framework[1]. Robles sees the problem in the difficulty of defining boundaries and distinguishing the continent from the region[2]. However, when it comes to defining the relations between two regions, several concepts have been used to analyze regionalism and interregionalism between Asia and Europe; bilateral interregionalism[3], crossregionalism[4], transregionalism[5], overlapping regionalism[6], bifurcated regionalism[7], stealth interregionalism[8],

---

[1] Julie Gilson, "New Interregionalism? The EU and East Asia", *Journal of European Integration* 27, no. 3, (2005): 309

[2] Alfredo C Robles, *The Asia-Europe Meeting: The Theory and Practice of Interregionalism* (London: Routledge, 2012), 12.

[3] Alan Hardacre and Michael Smith, "The EU and the Diplomacy of Complex Interregionalism," *The Hague Journal of Diplomacy* 4, no. 2 (2009): 167–88, https://doi.org/10.1163/187119109x440898.

[4] Jorge Garzón and Detlef Nolte, "The New Minilateralism in Regional Economic Governance," in *Handbook of South American Governance*, ed. Pía Riggorozzi and Christopher Wylde (London: Routledge, 2017).

[5] Andrea Ribeiro-Hoffman, "Inter- and Transregionalism," in *The Oxford Handbook of Comparative Regionalism*, ed. Tanja A. Börzel and Thomas Risse (Oxford: Oxford University Press, 2016), 653.

[6] Diana Panke and Sören Stapel, "Overlapping Regionalism in Europe: Patterns and Effects," *The British Journal of Politics and International Relations* 20, no. 1 (November 10, 2017): 239–58, https://doi.org/10.1177/1369148117737924.

[7] Frank Mattheis, "Towards Bifurcated Regionalism - the Production of Regional Overlaps in Central Africa," in *The New Politics of Regionalism - Perspectives from Africa, Latin America and Asia-Pacific*, ed. Ulf Engel *et al*. (London: Routledge, 2018), 37–51.

[8] Gian Luca Gardini and Andrés Malamud, "Debunking Interregionalism: Concepts, Types and Critique – with a Pan-Atlantic Focus," in *Interregionalism across the Atlantic Space*, ed. Frank Mattheis and Andréas Litsegård (Geneva: Springer International Publishing, 2018), 15–31.

and hybrid or quasi interregionalism[9]. Here, we consider Hanggi's "hybrid regionalism" especially useful as it attaches importance to the role of individual powers in their capability to affect and alter the relations among different regions[10]. In the context of Asia – Europe relations, Niquet put forward that China's influence and power in the international political economy render it a critical force in shaping Asian regionalism and characterizing Europe's relations with the region[11]. In this context, we consider China's positioning in the global political economy, political and economic influence in Europe, and its relations with European powers to make China an essential factor in the EU's policy in Asia. Furthermore, by the end of 2021, China remained the EU's largest trading partner with a volume of 828.1 billion USD, while the EU is China's second-largest trading partner after the United States (US)[12]. Therefore, the complicated nature of the EU – China relations makes it necessary for the EU and China to cooperate in various fields. The stability of the bilateral ties between the actors is also critical for its effect on the Asia – Europe interregionalism.

In the global political and economic conjuncture, different factors have the potential to alter and transform the EU – China relations. The multilayered nature of China – EU bilaterality necessitates both actors to cooperate in political and economic spheres on international and regional levels. The EU's EU – China factsheet defined China as "a partner for cooperation and negotiation, an economic competitor and a strategic rival."[13] Biscop states that while enjoying a strategic partnership in the economic sphere, China and the EU have to refrain from engaging in political conflicts to deepen the relations[14]. It is to note that different strategic links create contrasting interests in politics despite the nature of alliances. Given its economic agenda, the US-China rivalry has been

---

[9] Mario Telò, Louise Fawcett, and Frederick Ponjaert, *Interregionalism and the European Union a Post-Revisionist Approach to Europe's Place in a Changing World* (London: Routledge, 2015).

[10] Mario Telò, "'Perspectives,'" *Belgeo* 4, no. 4 (November 9, 2020), https://doi.org/10.4000/belgeo.43943.

[11] Valérie Niquet, "The Balance of Power in Asia: A Challenge for Europe?," *China Perspectives* 2006, no. 1 (February 1, 2006), https://doi.org/10.4000/chinaperspectives.579.

[12] "China-EU - International Trade in Goods Statistics," Statics Explained, Eurostat, accessed May 1, 2022, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=China-EU_-_international_trade_in_goods_statistics#:~:text=EU%20exports%20to%20China%20were.

[13] European Union External Action, "EU - China Factsheet," February 2022, https://www.eeas.europa.eu/sites/default/files/documents/EU-China_Factsheet_01Apr2022.pdf.

[14] Sven Biscop, "No Peace from Corona: Defining EU Strategy for the 2020s," *Journal of European Integration* 42, no. 8 (November 16, 2020): 1009–23, https://doi.org/10.1080/07036337.2020.1852230.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, Núm. Especial 05 (Octubre 2022), Bilbao, págs. 51-73
doi: https://doi.org/10.18543/ced.2555 • http://ced.revistas.deusto.es

pushing the EU to pursue a complex approach toward the US and China[15]. Similarly, Kavalski elaborates that China's investments and close relationships with Central and Eastern European countries have caused concerns among the EU officials, despite the growing EU – China ties[16]. Following, the EU and China relations are tested through different political dynamics. Maher believes that to deepen the relations and bolster the EU – China cooperation; both actors must acknowledge the security challenges and generate standard policies to overcome the geopolitical conflicts; otherwise, China and the EU have conflicting interests and values[17]. Here, Winseck[18], Lacy and Prince[19], and Sheldon[20] see the power struggle in cyberspace to characterize the global political and economic dynamics in International Relations.

Mühleisen points out that information technologies (IT) development and innovation are closely attached to the improvements in economic connectivity, productivity, and growth in the contemporary economic outlook[21]. Newman *et al*. stress that digital technologies' impact on trade and bureaucracy proliferates as businesses, companies, state organs, and society rely on information technology and network connections[22]. Unsurprisingly, "security" in cyberspace has become a critical part of the national security frameworks for global powers. However, we claim that cyberspace does not pose a geopolitical complexity for its sole role in "information flow." The data's role in the development and innovation of technology renders it a geopolitical concern.

---

[15] Johannes Gabriel and Susanne Schmelcher, "Three Scenarios for EU-China Relations 2025," *Futures* 97, no. 1 (March 2018): 26–34, https://doi.org/10.1016/j.futures.2017.07.001.

[16] Emilian Kavalski, "The Unexpected Consequences of China's Cooperation with Central and Eastern Europe," *International Studies* 57, no. 1 (December 22, 2019): 2, https://doi.org/10.1177/0020881719880739.

[17] Richard Maher, "The Elusive EU-China Strategic Partnership," *International Affairs* 92, no. 4 (June 20, 2016): 976, https://doi.org/10.1111/1468-2346.12659.

[18] Dwayne Winseck, "The Geopolitical Economy of the Global Internet Infrastructure," *Journal of Information Policy* 7, no. 2 (2017): 229, https://doi.org/10.5325/jinfopoli.7.2017.0228.

[19] Mark Lacy and Daniel Prince, "Securitization and the Global Politics of Cybersecurity," *Global Discourse* 8, no. 1 (January 2, 2018): 100–115, https://doi.org/10.1080/23269995.2017.1415082.

[20] John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly* 5, no. 2 (July 2011): 95–112, https://www.jstor.org/stable/26270559.

[21] Martin Mühleisen, "The Long and Short of the Digital Revolution," *Finance & Development* 55, no. 2 (June 2018): 6–8.

[22] Joshua Newman, Michael Mintrom, and Deirdre O'Neill, "Digital Technologies, Artificial Intelligence, and Bureaucratic Transformation," *Futures* 136, no. 2 (February 2022): 102886, https://doi.org/10.1016/j.futures.2021.102886.

While elaborating on tech companies' increasing turnover over the last decades, Szczepański attests that "data is the new oil."[23] Data generation, access, and storage are critical to trade, politics, security, economic development, and technological innovation. For these reasons, data security and data governance have become essential concepts in cybersecurity. However, what makes data so important in the geopolitical context? What are the implications of data governance in contemporary geopolitics? We benefit from Zhang and Flint's "paired Kondratieff cycle and hegemonic cycle model" to shed light on these questions[24]. As "Paired Kondratieff cycle and hegemonic cycle model" elaborates on the rise and fall of hegemonies, it defines a causal relationship between technological advancements and hegemonic shifts from a geopolitical outlook. This model investigates the impact of data governance on developing new technologies and thus the geopolitical interplays.

In the framework of contemporary global political-economic dynamics, when we analyze the EU and China, we see that digitalization policies constitute a critical part of foreign policy dynamics. While centering the Belt and Road Initiative (BRI) in its foreign policy, the Chinese government has been building the Digital Belt and Road (DBR) among the BRI countries[25]. In Europe, the European Commission defined cybersecurity and digitalization as the Union's strategic goals[26]. As Matthew and Streinz put forward, data governance has become a concept that poses implications in their domestic and foreign affairs for China and the EU[27]. Furthermore, data's essential role in developing new technologies and technological innovations renders it significant for economic development. In this context, the data's vital role in technical and economic development poses a geopolitical challenge to the EU – China relations.

---

[23] Martin Szczepański, "Is Data the New Oil? Competition Issues in the Digital Economy [Policy Podcast]," Epthinktank, January 10, 2020, https://epthinktank.eu/2020/01/10/is-data-the-new-oil-competition-issues-in-the-digital-economy-policy-podcast/.

[24] Xiaotong Zhang and Colin Flint, "Why and Whither the US-China Trade War?: Not Realist 'Traps' but Political Geography 'Capture' as Explanation," *Journal of World Trade* 55, no. 2 (April 2021).

[25] Hong Shen, "Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative," *International Journal of Communication* 24, no. 1 (June 2018): 18–36.

[26] European Commission, "COMMUNICATION from the COMMISSION to the EUROPEAN PARLIAMENT, the COUNCIL, the EUROPEAN ECONOMIC and SOCIAL COMMITTEE and the COMMITTEE of the REGIONS 2030 Digital Compass: The European Way for the Digital Decade," 118 § (2021), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.

[27] Matthew S Erie and Thomas Streinz, "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance," Ssrn.com, February 3, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3810256.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, Núm. Especial 05 (Octubre 2022), Bilbao, págs. 51-73
doi: https://doi.org/10.18543/ced.2555 • http://ced.revistas.deusto.es

In this research, the EU and China can utilize civil society organizations to define the legal and political incompatibilities, address conflicting interests, and have a better understanding of the dynamics of cyberspace. In this way, civil society organizations can help actors adopt data governance policies to avoid geopolitical vacuums. Furthermore, cooperation through civil society organizations can act as a cooperation model between the EU and Asian states to reinvoke the regionalism and interregionalism efforts between Asia and Europe. This study will further investigate the problems between Asia – Europe interregionalism from the EU – China relations framework and define the data governance's impact on the global power struggle. Finally, we will create a model of cooperation framework between the EU and China that employs civil society as a tool in problem defining.

II. **Data governance and geopolitics in cyberspace**

Despite its prevalent usage in daily language, "data" is a complicated concept that has introduced different fields to the social sciences. Zins defines data as the raw material used to build the information blocks[28]. In this relation, Zins asserts that data is a symbol, qualified and quantified, whereas information is a set of signs that can create knowledge[29]. In other words, knowledge is the information appropriated by the user in terms of information science. Similarly, Liew claims a correlation and causation between the control over data, information, and knowledge[30]. There are different ways to analyze and correlate data to politics, economics, society, and the military in social sciences. We can analyze data to measure the econometrics, generate models on actor behavior, compare the military capabilities, or even predict the results of an election. Data is widely used to create models, make predictions, and test hypotheses. Thence, data protection has even become a matter of national security across the globe[31]. Every entity constantly generates data through network technologies,

[28] Chaim Zins, "Conceptual Approaches for Defining Data, Information, and Knowledge," *Journal of the American Society for Information Science and Technology* 58, no. 4 (2007): 480, https://doi.org/10.1002/asi.20508.

[29] Zins, 480.

[30] Anthony Liew, "Understanding Data, Information, Knowledge and Their Inter-Relationships," *Journal of Knowledge Management Practice* 8, no. 2 (June 2007), http://www.tlainc.com/articl134.htm.

[31] Christopher Kuner *et al*., "The Challenge of 'Big Data' for Data Protection," *International Data Privacy Law* 2, no. 2 (April 23, 2012): 47–49, https://doi.org/10.1093/idpl/ips003.

people, businesses, societies, states, devices, and servers within network technologies. Although there are different uses of data, we want to focus on the relation between the data and the development of new technologies, especially artificial intelligence (AI).

When explaining the relationship between big data and AI, an article released by Maryville University elaborates, "…AI's ability to expertly work with data analytics is the primary reason why artificial intelligence and big data are now seemingly inseparable. AI machine learning and deep learning are pulling from every data input and using those inputs to generate new rules for future business analytics…"[32] So when it comes to the development of AI, big data has a critical role. O'Leary sees control over big data as a prerequisite for the research and development of AI technologies[33].

According to Buhl *et al*., big data is the generation of mass data through online and offline applications and gathering them in one source[34]. In this context, data generation, management, analysis, and data manipulation, as in computer sciences, are essential to create big data and feed the research and development of AI technologies, as we had indicated earlier. Furthermore, regarding the AI's role in international relations, in 2020, Russian President Vladimir Putin has asserted that the nation that will dominate the AI development will have technological, economic, and military superiority in the international arena[35].

In our analysis, regarding its role in developing AI technologies and research on machine learning, we see data governance as a geopolitical concept. To explain this relationship, we benefit from Zhang and Flint's model of "paired Kondratieff cycle and hegemonic cycle." Zhang and Flint see the trade tensions, between the US and China, as a manifestation of competition over the core technologies; furthermore, they note that historically, the hegemonic power has been the one that captured these core technologies[36]. Moreover, in their interpretation, Zhang and Flint elaborate

---

[32] Maryville University, "Big Data and Artificial Intelligence: How They Work Together," Maryville Online, July 21, 2017, https://online.maryville.edu/blog/big-data-is-too-big-without-ai/#:~:text=AI.

[33] Daniel E. O'Leary, "Artificial Intelligence and Big Data," *IEEE Intelligent Systems* 28, no. 2 (March 2013): 96–99, https://doi.org/10.1109/mis.2013.39.

[34] Hans Ulrich Buhl *et al*., "Big Data," *Business & Information Systems Engineering* 5, no. 2 (February 14, 2013): 65–69, https://doi.org/10.1007/s12599-013-0249-5.

[35] Indermit Gill, "Whoever Leads in Artificial Intelligence in 2030 Will Rule the World until 2100," Brookings, January 17, 2020, https://www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030-will-rule-the-world-until-2100/.

[36] Zhang and Flint, 7.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, Núm. Especial 05 (Octubre 2022), Bilbao, págs. 51-73
doi: https://doi.org/10.18543/ced.2555 • http://ced.revistas.deusto.es

that the rise and fall of hegemonies can be explained by two consecutive Kondratieff cycles[37]. Kondratieff cycles, put forward by the Soviet economist Nikolay Kondratieff, depicts a relation between the superiority over new technologies and the economic status of powers (Figure 1)[38]. With technological superiority, actors rise to become the hegemony; through their control over the economic means, they restructure the international order. In this picture, Colin and Flint see the dominance in the development of core technologies, including AI, as the gateway to rise as a hegemonic power in the liberal world order.

Our theoretical framework employs the "paired Kondratieff cycle and hegemonic cycle" to address the impact of the data governance frameworks in international relations from a geopolitical standpoint. While shaping the social, economic, and political trends and visions, data concerning big data and big data analytics has become a geopolitical phenomenon in international relations for the critical role in the development of AI[39]. In addition to data's role in developing AI technologies, Penchava *et al*. see its composition in the information building to aggravate the national security concerns among states[40]. Furthermore, the approach to data governance, or data governance regime, can determine how data can be generated, mined, accessed, and processed[41]. Therefore, data's role in international politics, security, economics, and international relations renders data governance a geopolitical challenge.

The widespread use of digital technologies and the interconnectivity between the technology and the user make it challenging to distinguish the ownership and endpoint of data use. For example, when a user in a country utilizes an application belonging to a company in another country, do the company can collect the data of this user? Does it belong to the state of the country resides? Concerns over the data have led states to create policies toward data governance. In this vein, the EU and China have undertaken several policies toward data governance. However, while developing and

---

[37] Zhang and Flint, 8.

[38] Zhang and Flint, 13.

[39] M. C. Elish and Danah Boyd, "Situating Methods in the Magic of Big Data and AI," *Communication Monographs* 85, no. 1 (September 19, 2017): 57–80, https://doi.org/10.1080/03637751.2017.1375130.

[40] Irina Pencheva, Marc Esteve, and Slava Jankin Mikhaylov, "Big Data and AI – a Transformational Shift for Government: So, What next for Research?," *Public Policy and Administration* 35, no. 1 (June 12, 2018): 095207671878053, https://doi.org/10.1177/0952076718780537.

[41] Marijn Janssen *et al*., "Data Governance: Organizing Data for Trustworthy Artificial Intelligence," *Government Information Quarterly* 37, no. 3 (July 2020): 101493, https://doi.org/10.1016/j.giq.2020.101493.

implementing these policies, the EU and China can shift towards a geopolitical confrontation. In that vein, it is critical to understand the approaches and concerns regarding data governance. Identifying the underlying concerns over the data can help states to create policies that will avoid a possible geopolitical confrontation and lead to a greater conflict in cyberspace.

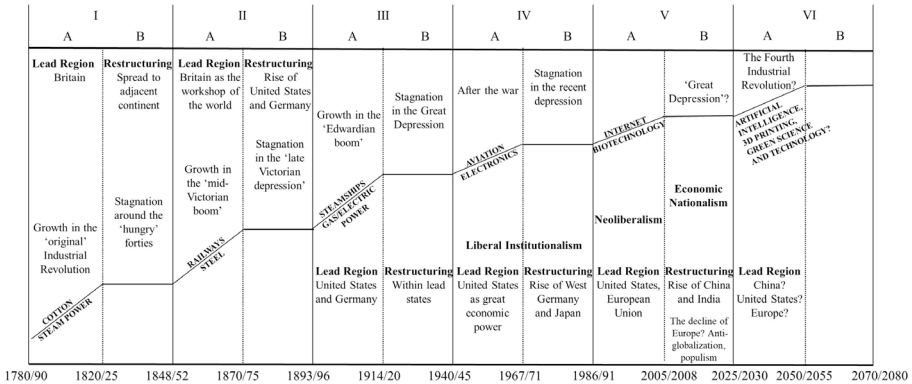

Figure 1

The Evolution of the Kondratieff Cycle and Hegemonic Cycle[42]

III. **Approaches to data governance & policies in the EU and China**

Big data analytics and artificial intelligence shape the world by driving innovation in different spheres. To develop new technologies and drive innovation, techno-hubs are harvesting the data ubiquitously from the users, plants, weather changes, cars, and many more components[43]. Regarding data's role in technological development, it is hardly a surprise that some are calling information "new oil". Although it is not unbiased, the rationale of the analogy lies in resembling the role of data in technological development to the position of oil in heavy industrialization. Furthermore, James and Scharfman considers the dominance over the data as a gateway

[42] Zhang and Flint, 9.

[43] Teresa Scassa, "Considerations for Canada's National Data Strategy," *Data Governance in the Digital Age* (Waterloo: The Centre for International Governance Innovation, March 2018), https://www.cigionline.org/static/documents/documents/Data%20Series%20Special%20Reportweb.pdf.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, Núm. Especial 05 (Octubre 2022), Bilbao, págs. 51-73
doi: https://doi.org/10.18543/ced.2555 • http://ced.revistas.deusto.es

to the superiority in the digital economy and even military intelligence[44]. As the impact of data grows, data governance assumes more importance in international politics, economy, and geopolitics. Likewise, with the use of data in different fields, novel problems such as data privacy violations[45], algorithm fairness[46], and mass surveillance have started to rank on the states' political agenda[47]. To regulate cyberspace, several initiatives, such as Osaka Track (Declaration)[48], have been launched to create a framework for data governance and ensure cross-border data flows. However, the nature of the field makes it challenging to define a framework for data governance and set global standards.

Data governance is a field that forces technological capabilities to meet the political agenda. Pisa *et al*. note that issuing regulations and laws, creating incentives and sanctions, and auditing the data require a level of technic expertise among the policymakers and bureaucrats[49]. Hence, it is critical to define data governance to analyze the data and investigate it in a legal framework. Samm and Sherman define data governance as rules that states impose to interact with the private sector[50]. Rupert *et al*. argue that the methodology in data collection and procession generates power imbalances and leads to information asymmetries in a strategical sense[51]. Similarly, in Micheli *et al*., data governance is attributed to "… the way

---

[44] James Marceau and Barry Scharfman, "Right AI Strategy a Must for Military Superiority," *National Defence*, 2019, JSTOR, https://www.jstor.org/stable/27022573.

[45] Nidhi Rastogi, Marie Joan Kristine Gloria, and James Hendler, "Security and Privacy of Performing Data Analytics in the Cloud: A Three-Way Handshake of Technology, Policy, and Management," *Journal of Information Policy* 5, no. 1 (2015): 130, https://doi.org/10.5325/jinfopoli.5.2015.0129.

[46] Akintande, Olalekan J, "Algorithm Fairness through Data Inclusion, Participation, and Reciprocity," in *Database Systems for Advanced Applications*, ed. Christian S Jensen *et al*., vol. 12683 (DASFAA 2021, Capital Region of Denmark: Springer International Publishing, 2021), 633–37.

[47] David Lyon, "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique," *Big Data & Society* 1, no. 2 (July 9, 2014): 1–13, https://doi.org/10.1177/2053951714541861.

[48] G20 OSAKA LEADERS, "G20 Osaka Leaders' Declaration | Documents and Materials," G20 Osaka Summit 2019, 2019, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html#:~:text=We%2C%20the%20Leaders%20of%20the.

[49] Michal Pisa *et al*., "Governing Data for Development: Trends, Challenges, and Opportunities," *CGD Policy Paper* 190 (November 2020): 1–61, https://www.cgdev.org/sites/default/files/governing-data-development-trends-challenges-and-opportunities.pdf.

[50] Samm Sacks and Justin Sherman, "Global Data Governance Concepts, Obstacles, and Prospects," *New America* (The Howard Baker Forum, December 2019), newamerica.org/cybersecurity-initiative/reports/global-data-governance/.

[51] Evelyn Ruppert, Engin Isin, and Didier Bigo, "Data Politics," *Big Data & Society* 4, no. 2 (July 3, 2017): 2–14, https://doi.org/10.1177/2053951717717749.

data is accessed, controlled, shared and used, the various socio-technical arrangements set in place to generate value from data, and how much value is redistributed between actors"[52]. Moreover, Erie and Streinz assess the capability of the digital infrastructure building as a power of control over the data flows[53]. Deriving from these definitions, we see it as a set of rules, laws, and negotiations on the digital and physical infrastructure in the digital sphere that state issues against the society, private sector, and other states to implement a political agenda. Hence, we see a reciprocal relationship between the political agenda and policies toward data governance. Again, in this context, concepts such as data colonialism, privacy laws, data flow, data classification, data localization, and data mirroring may lead to political clashes in the international arena.

Both the EU and China have acknowledged the role of the data and created legal and political frameworks for its governance. The EU enacted the "General Data Protection Regulation"[54] (GDPR) in 2016 and reached an agreement on the "Digital Services Act" in 2022 to "create a safer digital space where the fundamental rights of users are protected." Furthermore, in 2020, European Commission "Artificial Intelligence White Paper" has addressed the critical role of big data in AI research and development[55]. Similarly, the Chinese government revised the "Guarding State Secrets Law"[56] in 2010, enacted the "Cybersecurity Law"[57] in 2016, the "Encryption Law"[58] in 2019, and the "Data Security Law"[59], as well as

[52] Marina Micheli *et al*., "Emerging Models of Data Governance in the Age of Datafication," *Big Data & Society* 7, no. 2 (July 2020): 3, https://doi.org/10.1177/2053951720948087.

[53] Erie and Thomas Streinz, 46.

[54] European Parliament, "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)," 2016/679 § (2016).

[55] European Commission, "White Paper on Artificial Intelligence - a European Approach to Excellence and Trust," European Commission, February 19, 2020, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[56] Laney Zhang, "China: State Secrets Law Revised," Library of Congress, May 7, 2010, https://www.loc.gov/item/global-legal-monitor/2010-05-07/china-state-secrets-law-revised/#:~:text=Limits%20on%20the%20time%20period.

[57] Cyberspace Administration of China, "中华人民共和国网络安全法[Cyberspace Security of the People's Republic of China]," www.cac.gov.cn, November 7, 2016, http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

[58] National People's Congress of the People's Republic of China, "中华人民共和国密码法[People's Republic of China Encryption Law]," www.npc.gov.cn, October 26, 2019, http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml.

[59] The National People's Congress of the People's Republic of China, "中华人民共和国数据安全法[People's Republic of China Data Security Law]," www.npc.gov.cn, June 10, 2021, http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, Núm. Especial 05 (Octubre 2022), Bilbao, págs. 51-73
doi: https://doi.org/10.18543/ced.2555 • http://ced.revistas.deusto.es

"Personal Information Protection Law"[60] in 2021, creating a broader framework for the data governance principles within the country.

The GDPR is a comprehensive framework that underlines the values, concerns, and actions of the EU towards different subjects within the data governance sphere[61]. Via various institutions, the EU is working towards bolstering its cybersecurity and the privacy of its citizens while protecting their rights[62]. Similarly, Chinese legislatures are working on a legal framework to create more comprehensive laws and regulations that will protect the interests of the state and the people[63]. It is possible to analyze Chinese and EU data governance from various aspects of the data governance regime. Data processing regulations, privacy, security, innovation, cross-border data transfer, and surveillance are the thematics of the international data governance debates[64]. Although both actors have produced several laws and regulations to put the data exercises in a framework, the EU and China are far from building a consensus on the scope and the range of an international data governance structure. In this context, within our theoretical framework, the digital technologies' impact on economic production has the potential to push the actors toward a geopolitical standoff in cyberspace. Here, we see the concepts of "big data for development", "data collection regime", and "norms followed in third countries" as key fields for a potential geopolitical interplay in the EU – China relations. We will analyze the data governance approaches from these standpoints as the EU and Chinese executives, the international community, and the academic literature officially recognize them. While analyzing each of these concepts, we will also monitor the rules and approaches followed in China and the EU, with the purpose of defining the gray areas and potential conflict zones in cyberspace.

The United Nations (UN) sees big data as a critical factor in developing essential industries of emerging economies[65]. The European Commission

---

[60] The National People's Congress of People's Republic of China, "中华人民共和国个人信息保护法," http://www.npc.gov.cn/, August 20, 2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.

[61] Paul Voigt and Von Dem, *The EU General Data Protection Regulation (GDPR) : A Practical Guide* (Cham: Springer International Publishing, 2017): 2-7

[62] Ben Wolford, "What Is GDPR, the EU's New Data Protection Law?," GDPR.eu (European Union, November 7, 2018), https://gdpr.eu/what-is-gdpr/.

[63] Feng Liu, Jiayin Qi, and Chi Yaqiong, "数字化转型背景下企业数据保护成熟度模型构建[Construction of Enterprise Data Protection Maturity Model under the Background of Digital Transformation]," *Journal of Intelligence* 40, no. 9 (September 2021): 134–40, https://doi.org/10.3969/j.issn.1002-1965.2021.09.020.

[64] Andrea Mulligan, "Constitutional Aspects of International Data Transfer and Mass Surveillance," *Irish Jurist* 55, no. 1 (2016): 199–208.

[65] UNCTAD, "Digital Economy Report 2021" (Geneva: United Nations, August 2021).

foresees the data-driven applications to benefit society with improved healthcare services, cleaner transport systems, innovative products, and sustainable energy resources[66]. In its 14th Five Year Plan, the Chinese government has asserted that "Big data serves as a new driving force for economic transformation and development, offers a new way to improve government governance capacity (政府治理能力), and provides a new opportunity to reshape the country's competitive advantages"[67]. Furthermore, big data analytics is a set of operations that includes data generation, collection, process, and service. To build technical capacity and highlight the key catalyzers of the big data processors, the EU and China have taken various steps. China's big data strategy follows a "whole of state" approach, which incorporates state-owned enterprises, state-run organizations, government agencies, and several governing bodies, including the State Council and National Development Reform Commission[68]. Furthermore, in 2015, China's State Council issued the "Action Plan for Promoting the Development of Big Data"[69]. The plan focuses on creating databases throughout the country to leverage the mass data produced by the population and centralize them within the state control. Furthermore, China's big data strategy has implications in the economic, political, and military domains. In the European case, the EU has acknowledged the role of big data and formulated the Union's strategy of becoming the global leader in a "data-driven society"[70]. The European Commission has established various data hubs, research centers, and cooperation facilities to promote the public-private partnership within its data strategy[71]. Although

---

[66] European Commission, "Strategy for Data - Shaping Europe's Digital Future," digital-strategy.ec.europa.eu (European Union, 2020), https://digital-strategy.ec.europa.eu/en/policies/strategy-data.

[67] PRC Ministry of Industry and Information Technology, "'14th Five-Year' Plan for the Development of the Big Data Industry," Center for Security and Emerging Technology, February 2021, https://cset.georgetown.edu/publication/14th-five-year-plan-for-the-development-of-the-big-data-industry/.

[68] Derek Grossman *et al*., *Chinese Views of Big Data Analytics* (California: RAND Corporation, 2020), 1–18.

[69] Lindsay Gorman, "China's Data Ambitions: Strategy, Emerging Technologies, and Implications for Democracies," The National Bureau of Asian Research (NBR), August 14, 2021, https://www.nbr.org/publication/chinas-data-ambitions-strategy-emerging-technologies-and-implications-for-democracies/.

[70] Cyberwatching, "Toward a Data-Driven Society: A Technological Perspective on the Development of Cybersecurity and Data-Protection Policies," Cyberwatching (European Union, March 4, 2020), https://www.cyberwatching.eu/news-events/news/toward-data-driven-society-technological-perspective-development-cybersecurity-and-data-protection-policies.

[71] EUHubs4Data, "Members Archive," European Federation of Data Driven Hubs, 2020, https://euhubs4data.eu/members/.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, Núm. Especial 05 (Octubre 2022), Bilbao, págs. 51-73
doi: https://doi.org/10.18543/ced.2555 • http://ced.revistas.deusto.es

different laws and political frameworks regulate the EU and China's big data strategy, both actors attach a critical role to the big data within their development path. Sun *et al*. assert that even though they are shaped by different dynamics, the significance of big data renders cyberspace a strategic play zone in international relations[72]. In other words, despite its crucial role in accelerating the development and improving the livelihood of the society, the lack of a consensus on data governance may leave China and the EU in a geopolitical struggle. Winseck advocates that when big data strategies are regarded, the lack of international consensus and framework leaves gray areas open for a geopolitical interpretation[73].

The data collection regime indicates to any practice and technological outset that the collector uses the received data. According to Tyler, the data collection regime includes technical problems such as collecting data from external databases through data localization and mirroring and ethical issues such as allowing government access to the databases and free data flows[74]. Differences come forward when considering the different data collection regimes in the EU and China. First of all, the EU's data collection practices are executed under the legal GDPR. Whereas, in China, no singular law or execution works as a guideline for the data collection. Furthermore, the European Chamber press release argues that China's Data Protection Law has contradicting characteristics with GDPR's data collection principles[75]. Secondly, while the GDPR does not impose data localization practices on companies, the data localization is forced depending on the "entity that is processing data" and the "type of data that is being processed" under the Chinese law [76]. The data that is important for Chinese national security is to be stored in China, and data can only be transferred with authorities' approval. Furthermore, in their study for European Data Protection Board (EDPB), Czarnocki *et al*. claim that the EU standards on the EU companies'

---

[72] Liyuan Sun, Hongyun Zhang, and Chao Fang, "Data Security Governance in the Era of Big Data: Status, Challenges, and Prospects," *Data Science and Management* 2, no. 02 (June 2021): 41–44, https://doi.org/10.1016/j.dsm.2021.06.001.

[73] Winseck, 229.

[74] Isaac Taylor, "Data Collection, Counterterrorism and the Right to Privacy," *Politics, Philosophy & Economics* 16, no. 3 (June 22, 2017): 326–46, https://doi.org/10.1177/1470594x17715249.

[75] European Chamber, "European Chamber Stance on China's Data Security Law and Personal Information Protection Law," www.europeanchamber.com.cn, August 25, 2021, https://www.europeanchamber.com.cn/en/press-releases/3367/european_chamber_stance_on_china_s_data_security_law_and_personal_information_protection_law.

[76] Hunter Dorwart, "New FPF Report: Demystifying Data Localization in China - a Practical Guide," Future of Privacy Forum, February 2022, https://fpf.org/blog/new-fpf-report-demystifying-data-localization-in-china-a-practical-guide/#:~:text=Under%20Chinese%20law%2C%20data%20localization.

data transfer towards third party countries have no practical implications on the Chinese law or the data collection practices in China[77]. Finally, the EU and China follow different principles on data sharing and government access. Article 40 of the Chinese Constitution guarantees the private rights of the Chinese citizens; it states that for the matter of national security and criminal investigation, public security organs can act accordingly[78]. Riordan considers the differing practices within data collection regimes to cause a conflict of interest between the global powers[79].

Finally, arguably a more significant challenge for both the EU and China lies in the data governance practices that the actors will exercise in third countries. Third countries are important markets for global tech giants to increase their market cap and penetration. While operating in international markets, the EU and Chinese companies interact with users in different state jurisdictions, making it challenging to implement their data governance policies. Similarly, Brown from Human Rights Watch advocates that as less developed countries lack legal regulations and cyber law enforcement practices, these markets become open for exploitation by big tech companies and platforms[80]. Furthermore, digital connectivity projects such as DBR and Global Gateway (GG) render the "norms practices in third countries" critical for their scope and impact. As the data harvested in third markets are vital to big data analytics, the lack of a framework on data collection norms may force the EU and China to tackle data governance and implementation challenges in different markets and countries.

IV. **Civil society, cyberspace, and policymaking**

When we examine civil society from the framework of international relations, the arguably dominant challenge is determining civil society's functionality, impact, and role in foreign policymaking. While a vast literature discusses the nature of state-society relations in political science, civil society's role and function in international relations are limited and

---

[77] Jan Czarnocki *et al*., "Government Access to Data in Third Countries" (European Data Protection Board, November 2021).

[78] Tiffany C. Li, Jill Bronfman, and Zhou Zhou, "Saving Face: Unfolding the Screen of Chinese Privacy Law," *Journal of Law, International and Science (Forthcoming)*, August 22, 2017, 1–33, https://ssrn.com/abstract=2826087.

[79] Shaun Riordan, "The Geopolitics of Cyberspace: A Diplomatic Perspective," *Brill Research Perspectives in Diplomacy and Foreign Policy* 3, no. 3 (June 27, 2018): 1–84, https://doi.org/10.1163/24056006-12340011.

[80] Deborah Brown, "Big Tech's Heavy Hand around the Globe," Human Rights Watch, September 8, 2020, https://www.hrw.org/news/2020/09/08/big-techs-heavy-hand-around-globe.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, Núm. Especial 05 (Octubre 2022), Bilbao, págs. 51-73
doi: https://doi.org/10.18543/ced.2555 • http://ced.revistas.deusto.es

characterized by political perspectives. Here the question we ask is whether civil society organizations (CSO) can shoulder a different role in international relations by addressing the issues and creating consciousness among the policymakers. In other words, can civil society organizations act as a catalyzer in the resolution of security conflicts by charting the security interests and presenting alternative solutions to policymakers?

Hehir stresses that although they are not the actual power yielders, civil society organizations (CSO) can influence the states' by creating pressure mechanisms on policymakers[81]. Similarly, Kamimura claimed that establishing research organizations, institutions, and non-governmental organizations (NGOs) helped the Japanese people process the nuclear disarmament talks in Japan[82]. Das argues that in India, policymakers tend to believe that their actions are backed by public support in the lack of a robust civil society[83]. Civil society has a critical role in addressing the security challenges, reflecting the problems on the ground level, and pushing the agenda towards comprehensive policymaking. CSOs can articulate their expertise in related fields to avoid confrontations and consolidate international communication among societies, states, and decision-makers. First, CSOs can affect security policies by pressurizing the policymakers and offering policy alternatives to the decision-makers through interaction with state agencies[84]. Secondly, the CSO can shape the national security policies by addressing the policy perspectives that are unclear to the policymakers[85]. Takana and Wanandi suggest this relationship as "…Civil society organizations often have a clearer sense of how to solve concrete problems than governments; they are setting norms that governments increasingly heed"[86]. Next, CSOs can work as conflict de-escalators and intermediaries between the conflicting parties. Likewise,

---

[81] Aidan Hehir, *Humanitarian Intervention: An Introduction* (Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan, 2010), 28.

[82] Naoki Kamimura, "Civil Society, Nuclear Disarmament, and the U.S. Alliance:: The Cases of Australia, New Zealand, and Japan," *Analysis and Publications* (East - West Center, 2004), http://www.jstor.com/stable/resrep06487.

[83] Samir Kumar Das, *Conflict and Peace in India's Northeast: The Role of Civil Society*, vol. 42 (Washington D.C.: East-West Center, 2007), 23.

[84] Marina Caparini and Philipp Fluri, "Mapping Civil Society in Defense and Security Affairs: An Agenda for Research," *Connections* 1, no. 4 (December 2002): 51–62, https://www.jstor.org/stable/26322966..

[85] Délber Andrade Lage and Leonardo Nemer Caldeira Brant, "The Growing Influence of Non-Governmental Organizations: Chances and Risks," *Anuario Brasileiro de Direito Internacional* 3, no. 1 (2008): 79–93.

[86] Hitoshi Takana and Jusuf Wanandi, "The Regional Context: Civil Society and Changing Perceptions of Security," in *Civil Society Contributions on Regional Security Issues* (New York: Japan Center for International Exchange, 2010), 2–4.

CSOs can withdraw attention from public issues that the state may not fully understand amid a crisis. In the pandemic outbreak, civil society organizations in Argentina, Chile, and Brazil took the initiative to help the state develop a pandemic playbook[87].

The crucial role of the data in the development of AI renders it a critical asset. From our analysis of the "Paired Kondratieff cycle and hegemonic cycle model", data has a geopolitical significance that may push the EU and China towards a geopolitical confrontation. The lack of a global consensus on data governance, inadequate legal frameworks, and the absence of technical expertise may further cause a geopolitical vacuum that forces the actors to struggle. However, we claim that CSO can play a critical role in identifying the geopolitical challenges and creating a global data regime in the international arena to prevent confrontations.

In the outlook of the geopolitics of cyberspace, we see that the development of digital technologies causes the global power struggle to spill over to the cyber realm. Although the different approaches to data governance equally pose challenges to the EU and China, data is not the only concern that may force a geopolitical confrontation. The development of blockchain technology, the emergence of new financial products, and digital groups are challenging global financial pillars. While cyberspace is evolving and developing continuously, it creates political, economic, and societal implications. Therefore, to prevent conflicts and avoid confrontations in the international arena, states are tasked with identifying risks and cooperating to take the corresponding action.

Here, we claim that the involvement of civil society organizations in cyberspace can help the EU and China chart the geopolitical vacuums and cyber conflict zones while addressing the critical issues that may create further complications in Europe – Asia relations. Moreover, CSOs' role in conflict mapping and de-escalation can become a model for resolving geopolitical conflicts that hinder Europe – Asia interregionalism. As we have put forward, there are various gray zones in cyberspaces that states cannot define, cannot act on, or simply have competing interests on. Here, CSOs and non-governmental organizations can help policymakers comprehend the technical aspects of cyberspace. As Hanna notes, tech companies, businesses, and scholars are more capable of developing new technologies and working them out than states and the public sector[88]. In this context, CSOs can help the

[87] Carnegie Civic Research Network, "Civil Society and the Global Pandemic: Building Back Different?" (Washington DC: Carnegie Endowment for International Peace, September 2021).

[88] Nagy Hanna, "A Role for the State in the Digital Age," *Journal of Innovation and Entrepreneurship* 7, no. 1 (July 16, 2018): 2–16, https://doi.org/10.1186/s13731-018-0086-3.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, Núm. Especial 05 (Octubre 2022), Bilbao, págs. 51-73
doi: https://doi.org/10.18543/ced.2555 • http://ced.revistas.deusto.es

EU and China policymakers understand the technological dynamics of digital technologies so that legislation can respond to the technical mechanism. Furthermore, the CSOs can act as an intermediary between China and the EU to discuss the framework of the governmental policies and identify the overlapping and non-complying articles. CSOs in China and the EU can exchange information and insights to help the actors define each other's approach to data governance. Another aspect is that external actors affect both the EU and China's data governance approaches. Through CSO, players can identify and engage with other actors and third countries and map the concerns in less developed regions. As digital CSO are more capable of understanding the technological and digital trends, they can act as an intermediary between the state and data fields so that states can better understand the consequences of technological developments and trends[89]. Finally, creating a global norm or consensus on data governance basics is a challenging task. There are different states, businesses, companies, players, and digital organisms that affect the governance of cyberspace. States' political nature prevents them from comprehending the technological and digital trends, interacting with players on a societal level, and corresponding to their requirements. Here, CSO can address the problems, challenges, and possible roadmaps essential to states' decision-making mechanisms.

With scientific developments, inventions, and innovations, new technologies such as blockchain, artificial intelligence, and machine learning have affected every aspect of human life. CSOs in specific technological fields provide training, material, and guidance for people to understand and follow new developments. States may utilize the expertise of CSO to chart new technological developments and their impacts on society, trade, economy, political relations, and security. In this context, we claim that although CSO does not have the power or capacity to set political agendas, they can guide states on scientific and technological developments, as these fields require high technical education and expertise. Furthermore, to produce comprehensive policies on data governance, and to interact with other players, including technology companies, decentralized organizations, cryptocurrencies, and novel technologies, states can utilize the expertise of CSO. In this way, states can avoid geopolitical traps and confrontations in the digital sphere with the help of CSO. Finally, this cooperation model between the EU and China can act as a method of resolving the conflicts and confrontations that slows down the Europe – Asia interregionalism.

---

[89] Svetlana Morozova and Alexander Kurochkin, "Formation of Digital Competencies in the Public Policy Sphere: The EU and Russia Experience," ed. T. Kliestik, *SHS Web of Conferences* 129, no. 6 (2021): 06006, https://doi.org/10.1051/shsconf/202112906006.

V. **Policy recommendations**

EU – China cooperation has critical importance in the Asia – Europe Interregionalism. The quasi regionalism model between the EU and China can become an exemplary case in reinforcing the relations between the European and Asian countries while contributing to the Asia – Europe interregionalism. To overcome geopolitical confrontations and consolidate the welfare of the relations, the EU and China may cooperate on several issues. Here, we will put forward several policy recommendations to enhance CSOs' presence in the cybersphere and create digital civil society organizations. Likewise, through these policy recommendations, we believe the EU and China will work toward a global data governance regime that will lead to a worldwide framework for data politics.

First, the EU and China should start working groups on cyberlaw to explore the differences and approaches to data governance. As we have analyzed earlier, European and Chinese legal framework on data usage and collection shows varieties. Furthermore, the rapid development of digital technologies necessitates both actors to update their laws and regulations. To prevent further mismatch in approaches towards data governance, the EU and China need to start workgroups that will analyze the laws and regulations and highlight the overlapping areas and contradicting principles.

Secondly, as data governance requires technical qualification, both the EU countries and China need to encourage digital CSOs that can provide technical expertise to the state organs. In various cases, bureaucrats and the state organs do not possess the knowledge and capability to comprehend the impacts of technological developments. Here, digital civil societies can inform both the state and society about the consequences of laws and regulations in cyberspace. Furthermore, these CSOs can act as digital pathfinders and revealers that will forecast the results of technological developments, innovations, and financial trends in the tech industry.

Next, let us consider the technology giants, such as Google and Alibaba, from the perspective of their financial capitalization and impact on digital technologies. Their impact on the global political economy is evident. In this vein, China and the EU can consider appointing digital ambassadors to these companies to develop better relations and map their strategies. In contemporary political-economic conjuncture, technology companies are an asset for countries with technological and economic capabilities. Digital ambassadors can work with these technology giants to ensure the compatibility of their actions with state policies and regulations.

Finally, the EU and China need to cooperate with CSOs to work on an international data governance framework. While new technologies create power struggles between the semi-periphery and the hegemony, infrastruc-

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, Núm. Especial 05 (Octubre 2022), Bilbao, págs. 51-73
doi: https://doi.org/10.18543/ced.2555 • http://ced.revistas.deusto.es

ture investments and development projects in the periphery create further geopolitical complexities. In February 2022, the EU announced a 150 billion Euro investment package for infrastructure projects in Africa within GG[90]. DBR has been constructing information and communication technology infrastructure in BRI countries, including technologically underdeveloped regions of Southeast Asia, Central Asia, and North Africa[91]. In Sridhar and Sridhar, infrastructure building is essential for sustainable growth and development in developing economies[92]. However, the lack of an international data framework may politicize these efforts and create geopolitical vacuums in the international arena. Therefore, the EU, China, and other global powers need to work on an international data governance framework to implement equal practices in less developed and developing countries that will benefit from technology and infrastructure imports.

VI. **Conclusion**

Technological innovations have a profound impact on political and economic dynamics, as well as on human life. Among these technologies, AI has been widely recognized for its potential to transform public and private domains. However, AI and machine learning research require big data to operate and develop. Consequently, issues related to data – access, process, share, and transfer – have gained importance. Approaches to data governance have started to pose a geopolitical challenge to the countries. In this framework, we have investigated the data governance frameworks in the EU and China. In our research, we have found that the EU and China have been working on policies to define the legal and political framework of data governance. While these policies have overlapping sections, EU and Chinese data governance policies differ in their approach to big data, data collection regime, and practices in third countries. When big data

[90] European Commission, "EU-Africa: Global Gateway Investment Package," European Commission, 2022, https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/global-gateway/eu-africa-global-gateway-investment-package_en.

[91] Huadong Guo *et al*., "The Digital Belt and Road Program in Support of Regional Sustainability," *International Journal of Digital Earth* 11, no. 7 (May 10, 2018): 657–69, https://doi.org/10.1080/17538947.2018.1471790.

[92] Kala Seetharam Sridhar and Varadharajan Sridhar, "Telecommunications Infrastructure and Economic Growth: Evidence from Developing Countries," *Applied Econometrics and International Development* 7, no. 2 (2008): 54, Sridhar, Kala Seetharam and Sridhar, Varadharajan, Telecommunications Infrastructure and Economic Growth: Evidence from Developing Countries (August 23, 2008). Applied Econometrics and International Development, Vol. 7, No. 2, 2007, Available at SSRN: https://ssrn.com/abstract=1250082.

geopolitics are regarded, these differences have the potential to push the EU and China towards a geopolitical vacuum in cyberspace.

The EU – China relations have global and regional implications when the global political economy and international relations are regarded. On a regional level, cooperation between the EU and China is essential in fostering Asia – Europe interregionalism and interrelations. Furthermore, the EU – China quasi interregionalism can pave the way for Asian regionalism. However, for the EU and China to cooperate, it is essential for them to overcome geopolitical challenges. In the cyberspace, CSOs can shoulder an intermediary role between the EU and China by addressing the technological risks and identifying alternative policy options. Furthermore, the involvement of civil society in cyberspace can prevent uneven and unjust data regimes in third countries that do not possess IT technologies and infrastructure.

With digital connectivity, digital technologies are developing at an unprecedented rate. While these technologies can transform human life and offer better opportunities for societies, it is to note that they are not exempt from political challenges. Hence, states need to cooperate with each other and civil society to address the emerging challenges and consolidate the safe use of novel technologies.

About the author

Cem Nalbantoğlu is a Ph.D. student at Wuhan University, he obtained his master's degree in International Relations at Zhejiang University and his bachelor's degree at the Middle East Technical University's Political Science and Public Administration department. During his studies, he has also undertaken various classes at the University of Duisburg and Essen (2013) in Germany, and Chongqing Posts and Telecommunications (2017) in China. In 2021 he was awarded a research stay at the University of Deusto under the Jean Monnet Network project "European Union-Asia Pacific Dialogue: promoting European Integration and mutual Knowledge across Continents" (EUNAP). He has several publications on Chinese foreign policy and international relations. His research interests include Chinese foreign policy, Belt and Road Initiative, EU-China relations, and geopolitics. He is fluent in Turkish, English, Spanish, and Chinese.

Sobre el autor

Cem Nalbantoğlu es un estudiante de doctorado en la Universidad de Wuhan, obtuvo su máster en Relaciones Internacionales en la Universidad

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, Núm. Especial 05 (Octubre 2022), Bilbao, págs. 51-73
doi: https://doi.org/10.18543/ced.2555 • http://ced.revistas.deusto.es

de Zhejiang y su licenciatura en el departamento de Ciencias Políticas y Administración Pública de la Universidad Técnica de Medio Oriente. Durante sus estudios, ha tomado varias clases en la Universidad de Duisburg y Essen (2013) y Chongqing University of Posts and Telecommunications (2017). En 2021 realizó una estancia de investigación en la Universidad de Deusto en el marco del proyecto Jean Monnet Network "European Union-Asia Pacific Dialogue: promoting European Integration and mutual Knowledge across Continents" (EUNAP). Es autor de varias publicaciones sobre política exterior china y relaciones internacionales. Sus líneas de investigación incluyen la política exterior china, la iniciativa del cinturón y la ruta de la seda (BRI), las relaciones UE-China y la geopolítica. Habla turco, inglés, español y chino con fluidez.