Sovereignty Fever: The Territorial Turn of Global Cyber Order

Chien-Huei Wu*
Institute of European and American Studies, Academia Sinica, Taipei, Taiwan
wch@sinica.edu.tw

Abstract

This paper argues that the utopia of a borderless and interconnected cyberspace loses its charm and the global cyber order is witnessing a territorial turn. The proliferation of the notion of cyber sovereignty and its variances is a symptom reflecting sovereign states' attempt to retain autonomy and control gradually eroded with the digitalisation of societies and economies. The sovereignty fever can be attributed to four reasons: political ambition, economic value, security concerns, and human rights. However, sovereignty is not the last word in debates concerning the future of digital society, for even liberal democracies have advanced ideas of technological or digital sovereignty, and data sovereignty, for their own very different purposes.

Keywords

internet sovereignty – digital sovereignty – data sovereignty – cybersecurity – *Schrems* – China's Cybersecurity Law

* Associate Research Professor, PhD in Law, European University Institute.

I. Introduction

In 2010, China published its first White Paper on the Internet wherein China referred to the building, utilisation, and administration of the Internet as 'an issue that concerns national economic prosperity and development, state security and social harmony, state sovereignty and dignity, and the basic interests of the people'.[1] It went on: 'The Chinese government believes that the Internet is an important infrastructure facility for the nation. Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected.'[2]

The idea of Internet sovereignty, or cybersovereignty (*wangluo zhuquan*, 网络主权),[3] is reaffirmed and expressed in legal terms for the first time in China's National Security Law, effectuated in 2015, where in Article 25, the State is instructed to 'safeguard national sovereignty, security and development interests in cyberspace'.[4] Such an idea was further promoted and disseminated in the international arena when Chinese President Xi Jinping gave his keynote speech, calling for respect of Internet sovereignty, during the Second World Internet Conference (WIC) held in Wuzhen, in December 2015.[5]

China's jurisdictional and territorial claim of Internet sovereignty is in stark contrast to the United States (US) prevailing characterisations of cyberspace, which are conceptualised as 'global commons'[6] or 'multi-stakeholders governance'.[7] Internet sovereignty denotes that it is the State that exercises its

---

1 China Daily, 'The Information Office of the State Council, White Paper on Internet in China', China Daily, 8 June 2010, available at <https://www.chinadaily.com.cn>.

2 China Daily (n. 1).

3 Before Internet sovereignty gained its popularity in Chinese official statements and academic writings, a similar term, information sovereignty (*xunxi zhuquan*, 讯息主权) had been proposed, referring to the State's sovereign rights to regulate information flows.

4 National Security Law of the People's Republic of China, 1 July 2015, Art. 25.

5 Ministry of Foreign Affairs, the People's Republic of China, 'Remarks by H. E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet conference', 16 December 2015, available at <https://www.fmprc.gov.cn>. [The principle of sovereign equality enshrined in the *Charter of the United Nations* is one of the basic norms in contemporary international relations. It covers all aspects of state-to-state relations, which also includes cyberspace. We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation, and Internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs, or engage in, connive at, or support cyber activities that undermine other countries' national security.].

6 On cyberspace as 'global commons', see, e. g. Milton Mueller, 'Against Sovereignty in Cyberspace', International Studies Review 22 (2019), 779-801.

7 On multi-stakeholderist' approach on Internet governance, see, e. g. Jeanette Hofmann, 'Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice', Journal of Cyber Policy 1 (2016), 29-49.

 DOI 10.17104/0044-2348-2021-3-651

sovereignty over its territorial Internet. In accordance with this sovereign power, the State is competent and capable of delimitation, control, and regulation.[8] Free flow of information is only possible to the extent that is not against the laws and regulations of the State and in line with the national security and development interests.

Apart from Internet sovereignty, in the digital age emerge digital sovereignty, technological sovereignty, and data sovereignty, which are introduced with a view to reclaiming and retaining control, autonomy, and sufficiency over informational technologies and data flows. Surprisingly, these three types of sovereignty are advanced by not only those countries which guard sovereignty jealously, such as India, but also by countries embracing liberal democracy, such as Germany and France, under the auspice of the European Union (EU).

In view of the proliferation of these sovereignty terms, this paper aims to ascertain whether a 'liberal' cyber world embodied in free flows of expression, information, and data has evidenced a territorial turn. By territorial turn, I mean countries' attempt to delimit the boundary and erect barriers for information inflows/outflows, regardless of the considerations and motivations. The term 'territorial turn' here focuses on the countries' efforts or initiatives to control or regulate information flows and confine them in a given territorial realm.[9] If so, this paper aims to examine factors and actors driving this turn, and to imagine the future of this territorialised cyber order. Given that China is the most vocal advancing Internet Sovereignty and represents the key force reforming liberal cyber order shaped by the US, the contrast of US and China on their perceptions of global cyber order best evidences the territorial turn of global cyber order, if any. In addition, the EU represents an economic and political project aspiring to transcend national border and encourage 'integration of all countries into the world economy',[10] pursuing technological sovereignty or digital sovereignty in the name of autonomy and self-sufficiency signals a retreat from an open and liberal Europe. A comparison between these three key actors in embracing or

[8] Ronald J. Deibert and Masashi Crete-Nishihata observe a trend of Internet filtering, turning cyberspace from open commons to controlled access. Ronald J. Deibert and Masashi Crete-Nishihata, 'Global Governance and the Spread of Cyberspace Controls', Global Governance 18 (2012), 339-361 (341-346). See also Ronald Deibert and Rafal Rohozinski, 'Liberation vs. Control: The Future of Cyberspace', Journal of Democracy 21 (2010), 43-57.

[9] Given the cross-border nature of information flows, such efforts and initiatives might impact third countries or give rise to extraterritorial effects, but these side effects are not the main concern of this paper. Rather, I am more interested in the driving forces and rationale why countries delimit the cyberspace, originally conceived as 'global commons', and subsequently control and regulate activities in the territorialised cyberspace.

[10] Art. 21 para. 2 lit. a) TEU.

rejecting the sovereignty terms in global cyber governance contributes to our understanding on the changing dynamics underpinning international politics and the digital world.

With these aims, this paper first traces the evolution of mainstream conceptions of cyber order in the US context and then explores challenges introduced by China's rise in international relations and its expansionist ambition under the "Chinese Dream". The paper then examines the contagion of sovereignties, explains the reasons for this proliferation, and concludes with the future of this liberal, free, and open cyber order.

II. Contesting Global Cyber Governance: The Revisionist's Challenges

The rise of China, along with that of other emergent powers, has shaken every part of the globe and the concomitant threats to liberal international order have elicited discussion in international relations[11] and international law[12] fora, and led some scholars to argue that the authoritarian turn of international law is happening[13] and authoritarianism is going global.[14] However, it is misleading to argue that emergent countries, such as Brazil, Russia, India, China, and South Africa, collectively known as the BRICS, maintain one and unified position that are contrary to and compete with that of the US and other Western countries.[15] Moreover, the US and EU diverge on a number of Internet regulatory issues, in particular over privacy, as seen in the debate over involuntary surveillance and data collection by corporations and governments.[16]

That said, a consensus has held that the US and China each compete to shape the global cyber order in their favour. The US is the predominant cyber power

---

11 See, e.g. G. John Ikenberry, 'The End of Liberal International Order?', Int'l Aff. 94 (2018), 7-23; Naná De Graaff and Bastiaan Van Apeldoorn, 'US-China Relations and the Liberal World Order: Contending Elites, Colliding Visions?', Int'l Aff. 94 (2018), 113-131.

12 See, e.g. Eric A. Posner and John Yoo, 'International Law and the Rise of China', Chinese Journal of International Law 7 (2006), 1-15; Congyan Cai, *The Rise of China and International Law: Taking Chinese Exceptionalism Seriously* (Oxford: Oxford University Press 2019).

13 Tom Ginsburg, 'Authoritarian International Law?', AJIL 114 (2020), 221-260.

14 Ron Deibert, 'Authoritarianism Goes Global: Cyberspace Under Siege', Journal of Democracy 26 (2015), 64-78.

15 Hannes Ebert and Tim Maurer, 'Contested Cyberspace and Rising Powers', TWQ 34 (2013), 1054-1074 (1055).

16 See, David Drissel, 'Internet Governance in a Multipolar World: Challenging American Hegemony', Cambridge Review of International Affairs 19 (2006), 105-120 (111-113).

 DOI 10.17104/0044-2348-2021-3-651

possessing the core component of cyber resources, including infrastructures, networks, and servers, and leader shaping the multi-stakeholder Internet governance regime.[17] As a latecomer, and given its relatively weak position in the Internet governance regime, China calls for 'multilateral, democratic and transparent' global cyber governance, but interprets these terms differently than Western countries do. Multilateralism on Internet governance is to be built upon, and underpinned by, the United Nations (UN) framework.[18] Democracy dictates global cyber governance be subject to sovereign equality without being monopolised by a few countries, whereas transparency relates to the decision-making processes which are to be made known to all countries.[19] As this paper focuses on the proliferation of sovereignties, the contrast between multi-stakeholderism and multilateralism is most relevant.

Multi-stakeholderism departs from the traditional Westphalian system engaging actors other than governments in the global decision and policy-making processes.[20] Whereas some see multi-stakeholderism as a prerequisite for an inclusive and practice-oriented approach, it is opposed not only by those who embrace traditional state sovereignty, but also by critics who question the legitimacy, transparency, and accountability of multi-stakeholder initiative.[21] Internet governance based on multi-stakeholderism is best reflected in a report by the Working Group on Internet Governance, referring to 'the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet'.[22] Therefore, the objective of multi-stakeholderist Internet governance is to bring those affected into the policy-making processes and thus enhance procedural legitimacy and reach better policies.[23] The

17 As the former Secretary of State, John Kerry spoke at the University of Korea in 2015, '[u]nlike many models of government that are basically top-down, the Internet allows all stakeholders – the private sector, civil society, academics, engineers, and governments – to all have seats at the table. And this multi-stakeholder approach is embodied in a myriad of institutions that each day address Internet issues and help digital technology to be able to function.' John Kerry, Secretary of State, 'An Open and Secure Internet: We Must Have Both', *VOAnews*, 18 May 2015, available at <https://www.voanews.com>.

18 Cuihong Cai, 'China and Global Cyber Governance: Main Principles and Debates', Asian Perspective 42 (2018), 647-662 (656-657).

19 Cai (n. 18), 652-653.

20 On the multiple actors in global cyber governance, see generally, Joseph S. Nye, Jr., 'The Regime Complex for Managing Global Cyber Activities', Global Commission on Internet Governance Paper Series, 1 May 2014, available at <https://www.cigionline.org>.

21 Christine Kaufmann, 'Multistakeholder Participation in Cyberspace', Swiss Review of International & European Law 26 (2016), 217-234 (217-218).

22 Working Group on Internet Governance, Document WSIS-II/PC-3/DOC/5-E, para. 10.

23 Hofmann (n. 7), 29.

difficult question nonetheless relates to how to decide the scope of those affected, and to what extent decision making is improved.[24] Moreover, as powerful multi-national Internet companies and influential non-governmental organisations are located mostly in developed countries, worries arise as to whether developing or less developed countries are marginalised or prejudiced. In fact, this is the reason why China asserts the multi-stakeholderist approach in Internet governance is not 'democratic' and calls instead for multilateral Internet governance.

China's proposal for multilateral cyber governance is based on the Westphalian system and consistent with its attachment to national sovereignty and efforts to import into cyberspace a concept of sovereignty under which only sovereign states are entitled to decide the form and substance of the global cyber governance regime.[25] Multilateral models of global cyber governance are to be found in various UN groups, including the Group of Governmental Experts (GGE),[26] the Open-Ended Working Group (OEWG) and expert commissions, such as the Global Commission on the Stability of Cyberspace.[27] Within these multilateral frameworks, the most noteworthy attempts by China, in cooperation with Russia and other Shanghai Cooperation Organization (SCO) countries, to shape global cyber norms are their submissions of an International Code of Conduct for the Emerging Information Society to the UN General Assembly for debates in 2011[28] and 2015.[29] The Code of Conduct unsurprisingly underlines sovereignty, territorial integrity and political independence, and calls for UN members to refrain from using information and communications technologies and networks to interfere in

24 Alexander Klimburg and Louk Faesen, 'A Balance of Power in Cyberspace' in: Dennis Broeders and Bibi Van Den Berg (eds), *Governing Cyberspace: Behavior, Power and Diplomacy* (Lanham/Boulder/New York/London: Rowman & Littlefield 2020), 151-152.

25 Andrew N. Liaropoulos, 'Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-Stakeholderism, and Power Politics', Journal of Information Warfare 15 (2016), 14-26 (15).

26 The UNGGE constitutes a good forum to explore States' perception on Internet sovereignty, digital sovereignty, technological sovereignty, and data sovereignty. By investigating the practices and statements of States in this forum, it contributes to our understanding on the divergence and convergence of States in these complex concepts. The author owes this point to the anonymous reviewer.

27 Christian Ruhl, Duncan Hollis, Wyatt Hoffman and Tim Maurer, 'Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads', Carnegie Endowment for International Peace, 2020, 4-9.

28 Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359, 14 September 2011.

29 Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/69/723, 13 January 2015.

 DOI 10.17104/0044-2348-2021-3-651

the internal affairs of other States, or with the aim of undermining their political, economic and social stability. Such attempts were seen as an effort to use multilateral fora to justify domestic suppression of Internet freedoms by China and other authoritarian regimes.[30]

On the other hand, China aims to reduce the US' influence over key multi-stakeholderist cyber governance institutions, the best example being the *Internet Corporation for Assigned Names and Numbers (ICANN)*. China and other countries, emergent and developed alike, continue to complain about the privileged position of the US in the ICANN owing to the Internet Assigned Numbers Authority functions contract. Due to the growing resentment of other countries, the US Department of Commerce finally agreed to eliminate its contractual oversight of ICANN and handed over authority to the global multi-stakeholder community.[31] The case of ICANN illustrates the dominant position of the US in key multi-stakeholderist global cyber governance institutions and explains why China aims to pursue a multilateral cyber governance regime, as under such a system it would have an equal say with the US.

III. Sovereignty Fever and Its Driving Forces

While China's proposed concept of Internet sovereignty and a multilateral governance model is unsurprising, sovereignty has gained popularity in recent decades, not only in authoritarian regimes but also in liberal democracies. I argue that four key factors contribute to the sovereignty fever in cyberspace and the digital world: political control, economic value, security concerns, and human rights. However, it should be made clear that these four factors are not clear-cut. Security considerations may be of economic value, which at the same time contributes to political ambition, while security considerations may also be linked to human rights as a means of safeguarding ways of life or values. The four factors I propose and the relevant examples discussed in this paper are to advance a set of angles to perceive the proliferation of sovereignties and delineate the underlying rationale. Below, I will first trace the proliferation of sovereignties and explain their driving forces.

---

30 Jinghan Zeng, Tim Stevens and Yaru Chen, 'China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"', Politcs & Policy 45 (2017), 432-464 (440).

31 Milton Mueller, 'Detaching Internet Governance from the State: Globalizing the IANA', Georgetown Journal of International Affairs 4 (2014), 35-44 (35).

1. The Proliferation of Sovereignties

When the Internet was first invented, it was expected that it would be transnational and boundaryless, and thus know no border. When John Perry Barlow presented the well-known *A Declaration of the Independence of Cyberspace*, it was proclaimed that governments of the industrial world exercise no sovereignty over cyberspace.[32] That vain hope soon faded. On the contrary, sovereignty became common parlance in cyberspace over the past decade among liberal democracies and authoritarian regimes alike.

Empirically, Marie Baezner and Patrice Robin review national cybersecurity strategies and explore how the concept of sovereignty is understood and applied in cyberspace. Some states use the word to highlight the need to protect governmental information systems, defence forces, and critical infrastructures in order to safeguard state sovereignty. Second, states refer to cyberattacks or other malicious cyber-activities as threats to their sovereignty. Third, states may also go beyond cybersecurity strategies and use the word 'sovereignty' in other policy documents. Finally, states argue that a secure cyberspace would protect their sovereignty.[33] However, the relevance of sovereignty in cyberspace is not limited to cybersecurity. In fact, when China pronounces Internet sovereignty, its scope is much more comprehensive than cybersecurity alone. Further, security concerns in cyberspace relate not only to safety from theft, disruption, destruction, or espionage, but also include insufficiency, unavailability, or inadequacy. In correspondence with their divergent views on cyberspace and their different values and interests, China, the US, and the EU conceive of cyberspace differently, and pursue different cyber strategies.[34]

In 2015, Chinese President Xi Jinping declared the concept of 'Internet sovereignty', illustrating cyberspace's territorial concept under the jurisdiction of a country. Contrary to conventional ideas of international freedom embraced by western countries, China attempts to include the cyberspace in the domestic jurisdiction and legitimises its governance and supervision of the Internet.[35] Under international law, countries enjoy supreme dominance

---

32 John Perry Barlow, 'A Declaration of the Independence of Cyberspace', Davos, Switzerland, 8 February 1996, available at <https://www.eff.org>.

33 Marie Baezner and Patrice Robin, *Cyber Sovereignty and Data Sovereignty*, (Zurich: Center for Security Studies, ETH 2018), 9.

34 Andrés Ortega Klein, 'The U.S.-China Race and the Fate of Transatlantic Relations', CSIS Report, 23 April 2020, available at <https://csis-website-prod.s3.amazonaws.com/>.

35 Michael Kolton, 'Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence', The Cyber Defense Review 2 (2017), 119-154.

 DOI 10.17104/0044-2348-2021-3-651

over their own territory, and China wishes to see the application of sovereignty to the cyberspace extends this dominance.[36]

By contrast, the EU proposes the concepts of 'digital sovereignty'[37] or 'technological sovereignty' to address the challenges facing Europe arising from digitalisation of the economy and society. The President of the European Commission, Ursula von der Leyen, in her 2019 inauguration speech, claimed: 'we must have mastery and ownership of key technologies in Europe'.[38] The digital sovereignty strategy is intended to maintain the EU's independence in cyberspace and to safeguard the privacy of its people. The term 'sovereignty' as used by the European Commission, addresses economic issues but also extends to the EU's political operations and strategic concerns.

The EU, following others' lead, embraced the idea of 'data sovereignty', meaning that online data and information are subject to domestic jurisdiction.[39] Namely, all information which has been stored in binary digital form is subject to the laws of the country in which it is located;[40] the same applies to data/information inflows into and outflows out of this country. Many of the current concerns surrounding data sovereignty relate to enforcing privacy regulations and preventing data that is stored in a foreign country from being subpoenaed by the host country's government. The concept of data sovereignty addresses stored data and its flows (data in transit), not overall jurisdiction of cyberspace.

The US does not use the term of 'sovereignty' but rather addresses cyberspace in security terms. As it stands, the US possesses the largest number of root servers and treats data as an asset[41] to be leveraged for the public good;[42]

---

36 Zeng, Stevens and Chen (n. 30), 434-464.

37 Silvia Amaro, 'Europe's Dream to Claim Its "Digital Sovereignty" Could Be the Next Big Challenge for US Tech Giants', CNBC, 20 November 2019, available at <https://www.cnbc.com/>; Luciano Floridi, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU', Philosophy & Technology 33 (2020), 369-378.

38 Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme, 27 December 2020, available at <https://ec.europa.eu>; see further, Tyson Barker, 'Europe Can't Win the Tech War It Just Started', Foreign Policy, 26 January 2020, available at <https://foreignpolicy.com/>.

39 Dana Polatin-Reuben and Joss Wright, 'An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet' in: *4th USENIX Workshop on Free and Open Communications on the Internet* (*FOCI 14*) (San Diego, CA: USENIX Association 2014), available at <https://www.usenix.org>.

40 Stephane Couture and Sophie Toupin, 'What Does the Notion of "Sovereignty" Mean When Referring to the Digital?', New Media & Society 21 (2019), 2305-2322.

41 U.S. Department of Defense, 'U.S. Dep't of Defense', DoD Data Strategy, 30 September 2020, available at <https://media.defense.gov>.

42 Federal Data Strategy, 'Components of the Federal Data Strategy', Official website of the United States Government, available at <https://strategy.data.gov>.

it emphasises limitless, free flow of data across borders with the goal of reducing the regulation of data as much as possible.[43] In 2013, the Open Data policy required government agencies to provide data in a machine-readable format to strengthen democracy and efficiency.[44] However, challenges stemming from China's claims of cyber sovereignty, together with cyberattacks originating in China, led the US to announce a revised cybersecurity policy. Thus, in 2018, the White House published the *National Cyber Strategy of the United States of America* (the USNCS),[45] contending that the competitors and adversaries of the US hide behind notions of sovereignty while recklessly violating the laws of other states by engaging in pernicious economic espionage and malicious cyber activities.[46] With a view to address these threats, the USNCS aims to

> '[…] defend the homeland by protecting networks, systems, functions, and data; promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; reserve peace and security by strengthening the ability of the United States – in concert with allies and partners – to deter and, if necessary, punish those who use cyber tools for malicious purposes; and expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.'[47]

While the USNCS does not speak of sovereignty in cyberspace, its overarching aim is to safeguard American interests, a function of the exercise of sovereignty.

2. Driving Forces Leading to Sovereignty Fever

a) Political Ambition

The leading proponent of Internet sovereignty is undoubtedly China, motivated by its need to maintain regime stability. China's capacity to control and regulate information flows is a key instrument of its censorship and surveillance of its citizens, and a means of ensuring that the Chinese Commu-

43 Adil Nussipov, 'How America and Europe Deal with Data', Central European University School of Public Policy, 7 January 2020, available at <https://cmds.ceu.edu>.

44 Exec. Order No. 13642, 3 CFR 13642, Making Open and Machine Readable the New Default for Government Information (2013), available at<https://www.govinfo.gov>.

45 U.S. White House, 'National Cyber Strategy of the United States of America', September 2018, available at <https://www.whitehouse.gov>.

46 See III. 1.

47 See II.

 DOI 10.17104/0044-2348-2021-3-651

nity Party is not challenged. Consistent with its 'peaceful rise',[48] China is no longer content with being a 'rule-taker' but rather strives to be a 'rule-shaper' or 'rule-maker'; as such it desires to shape international order to its ends.[49] China's promotion of the concept of Internet sovereignty internationally is reflective of its willingness to set new norms in cyber governance.[50] Budnitsky and Jia thus argue that Internet sovereignty is not only an expression of digital policy, but also an instrument of 'nation branding' employed to promote China's national identity as a great power on the international scene. Thus, cyber sovereignty extends beyond traditional state territorial authority and rather functions as an expression of nationalism; that is, it promotes a distinct national identity, or national vision of what the Internet should be.[51]

Chinese political leaders see Internet sovereignty as a cornerstone of its overarching cybersecurity strategy, part and parcel of its national security, and comprised of three dimensions: governance, internal influence, and national defence.[52] The governance dimension relates to a State's right to participate in international cyber governance on an equal footing, which corresponds to the principle of sovereign equality. The internal influence dimension concerns a State's paths and models of cyber development and regulation free from foreign interference – reflective of China's preference for the principle of non-interference. The national defence dimension addresses third countries' online activities undermining its national security. In a word, China's concept of Internet sovereignty is an extension or application of its preferred interpretation of the conventional Westphalian sovereignty concept to cyberspace. Internally, it can justify its regulatory or suppressive measures against its citizens. Externally, it can claim due representation in international cyber governance and seek to safeguard itself from foreign threats and influence in the name of national security.

China's efforts to monitor and censor information flows comprise a dense web of sophisticated measures. After the crackdown of student protests in

48 See, e. g. Zheng Bijian, 'China's "Peaceful Rise" to Great-Power Status', Foreign Aff. 84 (2005), 18-24; Barry Buzan, 'China in International Society: Is "Peaceful Rise" Possible?', The Chinese Journal of International Politics 3 (2010), 5-36; Herbert S. Yee (ed.), *China's Rise – Threat or Opportunity* (London: Routledge 2011).

49 Shiping Tang, 'China and the Future International Order(s)', Ethics & International Affairs 32 (2018), 31-43; G. John Ikenberry, 'The Rise of China and the Future of the West – Can the Liberal System Survive?', Foreign Aff. 87 (2008), 23-37; Shaun Breslin, 'China and the Global Order: Signalling Threat or Friendship?', InternInt'l Aff. 89 (2013), 615-634.

50 Zeng, Stevens and Chen (n. 30), 434.

51 Stanislav Budnitsky and Lianrui Jia, 'Branding Internet Sovereignty: Digital Media and the Chinese-Russian Cyber Alliance', European Journal of Cultural Studies 21 (2015), 594-613.

52 Sarah McKune and Shazeda Ahmed, 'The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda', International Journal of Communication 12 (2018), 3835-3855 (3837).

Tiananmen Square, Chinese leaders pondered how to fence China off from the intrusion of Western liberal ideas from the Internet. To this end, the Golden Shield project, which gave rise to the so-called 'Great Firewall of China', enabled the government to block access to blacklisted Internet resources and to censor network traffic related to banned keywords and phrases.[53] A more recent instrument with which China has strengthened its online monitoring and surveillance of its citizens is its 'social credit system (*shehui xinyong tixi*, 社会信用体系)' which enables the State to trace the digital footprint of every individual.[54] The underlying feature of China's Internet control and regulatory regimes is a real-name requirement complemented by biometric data. Under China's Cybersecurity Law the real-identity requirement applies when seeking: access to a stationary or mobile network; registration of a domain name; information publication; or instant messaging;[55] mandatory facial recognition is required for the purchase of a SIM card in accordance with a circular issued by the Ministry of Industry and Information Technology in 2019.[56]

Externally, China is keen to export its Internet regulatory model to other authoritarian countries, Russia and African countries in particular, and to project it onto the global cyber order, which contributes to the legitimacy of its Internet monitoring and control regime. This objective may be achieved via different channels: bilaterally, regionally or multilaterally. *Bilaterally*, China concluded an agreement on information security with Russia on 8 May 2015, where the Parties reaffirm that 'the sovereignty and international norms and principles derived from the state sovereignty, apply to the conduct of States in the framework of activities related to the use of information and communication technologies, and the jurisdiction of States over information'.[57] *Regionally*, China has used the SCO as a platform to promote the concept of Internet sovereignty and participant countries of the SCO are also

53 Zeng, Stevens and Chen (n. 30), 438. Some illustrative words and phrases are '4 June 1989', 'Tiananmen Square' and 'Arab Spring'.

54 On this social credit system, see, e.g. Yu-Jie Chen, Ching-Fu Lin and Han-Wei Liu, '"Rule of Trust"': Powers and Perils of China's Social Credit Megaproject', Columbia Journal of Asian Law 32 (2018), 1-36.

55 Art. 24 Cybersecurity Law of the People's Republic of China (China's Cybersecurity Law), Effective 1 June 2017.

56 BBC, 'China Due to Introduce Face Scans for Mobile Users', 1 December 2019, available at <https://www.bbc.com>.

57 Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in Ensuring International Information Security (China-Russia Information Security Agreement), 8 May 2015, Preamble, available at <http://treaty.mfa.gov.cn> (Chinese version); an unofficial English version is available at <https://cyber-peace.org/>. It should be noted that whereas the English version use 'jurisdiction', the Chinese version uses 'sovereign rights (*zhuquan quanli*, 主权权利)'.

prominent attendees of the WIC. Therefore, the SCO and Wuzhen processes are two fora/platforms through which China can promote its Internet governance model and cement the concept of Internet sovereignty.[58] *Multilaterally*, China, in collaboration with Russia and other SCO members, has attempted to project the concept of Internet sovereignty to global cyber order. As already mentioned, in 2011 and 2015, they submitted to the United Nations General Assembly an International Code of Conduct for Information Security with a view to create a consensus for preferred norms surrounding Internet sovereignty and information security.[59] While these attempts were rejected by the US and other Western countries, which see them as an effort to establish a strict national sovereignty model for information flows on the Internet and a potential instrument for suppressing dissents,[60] the attempts demonstrate the ambition of China and other SCO members to shape global cyber governance around the concept of sovereignty.

b) Economic Value

Economic value – the second driver contributing to the sovereignty fever – ranges from E-commerce to digital economy and has spread in both China and European countries. The US is no exception, although it does not spell out sovereignty *per se*.

When China joined the World Trade Organisation (WTO) in 2002, it was expected that China would open its market to foreign enterprises, including online services providers. This hope was soon dampened. Google withdrew from China in 2010, ten years after the launch of its Chinese version. During that decade, Google had sought a license from China and succeeded in securing one, but its search engine was nonetheless blocked from time to time. At the same time, Google was accused of sacrificing its commitment to business ethics and human rights for access to China's market.[61] Following repeated compromises and frustrations, Google decided to withdraw from the Chinese market. One of the key reasons for Google's withdrawal is believed to have been hacking attacks targeting everything from Google's intellectual property to the email accounts of Chinese activists. By the time it withdrew, Google accounted for more than one-third of the Chinese search

58 McKune and Ahmed (n. 52), 3841-3850.

59 McKune and Ahmed (n. 52), 3835-3842; Zeng, Stevens and Chen (n. 30), 440.

60 Zeng, Stevens and Chen (n. 30), 440.

61 See, e. g. G. Elijah Dann and Neil Haddow, 'Just Doing Business or Doing Just Business: Google, Microsoft, Yahoo! And the Business of Censoring China's Internet', Journal of Business Ethics 79 (2008), 219-234.

market, while China's domestic search engine, Baidu, had captured the lion's share with 58 percent.[62] The same story applies to Yahoo, except that Yahoo decided to sell its China operations to Alibaba, China's E-commerce giant, in exchange for a 40 percent stake in Alibaba,[63] which Yahoo sold back to Alibaba in 2012.[64] Most social media sites are not available in China; notably, Facebook has attempted to gain access to China but without success.

The exclusion or deterrence of foreign Information and Communications Technology (ICT) enterprises from China's domestic market is complemented and supplemented by subsidies, and an industrial policy favouring local firms modelled on state-capitalism. According to a study by the European Centre for International Political Economy, trade barriers targeting the ICT sectors and online markets substantially increased in the years 2007 to 2016, accounting 54 out of total of 76 measures.[65] Such an increase in trade barriers corresponded with China's 13th Five-Year Plan for the period of 2015 to 2020, which called upon ICT to 'underpin China's rise as a global power and its internal transformation.'[66] Jean-Christophe Plantin and Gabriele de Seta further detail how WeChat (*Weixin*, 微信), first developed as a mobile-oriented messaging application by Tencent, has evolved to be a part of the infrastructure for China's techno-nationalist digital economy. They note, 'protectionist environment resulting from the demanding regulatory conditions to operate in the Chinese market and the outright ban of foreign companies still allow Chinese platforms to easily reach the criticality and scale'.[67] The dominance of domestic social media or other online services in turn contributes to China's capacity to enforce censorship and maintain regime stability.[68]

Money talks not only in China but also in the EU and the US, albeit in different currencies. The EU frames the economic value with 'digital sover-

---

62 Matt Sheehan, 'How Google Took on China – and Lost', MIT Technology Review, 19 September 2018, available at <https://www.technologyreview.com/>.

63 David Barboza, 'Yahoo Is Paying $1 Billion for 40 % Stake in Alibaba', New York Times, 11 August 2005, available at <https://www.nytimes.com/>.

64 Kevin Voigt, 'Yahoo, Alibaba Reach $7.1 Billion Deal', CNN, 20 May 2012, available at <https://edition.cnn.com/>.

65 Martina E. Ferracane and Hosuk Lee-Makiyama, 'China's Technology Protectionalism and Its Non-Negotiable Rationales', ECIPE Working Paper, 27 June 2017, 3.

66 Yu Hong, 'Reading the 13th Five-Year Plan: Reflections on China's ICT Policy', International Journal of Communication 11 (2017), 1755-1774 (1755).

67 Jean-Christophe Plantin and Gabriele de Seta, 'WeChat as Infrastructure: the Techno-Nationalist Shaping of Chinese Digital Platforms', Chinese Journal of Communication 12 (2019), 257-273 (267-268).

68 Jennifer Pan, 'How Market Dynamics of Domestic and Foreign Social Media Firms Shape Strategies of Internet Censorship', Problems of Post-Communism 64 (2017), 167-188 (168).

 DOI 10.17104/0044-2348-2021-3-651

eignty' based on digital economy whereas the US sees dependence on China's ICT products and services as a threat to US economic security, a central element of national security under the National Security Strategy of the Trump Administration.[69] The President of the European Commission, Ursula von der Leyen, in seeking for her nomination, proclaimed that digital technologies are transforming the world at an unprecedented speed, changing both societies and economies, and digitalisation and cyber are two sides of the same coin. 'It may be too late to replicate hyperscalers, but it is not too late to achieve technological sovereignty in some critical technology areas.'[70] The concept of technological sovereignty is further elaborated by the European Commission in its Communication on Shaping Europe's Digital Future: 'European technological sovereignty starts from ensuring the integrity and resilience of our data infrastructure, networks, and communications. It requires creating the right conditions for Europe to *develop and deploy its own key capacities, thereby reducing our dependency* on other parts of the globe for the most crucial technologies. Europe's ability to define its own rules and values in the digital age will be reinforced by such capacities.'[71]

According to a briefing paper by the European Parliament Research Service, the notion of technological or digital sovereignty is proposed and portrayed as 'a means of promoting the notion of European leadership and strategic autonomy in the digital field'.[72] Concerns have been raised over the social and economic influence of non-EU technology companies, exemplified by contact tracing apps during the COVID-19 pandemic, which may undermine the EU's capacity to enforce its law and regulations, constrain European companies' potential for growth and weaken European citizens' control over their personal data.[73] Conceived of thus, digital sovereignty has economic value. As Frances Burwel and Kenneth Propp point out, the underlying rationale running through various legislative proposals by the European

69 National Security Strategy of the United States of America, December 2017, 13.

70 Ursula von der Leyen, 'A Union that Strives for More: My Agenda for Europe by Candidate for President of the European Commission', October 2019, 13. The concept of digital sovereignty as a new paradigm for Internet governance in fact emerged in European discourse before the von der Leyen Commission. Among the EU Member States, France is one of the most vocal in proposing such an idea. See, e. g. Farid Gueham, Digital Sovereignty – Steps Towards a New System of Internet Governance (translated by Caroline Lorriaux and Michael Scott, the Fondation pour l'innovation politique 2017).

71 COM(2020) 67 final, p. 2 (emphasis added).

72 Tambiama Madiega, 'Towards a More Resilient EU: Digital Sovereignty for Europe', EPRS Ideas Paper, PE 651.992 – July 2020, 1. Several Members of European Parliament, including Viviane Reding and Axel Voss, also promote enthusiastically the concept of 'digital sovereignty'.

73 Madiega (n. 72).

Commission, ranging from development and use of artificial intelligence and the participation of high-risk vendors in critical networks and management of data, lies in the EU's desire to strengthen its competitiveness vis-à-vis dominant players in the digital space.[74]

Upholding Internet sovereignty, digital sovereignty or data sovereignty in the interests of economic competitiveness will inevitably lead to suspicion and critiques of digital-protectionism or techno-protectionism. In a paper published by the European Political Strategy Centre (EPSC) in 2019, it is argued that China adopts techno-protectionism by pursing a state-centric approach built-upon comprehensive industrial strategic instruments and reduced dependence on imported foreign technologies. In this context, the EPSC underlines China's concept of cyber sovereignty contributes to this techno-protectionism.[75] Interestingly, Susan Ariel Aaronson, a professor at George Washington University, sees the EU (as well as the US) as hypocritical on the grounds that while the EU condemns digital protectionism, it adopts policies and practices which it would target and label as trade-distorting if adopted by other countries.[76]

In fact, economic competitiveness is situated in a broad context of economic independence or self-sufficiency,[77] which digital sovereignty aims to safeguard through the preservation of strategic autonomy. In this way, the EU is able to decide to maintain or reshape European ways of life. This thus links to the security rationale for the sovereignty fever in the cyber governance; the forerunner is undoubtedly the Trump Administration, but the Juncker Commission was also supportive of a technological race in the name of economic security and such position is followed and strengthened by the

---

74 Frances Burwel and Kenneth Propp, 'The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World, Atlantic Council Future Europe Initiative', Atlantic Council – Future Europe Iniative, Issue Brief, June 2020, 2. See Matthias Bauer and Fredrik Erixon, 'Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls', ECIPE Occasional Paper, 02/2020, 18-26. It should also be noted that the EU's desire to strengthen competitiveness extends from digital sovereignty to data sovereignty. According to the European Commission, the current situation of a small number of Big Tech firms dominating a large part of the world's data suppresses the potential of data-driven economy. The European Commission thus calls for finding a European way of data strategy to unleash the potential by 'balancing the flow and wide use of data, while preserving high privacy, security, safety and ethical standards'. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: a European Strategy for Data, Brussels, COM(2020) 66 Final, 19 February 2020, 3.

75 European Political Strategy Centre, 'Rethinking Strategic Autonomy in the Digital Age', EPSC Strategic Notes, Issue 30, July 2019, 12.

76 Susan Ariel Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?', World Trade Review 18 (2019), 541-577 (557).

77 European Political Strategy Centre (n. 75), 8-11.

 DOI 10.17104/0044-2348-2021-3-651

von der Leyen Commission.[78] As for China, national security is the upmost imperative and safeguarding cybersecurity in the name of Internet sovereignty is no surprise.

c) Security Concerns

Security concerns regarding the Internet are equally shared by the US, China, and the EU, but each conceives security differently. On the one hand, the US and China accuse one another of cyber theft and cyber espionage; on the other hand, China's conception of cybersecurity endorses giving greater weight to maintaining control of the Internet in the name of national security.

China's cybersecurity policy is built upon its National Security Law and specified and amplified in Cybersecurity Law. Article 59 of the National Security Law instructs the State to establish a national security review and oversight mechanism for foreign investments, critical materials and technologies, *the Internet and information technologies and services*. Under this overarching objective, the Cybersecurity Law regulates cybersecurity in two dimensions: network security and information security. Regarding network security, two provisions are most controversial: Articles 23 and 27. *Article 23* of the Cybersecurity Law instructs Chinese cybersecurity and information departments, together with the relevant departments of the State Council, to formulate and release a catalogue of critical network equipment and specialised cybersecurity products which are to comply and be certified with national security standards before coming to market.[79] Given the vague definitions of critical network equipment and specialised products, the scope of its application relies heavily on the discretion and interpretation of the administrative agencies.[80] Moreover, there are concerns that intellectual property rights may be infringed,[81] or malicious items or software inserted during

[78] In the wake of the COVID-19 pandemic, the European Commission in its recent communication on 2030 Digital Compass proclaims that '[t]he pandemic has also exposed the vulnerabilities of our digital space, its dependencies on non-European technologies, and the impact of disinformation on our democratic societies'. 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, COM(2021) 118 final, 9 March 2021.

[79] Art. 23 China's Cybersecurity Law.

[80] Jyh-An Lee, 'Hacking into China's Cybersecurity Law', Wake Forest Law Review 53 (2017), 57-104 (72).

[81] It is argued that foreign companies may be forced to hand over intellectual property to operate in China. Also, there is a danger of leakage of trade secrets during the security review processes as politically well-connected competitors may have a chance to see their profiles. Lee, (n. 80), 85.

the inspection and certification process. *Article 23* of Cybersecurity Law further obliges network operators to provide technical support and assistance to public security organs and national security organs safeguarding national security and investigating criminal activities.[82] Worries are voiced that network operators may lose their confidential information or trade secrets; or they may act as an instrument of Chinese cyber theft, surveillance and control, or espionage.[83]

In addition to enacting national legislation to safeguard cybersecurity, China has also pursued cybersecurity through diplomacy both with its allies and adversaries. Under the China-Russia Information Security Agreement, the two sides have attempted to strengthen cooperation in addressing threats to international information security arising from the application of information technologies, including national security and territorial integrity, critical information technology infrastructure, terrorism, crimes; also interference in countries' internal affairs, breaches of public order, and subversions of social-economic systems.[84] The broad scope and wide application of this agreement is reflective of the two countries' overly-inclusive conception of cybersecurity, and their obsessions with regime stability. Regionally, China has used SCO to address cybersecurity and fight what SCO members describes as three-evils: extremism, separatism, and terrorism.[85] The SCO led to the Agreement on Cooperation in Ensuring International Information Security in 2009 (SCO Information Security Agreement). Importantly, the parties see the 'use of *dominant position* in information space to the detriment of interests and safety of other states'[86] as a threat to their cybersecurity. The dominant position referred to here is, without doubt, that of the US.

Interestingly, whereas China sees the dominant position of the US as a threat to its cybersecurity, the US (and its allies) view China's cyber intrusions and operations against their governments, enterprises, and civil organisations, as threats to their cybersecurity. The US Department of Justice, under the Obama Administration, for the first time filed a criminal charge against known state actors, Chinese military hackers, for computer hacking and economic espionage.[87] The Chinese Defence Ministry responded with a strongly-worded statement which, referring to the Snowden and WikiLeaks,

82 Art. 27, China's Cybersecurity Law.

83 Lee (n. 80), 75.

84 Art. 2 China-Russia Information Security Agreement.

85 McKune and Ahmed (n. 52), 3842.

86 Art. 2.4 SCO Information Security Agreement.

87 Office of Public Affairs, Department of Justice, 'U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U. S. Corporations and a Labor Organization for Commercial Advantage', 19 May 2014, available at <https://www.justice.gov>.

accused the US of implementing worldwide surveillance based on its advantage in critical information technology infrastructure.[88] Diplomatic tensions between the US and China were resolved, or at least deescalated, with the signing of the US-China Cybersecurity Agreement in the lead up to President Xi Jinping's state visit to the US.[89] This agreement soon lost its relevance as Xi decided to pursue his China Dream and more aggressive diplomacy, and relations were complicated by the victory of Donald Trump in the 2016 US presidential election. The vulnerabilities of information and communication technologies and services to foreign actors, notably, China, are exposed and felt first by the US, and then the EU.

On 15 May 2019, US President Donald Trump issued an Executive Order on Securing the Information and Communications Technology and Services Supply Chain wherein he found that 'foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services […] in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people.'[90] He further found that the unrestricted acquisition, or use in the US, of information and communication technologies or services by foreign adversaries 'constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States'.[91] President Trump thus declared a national emergency with regards to that threat and ordered a halt to transactions on information and communication technologies, or services with foreign adversaries.[92] With this order, the participation of Huawei, a giant China telecom supplier, in US information and communication technologies and services have been effectively excluded.

Given the critical role of Huawei in the fifth-generation (5G) communications infrastructure and its close relations with the Chinese military, the US has strengthened its efforts to contain Huawei. Internally, on 16 May 2019, the Bureau of Industry and Security (BIS) of the Department of Commerce announced its decision to add Huawei and its sixty-eight non-US affiliates onto the Entity List of the Export Administration Regulations (EAR) as the BIS found that there was 'reasonable cause to believe that Huawei has been

88 The statement of the Ministry of Defense on the Decision of the US Department of Justice in Filing a Charge against Chinese Soldiers (国防部新闻发言人耿雁生就美司法部起诉中国军人发表谈话), 20 May 2014, available at <http://news.mod.gov.cn>.

89 On this agreement, see, e. g. Gary Brown and Christopher D. Yang, 'Evaluating the US-China Cybersecurity Agreement', The Diplomat, 19 January 2017, available at <https://thediplomat.com/>.

90 Executive Office of the President, Securing the Information and Communications Technology and Services Supply Chain, 15 May 2019, 84 Federal Register 22689.

91 Executive Office of the President (n. 90).

92 Executive Office of the President (n. 90), Sect. 1.

involved in the activities contrary to national security or foreign policy interests of the United States'.[93] Externally, the US has exercised a number of foreign policy instruments encouraging or coercing its allies to exclude Huawei from their telecommunications networks.

Built upon existent efforts in enhancing security in critical information and communication infrastructure and containing Huawei, the US intends to collaborate with its allies to form a coalition of trusted partners and establish a clean network, rooted in 'internationally accepted digital trust standards and is a reflection of our commitment to an open, interoperable, and secure global Internet based on shared democratic values and respect for human rights,'[94] and covering clean carriers, stores, apps, cloud services, and cables. 'The Clean Network initiative is a comprehensive effort to address the long-term threat to data privacy, security, and human rights posed to the free world from authoritarian malign actors.'[95] The Clean Network initiative, if implemented successfully, would lead to a two-speed or divided information and communication network between liberal democracies and authoritarian regimes, China in particular.

However, even though the Trump Administration sees economic dependence on China as a threat to US national security and the threat of China's potential exploitation of the vulnerabilities in information and communication technologies and services as a national emergency, the US has been cautious to avoid the term Internet sovereignty or its relevant variations. That said, in Trump's Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, a section on Internet freedom and governance supporting multi-stakeholder process, nearly made it into the final text, being edited out of the final version.[96] Similarly, whereas President Trump issued an Executive Order on Preventing Online Censorship, 'Internet freedom', the underlying value sustaining the US Internet policy, is not mentioned.[97] This reflects a shift in the Trump Administration's attitude toward cyber governance.

In contrast to the Trump Administration's resolute antipathy towards China, the EU's position is rather ambiguous on a number of measures to

93 Bureau of Industry and Security, Commerce. Addition of Entities to the Entity List, 16 May 2019, 84 Federal Register 22961.

94 U.S. Department of State, 'The Clean Network Safeguards America's Assets (Fact Sheet)', 11 August 2020, available at <https://www.state.gov>.

95 U.S. Department of State (n. 94).

96 Adam Segal, 'Chinese Cyber Diplomacy in a New Era of Uncertainty', Aegis Paper Series No. 1703 (Hoover Institution), 2.

97 White House, Executive Order on Preventing Online Censorship, 28 May 2020. See the Remarks of Hillary Clinton, former Secretary of State, on Internet Freedom, 21 January 2010, available at <https://2009-2017.state.gov>.

 DOI 10.17104/0044-2348-2021-3-651

strengthen cybersecurity, both at the EU- and Member State-level. The EU firstly established the European Union Agency for Cybersecurity (ENISA) through Regulation (EC) No 460/2004, the latest revision of Regulation (EU) 2019/881 that sets up a cybersecurity certification scheme for information and communications technologies.[98] Before this revision, it also adopted Directive 2016/1148 of the European Parliament and the Council concerning measures for common, high-level security of networks and information systems across the Union (the 'NIS Directive'), which obliges the Member States to identify operators of essential services and aims to pursue minimum level of harmonisation in safeguarding security of network and information systems.[99] Moreover, the European Commission published its recommendation on cybersecurity of 5G networks in 2019.[100] For the ENISA's part, it updated the Guideline on Security Measures under the European Electronic Communications Code (EECC),[101] released 5G Supplement to the Guideline on Security Measures under the EECC,[102] and published NIS investment reports based on survey of 251 organisations in France, Germany, Italy, Spain, and Poland.[103] However, these measures relate largely to coordination and exchange of information among Member States, but fail to address cybersecurity in a strategic way. Crucially, the EU's position on Huawei is not yet defined. 'The EU finds itself squeezed between an emergent China and a US fighting to retain its global tech supremacy.'[104]

With some hesitation, the EU, or at least some of its Members States, decided to join with the US in safeguarding cybersecurity. On 23 September 2019, on the side-lines of the General Debates of the UN General Assembly, 21 of 28 EU Members States, in conjunction with the US, issued a Joint Statement on Advancing Responsible State Behaviour in Cyberspace. The statement, without naming China, calls out irresponsible cyber behaviour targeting critical infrastructure and citizens, undermining democracies and international institutions and organisations, and undercutting fair competi-

98 Regulation (EU) 2019/881 of The European Parliament and of The Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 of 7 June 2019 on (Cybersecurity Act), OJ L 151/15.

99 OJ L 194/1, 19 July 2016.

100 Commission Recommendation of 26 March 2019, Cybersecurity of 5G networks, C (2019) 2335 final, Strasbourg, 26 March 2019.

101 ENISA, Guideline on Security Measures under the EECC, December 2020, 3rd edn, available at <https://www.enisa.europa.eu>.

102 ENISA, 5G Supplement-to the Guideline on Security Measures under the EECC, December 2020, available at <https://www.enisa.europa.eu>.

103 ENISA, NIS Investment Reports, December 2020, <https://www.enisa.europa.eu>.

104 European Political Strategy Centre (n. 75), 14.

tion in the global economy through cyber theft and cyber espionage, and called for 'safeguarding the benefits of a free, open, and secure cyberspace for future generations'.[105] The coordinated action of the Member States of the EU foreshadows the EU's realisation of its vulnerability to cyberattacks, which eventually led to the joint communication on *The EU's Cybersecurity Strategy for the Digital Decade*.[106] The European Commission and High Representative for the Common Foreign and Security Policy see cybersecurity as integral part of European security and propose three dimensions of the EU cybersecurity: (1) resilience, technological sovereignty, and leadership, (2) building operational capacity to prevent, deter, and respond, and (3) advancing a global and open cyberspace.[107] Most notably in this joint communication is its global dimension. On the one hand, the EU aims to work with international partners to advance and promote a global, open, stable, and secure cyberspace where international law and voluntary non-binding norms, rules, and principles of responsible state behaviour are respected.[108] On the other hand, the joint communication cautions that 'increased global connectivity should not lead to censorship, mass surveillance, data privacy breaches and repression against civil society, academia and citizens'.[109] In this connection, the promotion of human rights and fundamental freedoms online is critical and will be addressed below.

d) Human Rights

The divergent views on freedom of information vis-à-vis privacy against corporate collection on personal information are the underlying rationale that results in the different attitudes of the US and EU on global internet governance. Whereas internet freedom may arguably be upheld as a human right,[110] where the boundary of such freedom lies and how to reconcile and balance internet freedom/freedom of information and other human rights and public interests are the challenges facing sovereign states or regional integration organisations in this digital society. The US in its external (trade) agreements promote the free flows of data and information, which dictates

105 U.S. Department of State, 'Joint Statement on Advancing Responsible State Behavior in Cyberspace', Other Release, 23 September 2019, available at <https://www.state.gov>.

106 Joint Communication to the European Parliament and to the Council: the EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final, 16 December 2020.

107 Joint Communication to the European Parliament and to the Council (n. 106), 4.

108 Joint Communication to the European Parliament and to the Council (n. 106), 20.

109 Joint Communication to the European Parliament and to the Council (n. 106), 21.

110 See, e. g. Daniel Joyce, 'Internet Freedom and Human Rights', EJIL 26 (2015), 493-514 (493).

 DOI 10.17104/0044-2348-2021-3-651

the contracting parties, subject to limited exception, not to 'prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person'.[111] By contrast, the EU, in accordance with the European Charter of Fundamental Rights and General Data Protection Regulation (GDPR);[112] sets out the default position to prohibit data flows out of the EU unless similar degree of protection of personal information is ensured. In the past decade, three agreements between the US and EU (passenger name record, safe harbour, and shield) were held unconstitutional due to the insufficiency of US human rights protection). Therefore, the different weight endorsed to internet freedom and freedom of information on the one hand, and privacy and data protection on the other by the US and the EU is reflected in their respective regulatory approaches on cyber governance. Of greater relevance to this paper is privacy and data protection, which the EU relies on to defend its data sovereignty and this is one of the key divergences between the perceptions of the US and EU on cyber governance.

The GDPR recognises the threat posed to the protection of personal data arising from cross-border flows of personal data,[113] and dictates that in cases of personal data transferred to controllers, processors, or other recipients in third countries or to international organisations, the level of protection of natural persons ensured by the GDPR is not to be undermined.[114] Therefore, the GDPR sets up a default position that any transfer of personal data to a third country or an international organisation, subject to other provisions thereof, can only take place when the conditions laid down in Chapter V of the GDPR are complied with by the controllers and processors.[115] The legal effect arising from this provision is that unless equivalent level of protection on personal data is ensured, its cross-border transfer is prohibited, introducing a key feature of data sovereignty.

The incompatibility of the US legal regime on privacy and personal information with the EU data protection standard has given rise to several disputes, including *Passenger Name Records Agreement*,[116] *Schrems I* on safe

111 Art. 19.11.1 UMSCA and Art. 11.1 US-Japan Digital Trade Agreement.

112 See generally, Christopher Kuner, Lee A. Bygrave, Christopher Docksey and Laura Drechsler(eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press 2020).

113 Recital 2, GDPR.

114 Recital 3, GDPR.

115 Art. 44, GDPR.

116 Joined cases *European Parliament v. Council of the European Union* (C-317/04) and *Commission of the European Communities* (C-318/04), judgement of 30 May 2006, ECLI:EU:C:2006:346.

harbour decision,[117] and *Schrems II* on shield decision.[118] The main thrust of this series of decisions basically relates to the delicate balance between national security, public interest, or law enforcement, and individual rights on data protection; the Court of Justice of the European Union (CJEU) ruled in all three cases that the transfer of personal data from the EU to US is not permissible as an equivalent level of protection is not ensured in the US legal system and thus poses a threat to the personal information of EU citizens.

As the CJEU declares in *Schrems II*, 'the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter [of Fundamental Rights of the European Union] […]. The same is true of the retention of personal data and access to that data with a view to its use by public authorities.'[119] The CJEU nonetheless cautions that such rights are not absolute rights, but must be considered in relation to their function in society.[120] The CJEU holds that 'any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms',[121] and the principle of proportionality shall guide this limitation. The CJEU thus arrives at the conclusion that the privacy shield decision does not comply with the requirements of the GDPR and Charter as Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333 excessively interfere individual rights and undermine protection of personal data.[122]

The reasoning of the CJEU marks a sharp contrast with the position of the US, in particular under the Trump Administration. Whereas the US places great weight on national security and less on data protection obligations, the CJEU emphasises the role of the Charter in regulating cross-border transmission of personal data and the importance of principle of proportionality in constraining such regulation. Seen from this perspective, the reason for preventing cross-border transfer of personal information and localising of data within the EU is to ensure the high degree of data protection enjoyed under the European legal order is not undermined through its export to third countries.

---

117 Request for a preliminary ruling under Article 267 TFEU from the High Court (Ireland) in the proceedings *Maximillian Schrems v. Data Protection Commissioner* (*Schrems I*), judgement of 6 October 2015, case no. C-362/14, ECLI:EU:C:2015:650.

118 Request for a preliminary ruling under Article 267 TFEU from the High Court (Ireland) in the proceedings *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems* (*Schrems II*), judgement of 16 July 2020, case no. C-311/18, ECLI:EU:C:2020:559.

119 CJEU, *Schrems II* (n. 118), para. 171.

120 CJEU, *Schrems II* (n. 118), para. 172.

121 CJEU, *Schrems II* (n. 118), para. 174.

122 CJEU, *Schrems II* (n. 118), para. 184.

 DOI 10.17104/0044-2348-2021-3-651

IV. Concluding Remarks: The Territorial Turn and Two-Speed Internet

The rise of emergent countries in general, and China in particular, has challenged the liberal global Internet, which evolved in a multi-stakeholder environment. In territorialising cyberspace and translating the concept of national sovereignty into cyberspace, China has introduced a concept of Internet sovereignty designed to serve its domestic needs: the maintenance of regime stability by controlling information flows. The concept of Internet sovereignty has also an external dimension, for China aims to transform the multi-stakeholderist cyber governance model into a multilateral one, wherein countries enjoy sovereignty and the ultimate authority to shape their online spaces. As a country that guards sovereignty jealously, China's preference for bringing sovereignty into the cyberspace is not surprising. However, sovereignty is not the last word in debates concerning the future of digital society, for even liberal democracies have advanced ideas of technological or digital sovereignty, and data sovereignty, for their own very different purposes.

This article argues that the proliferation of the notion of Internet sovereignty and its variances can be attributed to four reasons: political ambition, economic value, security concerns, and human rights. A sharp contrast can be seen in the divergences between the EU and the US on the cross-border transfer of personal data, giving rise to several disputes in the CJEU. On the one hand, these disputes illustrate the delicate balance between national security and human rights, and the different weights the EU and US give to these two competing values. On the other hand, the EU's struggle for technological sovereignty also reflects the security threat posed by the digital transformation of society. If the EU aims to persevere its values and ways of life, it has to retain strategic autonomy and technological sufficiency. This reflects a critical change in economic interdependence and a return to economic independence, at least self-sufficiency.

Seen in this light, the sovereignty fever is a symptom reflecting sovereign states' attempt to retain autonomy and control gradually eroded with the digitalisation of societies and economies. The utopia of a borderless and interconnected cyberspace thus loses its charm and the global cyber order is witnessing a territorial turn. China has long established the Great Firewall to control and filter information flows. The EU, in the name of data protection, erects substantial barriers for personal information from transferring outside the Union. Most importantly, in the long race of 5G competition and safeguarding critical information and communication infrastructure, the US and its allies aim to build a Clean Network by bypassing China, which will result

in a two-speed network between liberal democracies and authoritarian regimes, China in particular.

Probing into the future, the trend for territorialising the cyberspace and the ambition to regulate and control information and data flows and retain technological autonomy in the digital society will be intensified as one of the bitter lessons learnt from the global pandemic of COVID-19 is how weak the global supply chain is. Countries thus rush for technological independence and self-sufficiency in the name of technological sovereignty. The global pandemic also exposes the threats of disinformation in the digital age and how to regulate social media becomes a top priority for sovereign states and regional integration organisations. Digital and data sovereignty will be the catchy words for the years to come and the sovereignty fever will persist.

 DOI 10.17104/0044-2348-2021-3-651