Chapter 27
Balkanization Instead of Eurasianism: Fragmented Technological Governance Across the OSCE Domain and Its Implications

Tobias Burgers

27.1 Introduction

Digital technologies have fundamentally changed and transformed our lives, and cyberspace has assumed dominance in society. Indeed, as Nassehi (2019) illustrates, while not all of society's interactions occur in the digital realm or through digital technologies, we have become a society that predominantly can be understood by and through digital means. The importance of and reliance on digital technology will only further increase with the integration of technologies such as AI, big data, deep learning, autonomous machines, and the internet of things (IoT). These technologies, at times described as "general-purpose technologies," are finding ways to change and even overhaul our societies (UNESCAP, 2020). It is these changes that will determine how technologies will be placed and valued in any given societal context. While we may think of these technologies as neutral, they will have a substantial impact, evoking changes depending on how and for what objectives they are being used. Considering these changes up to the present time and those currently emerging, fundamental questions must be raised about how nations and societies will control and direct these technologies. What previously were considered questions and concerns of technical and technological management, best left to technical experts, have evolved into questions of societal importance, requiring urgent governance of technologies by lawmakers, politicians, and bureaucracies (Goodman & Lin, 2007). Among these questions are those addressing the purpose of the concerned technologies and whom they should benefit.

T. Burgers (✉)
Faculty of Social Sciences, Fulbright University, Ho Chi Minh City, Vietnam
e-mail: tobias.burgers@pm.me

A. Mihr et al. (eds.), *Securitization and Democracy in Eurasia*,
https://doi.org/10.1007/978-3-031-16659-4_27

27.2 Technological Governance in Eurasia

For a considerable time, the rise of digital technologies and the global proliferation of the internet were popularly considered a force for the good, one which would promote and foster democracy (Best & Wade, 2009; Gotlieb, 2002) by disseminating information and increasing its quality and availability (Hindman, 2008). This would enable it to support human rights and good governance (Selian, 2002). Such a utilitarian view of technology saw prominence in the first decade of this century with the mass social uprisings of the Arab Spring, the Twitter revolution in Iran, and the Rose and Orange revolutions in Ukraine and Georgia. It seemed that cyberspace and digital technologies—in particular social media—functioned in all of them as catalysts for democratic change and human rights progress (Wolfsfeld, 2013). These desirable values went hand in hand with a tech governance model that emphasized that the internet and digital technologies should be minimally controlled by individual nation states. Some proponents of this model even argued that the internet and digital technologies were in fact difficult, if not impossible, to administer and govern. Famed is the quote by the then US President, Bill Clinton, who commented on early Chinese efforts to regulate and control the internet and digital technologies, saying, "Now there's no question China has been trying to crack down on the Internet. Good luck! That's sort of like trying to nail Jell-O to the wall" (New York Times, 2000). This vision of technology was combined with a tech governance model, advocated by the USA and supported by the EU, that sought to keep state interference to a minimum, with minimal governmental oversight and responsibility for managing and governing cyberspace and digital technologies in the hands of tech companies. However, over the last two decades, other visions of how technology should be used, regulated, and governed in view of definite objectives have arisen. Chief among the proponents of such a vision is China, which has been developing an alternative governance model since the start of this century, known as the "Networked Authoritarianism" model (Burgers & Robinson, 2016; MacKinnon, 2011). This model is extensive in its aims and in the reach of governance efforts and has been remarkably successful. China has been able to control its national internet through the Great Firewall and has been highly effective in surveilling its cyberspace, imposing rules on information allowed onto the Chinese internet, and setting out under which conditions selected companies—national and international—can participate in Chinese cyberspace activity (Ibid, 2011, 2016). These policies demonstrate that it is possible to nail Jell-O to the wall (Allen-Ebrahimian, 2016). Through legal and regulatory frameworks, the Chinese government strictly regulates and controls tech companies while advocating—nationally and internationally—for cyber sovereignty. The frameworks determine data management practices and content that can be hosted in authorized frameworks with government access to and control over data. Meanwhile, and more recently, the Chinese Communist Party (CCP) has also set (micro) rules and regulations aimed at internet celebrities and influencers, illustrating the broad and in-depth reach of Chinese tech governance efforts. Their success illustrates two things. First, it is perfectly feasible to control, regulate, and govern digital technologies and cyberspace. Second, cyberspace and digital technologies are well suited to the attempts of authoritarian regimes to surveil and control their societies. Inspired by China, its northern neighbour Russia has sought to follow suit, albeit less successfully. Its tech model overlaps with the Sino model in its aims to rein in tech companies, ensure official access to and control over data, and establish cyber sovereignty. However, the Russian governance efforts have been less extensive and detailed.

27.3 External Technological Players in the Region

While China has perfected its Networked Authoritarianism model, the European Union (EU), witnessing the growing power of tech companies and the harmful effects of data-driven economies and societies, has sought to put the brakes on "big tech," and regulate and govern cyberspace and digital technologies (Bremmer, 2021). These efforts have led to the emergence of a distinctive European tech governance model which emulates that of China in its strong regulatory efforts and the reach of its governance model. This is reflected in policies such as the European Commission's digital policy roadmap "Shaping Europe's Digital Future," the General Data Protection Regulation (GDPR), the Digital Markets Act (DMA), and the Digital Services Act (DSA). Part of these policies is the integration of Artificial Intelligence (AI) under the concept of "trustworthy AI" (Fefer, 2021). In this regard, the EU has sought to curb the excesses of digital technology, while maintaining the vision that digital technology can remain a force for the better, the promotion of democracy, the fostering human rights, and the supporting of equality. Finally, there seems to be a noticeable shift even in the United States, with the growing perception that its laissez-faire model needs a regulatory overhaul. The recent Facebook revelations and the growing power of big tech, among other concerns, are spurring a national movement to develop a new tech governance model that would seek to restrain the sprawling power of the tech companies themselves (Bremmer, 2021). Some success has been achieved, most notably with the California Consumer Privacy Act (CCPA). Yet, on a federal level, strong(er) regulations are still a work in progress, with an uncertain outlook on what an updated American model of tech governance might look like.

27.4 (Tech) Competition or "Balkanization" Ahead?

We have seen how, across two decades, the early unipolar and utilitarian vision of tech governance has transformed into a mosaic of different tech governance models. While there is some overlap between these models, including—surprisingly—between the Chinese and the EU models, they are essentially different. This diversification of tech governance models along separate paths has led to the emergence of what Malcomson

(2015) refers to as the “splinternet” or, as it is alternatively known, the “Balkanization” of cyberspace and tech governance (O’hara & Hall, 2018). Diversification has provided other nations, which are increasingly seeking to integrate new digital technologies into their societies, with a number of policy options regarding the purpose and the means with which to achieve it. This development has unsurprisingly created competition between the various models. In the current era of increasing geopolitical competition between the United States and China, and increasingly also between the EU and China, as well as the United States and Russia, the tech domain has also become subject to intense competition.

27.5 The Role of the OSCE in Global Tech Competition

The Organization for Security and Co-operation in Europe (OSCE) currently finds itself amidst competing international approaches to cyberspace oversight. As an intergovernmental organization that “assists host countries in putting their OSCE commitments into practice,” it plays a role of considerable importance (OSCE, 2021a). Furthermore, through its field operations, it supports national authorities in developing new policies (Ibid, 2021a). This gives the OSCE the ability to influence policies and thereby punch above its weight in the technological governance debate. It could, in theory, function as an actor that, through the promotion of specific tech governance models, might enhance unipolarity and limit the possible balkanization of cyberspace. However, for this to occur, emerging tech nations need to be receptive to OSCE tech policies. Also, we need to determine if any other actors that provide alternative models, such as China, would have the ability to steer the development of technological governance.

Being receptive to OSCE tech policies starts with understanding what they offer. Here, we must differentiate between policies and programmes that focus on digital security governance (ICT, cybersecurity, cyber conflict, and critical infrastructure protection) and policies that provide a framework for governing digital technologies suited to particular objectives (OSCE, 2021b). The former policies focus on preventing actual cyber conflict and crime. These can be bolstered through projects such as cyber awareness month, a training programme of national cyber police forces and courses on cyber security confidence-building measures (OSCE, 2021b; 2021c, 2021d). With regard to providing frameworks for governing digital technologies for particular outcomes, it is apparent that the OSCE views digital technologies as (potential) enablers for good governance. The organization regards digital technology as a force that can contribute to shaping better and fairer media, improve accessibility to information, support freedom of expression, and constitute a tool that combats corruption, labour issues, sex trafficking, and so on. In addition, the OSCE believes that technology can enhance democratic functions and foster sustainable development (OSCE, 2021e, 2021f, 2021g, 2021h, 2021i). In particular, the Office for Democratic Institutions and Human Rights (ODIHR) within the OSCE promotes the idea of digital technologies in just this sense (2021); “Governments, civil society and religious or belief communities can engage in the digital sphere to foster mutual respect, understanding, and inclusion. Increased digitalization can go a long way towards addressing systemic inequalities and barriers […] At the same time, civil society can tap into the potential of the digital space to streamline and synergize its efforts, which increasingly depend on new technologies when faced with limited resources, increased workload and decreased capacity, especially during the pandemic" (ODIHR, 2021). The OSCE seeks to bring these beliefs into practice through ODIHR co-sponsored meetings such as the Supplementary Human Dimension Meeting (SHDM) III, which is focused entirely on digital technologies. In the words of OSCE Director-General Elinor Hammarskjöld, "Digital technologies have great potential to promote and enhance the enjoyment of human rights, democracy, and the rule of law" (OSCE, 2021i).

Clearly, the OSCE, and in particular the ODIHR, advocate for and aim to advance a tech governance model that is situated between the American and European models: A model that understands digital technologies as tools that can foster good governance, promote, and enhance democracy, and foster human rights and freedoms, rather than one which regards them as tools for surveillance and digital control. Furthermore, through its activities, the OSCE seeks to advance data protection policies in its member states. Thus, the OSCE's digital governance policies and ideas align with the organization's overall goals of supporting and promoting democratic development, human rights, the rule of law, and good governance.

27.6 Digital Policies and Politics in the Central Asian Nations

Examining the literature for ongoing tech projects, developments, and early tech governance efforts in three Central Asian nations—Kyrgyzstan, Tajikistan, and Turkmenistan—we find indicators of emerging tech governance (UNESCAP, 2020). Projects such as "Digital Kyrgyzstan 2019–2023" illustrate this point very well. Tajikistan has likewise presented such initiatives (World Bank, 2016). Much of this initial vision of how digital technologies should be utilized focuses on economic development. It is felt that they should streamline and improve the financial sector and supply chain management, allow for the development of e-commerce, and finally enhance agricultural output (Jenish, 2019; UNESCAP, 2020). Beyond this, there is some limited evidence that the three nations additionally saw digital technologies also as tools for improving governance. As the then President of Kyrgyzstan, Jeenbekov, noted "The digitization of society is a requirement of today. This will open up new opportunities for our citizens. The human factor in the provision of public services will be excluded, which will contribute to the eradication of corrupt elements" (Jeenbekov, in Alkanova, 2019). Other literature shows how regional governments initially saw digital technologies as tools for enhancing governmental services and improving democratic local governance, particularly in Kyrgyzstan (Brimkulov &

Baryktabasov, 2014; Dzhusupova, 2015). This indicates, at least in theory, that the three nations appeared to be supportive of the original OSCE vision. Nevertheless, observing the current situation, it seems those lofty goals and ideas have not been turned into reality. Spurred by the COVID-19 pandemic, a wide-ranging group of authors notes how the three nations have used digital technologies for surveillance and control purposes and as tools to suppress free speech, human rights, and democratic liberties instead. As Shastry notes, “Too many governments in the region are focusing on control and surveillance instead of citizens’ rights.” This indicates that, despite best earlier intentions, the three nations are increasingly rejecting the OSCE tech governance model and are moving towards a tech governance model akin to the Chinese model.

Furthermore, strong support from Chinese official and private actors increases the likelihood of Kyrgyzstan, Tajikistan, and Turkmenistan advancing along the Sino model of technological governance. Through the framework of the Belt and Road Initiative (BRI) and the Digital Silk Road (DSR), Chinese state and non-state actors can provide these Central Asian nations with below-market priced digital tools and technologies such as big data and deep learning programmes, hardware for mobile infrastructure, digital command centres for police forces, facial recognition software, digital monitoring systems, and other video surveillance systems (Burgers, 2022). What only enhances the interest of the region in Chinese technology projects, such as the “Safe Cities” and “Sharp Eyes” projects, is that these governmental programmes utilize digital technologies for surveillance purposes (Marat & Sutton, 2021). This suggests that Chinese hardware and tech governance policies will assume an ever-widening presence, and may even become the standard among those three nations.

27.7 Balkanization Instead of Eurasianism: Implication and What the OSCE Can Do

Whereas initial technology policies indicated some desire to follow a liberal model of technological governance, with limited regulation and the use of technology as a force for good, the current observation is that, because of the growing degree of Chinese technological surveillance resources and programmes, the Central Asian states are pivoting away from their initial preference for the liberal model towards the Chinese technological governance model. This development, which is likely to receive Russian support, seems to ensure that Kyrgyzstan, Tajikistan, and Turkmenistan will most likely embrace tech governance models in line with those of China and Russia. This will lead to a further fragmentation and increased cyberbalkanization of the digital sphere in the region. This brings up the question of what the OSCE, as an active participant in these countries, can effectively do to advance its own model of technological governance, i.e. a model that seeks to utilize digital technologies as tools with which to positively impact the economic sector, assist political freedom, enhance good governance, and ensure that digital technologies are embraced as a force for the social good. It is a question which remains unanswered, and a topic which requires much further research and discussion.

References

Allen-Ebrahimian, B. (2016, June 29). The man who nailed Jello to the wall. *Foreign Policy*. Retrieved November 10, 2021, from https://foreignpolicy.com/2016/06/29/the-man-who-nailed-jello-to-the-wall-lu-wei-china-internet-czar-learns-how-to-tame-the-web/.

Best, M. L., & Wade, K. W. (2009). The internet and democracy: Global catalyst or democratic dud? *Bulletin of Science, Technology & Society, 29*(4), 255–271. https://doi.org/10.1177/0270467609336304

Bremmer, I. (2021, November 9). The technopolar moment how digital powers will reshape the global order. *Foreign Affairs*. Retrieved November 10, 2021, from https://www.foreignaffairs.com/articles/world/2021-10-19/ian-bremmer-big-tech-global-order.

Brimkulov U. & Baryktabasov K. (2014). Public transactional e-services through government web sites in Kyrgyzstan. *Electronic Journal of e-Government*, *12*(1), 39–53. www.ejeg.com

Burgers, T. J. (2022). Assessing the economic and political success of the digital silk road throughout the Indo-Pacific Region. In F. Liu., & D. Karalekas, (Eds.), *Middle-Power responses to China's BRI and America's Indo-Pacific strategy: A transformation of geopolitics*, Emerald Publishing, (forthcoming)

Burgers, T., & Robinson, D. R. (2016). Networked authoritarianism is on the rise. *Sicherheit & Frieden, 34*(4), 248–252. https://doi.org/10.5771/0175-274x-2016-4-248

Dzhusupova, Z. (2015). Enabling democratic local governance through rural E-municipalities in Kyrgyzstan. *Human rights and ethics, 1009–1033*. https://doi.org/10.4018/978-1-4666-6433-3.ch055

Fefer, R. F. (2021). EU digital policy and international trade .*Congressional research service*. Retrieved November 11, 2021, from https://crsreports.congress.gov/product/pdf/R/R46732/4.

Goodman, S. E., & Lin, H. (2007). *Toward a safer and more secure cyberspace*. National Academies Press.

Gotlieb, C. C. (2002). Does the internet promote democracy? *IFIP Advances in information and communication technology, 21–29*. https://doi.org/10.1007/978-0-387-35609-9_2

Hindman, M. (2008). The internet and the "democratization" of politics. (2009). *The Myth of digital Democracy*, 1–19. https://doi.org/10.1515/9781400837496-003

Jenish, N. (2019). Macroeconomic policy frameworks and technological development: Case studies of Kyrgyzstan, Tajikistan and Afghanistan, *University of Central Asia – Institute of Public Policy and Administration (IPPA)* Working Paper No. 49. SSRN: https://ssrn.com/abstract=3807758 or https://doi.org/10.2139/ssrn.3807758

MacKinnon, R. (2011). China's networked authoritarianism. *Journal of Democracy, 22*(2), 32–46. https://doi.org/10.1353/jod.2011.0033

Marat, S., & Sutton, D. (2021). Technological solutions for complex problems: Emerging electronic surveillance regimes in Eurasian Cities. *Europe-Asia Studies, 73*(1), 243–267. https://doi.org/10.1080/09668136.2020.1832965

Malcomson, S. (2015, December 23). Welcome to the splinternet. *Techonomy*. Retrieved November 10, 2021, from https://techonomy.com/2015/12/welcome-to-the-splinternet/.

Nassehi, A. (2019). *Muster Theorie der Digitalen Gesellschaft*. C. H. Beck Verlag.

The New York Times. (2000, March 9). Clinton's words on china: Trade is the smart thing. *The New York Times*. Retrieved November 10, 2021, from https://www.nytimes.com/2000/03/09/world/clinton-s-words-on-china-trade-is-the-smart-thing.html.

Organization for Security and Co-operation in Europe (OSCE). (2021a). *OSCE cyber security awareness month.* OSCE. Retrieved November 10, 2021, from https://www.osce.org/cyber-security-awareness-month.

Organization for Security and Co-operation in Europe (OSCE). (2021b). *Cyber/ICT security.* OSCE. Retrieved November 10, 2021, from https://www.osce.org/cyber-ict-security.

Organization for Security and Co-operation in Europe (OSCE). (2021c). *To serve and to protect: The OSCE trains the next generation of Ukraine's cyber police.* OSCE. Retrieved November 10, 2021, from https://www.osce.org/ukraine/270776.

Organization for Security and Co-operation in Europe (OSCE). (2021d). *OSCE Cyber/ICT security confidence-building measures.* elearning.osce.org. Retrieved November 10, 2021, from https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCBM_v1+2020_11/about.

Organization for Security and Co-operation in Europe (OSCE). (2021e). *Media freedom and development*. OSCE. Retrieved November 10, 2021, from https://www.osce.org/media-freedom-and-development.

Organization for Security and Co-operation in Europe (OSCE). (2021). *OSCE Webinar promotes use of digital technologies in combating corruption in Turkmenistan.* OSCE. Retrieved November 10, 2021, from https://www.osce.org/centre-in-ashgabat/466800.

Organization for Security and Co-operation in Europe (OSCE). (2021g). *Greater efforts needed to ensure digital technologies empower human rights, OSCE Leaders Say*. OSCE. Retrieved November 10, 2021, from https://www.osce.org/chairmanship/492730.

Organization for Security and Co-operation in Europe (OSCE). (2021h). *Principles on identification for sustainable development: Towards the digital age.* OSCE. Retrieved November 10, 2021, from https://www.osce.org/odihr/principles-on-identification-for-sustainable-development-towards-the-digital-age.

Organization for Security and Co-operation in Europe (OSCE). (2021i). *Principles on identification for sustainable development: Towards the digital age (second edition).* OSCE. Retrieved November 10, 2021, from https://www.osce.org/odihr/496387.

Office for Democratic Institutions and Human Rights (ODIHR). (2021). *The power of digital technologies must be harnessed to counter hatred based on religion or belief, Odihr says.* OSCE. Retrieved November 10, 2021, from https://www.osce.org/odihr/461140.

O'hara, K., & Hall, W. (2018). *Four internets: The geopolitics of digital governance*, (CIGI Papers, 206). The Centre for International Governance Innovation (CIGI)/Chatham House, pp. 28.

Selian, A.N. (2002). *ICTs in support of human rights, democracy and good governance.*

United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP). (2020). *Realizing digital potential in North and Central Asia.* United Nations. Retrieved November 10, 2021, from Realizing_digital_potential_in_North_and_Central_Asia.

Wolfsfeld, G., Segev, E., & Sheafer, T. (2013). Social media and the arab spring. *The International Journal of Press/politics, 18*(2), 115–137. https://doi.org/10.1177/1940161212471716

World Bank. (2016, March 18). *Reaping the benefits of digital technology in Central Asia.* World Bank. Retrieved November 10, 2021, from https://www.worldbank.org/en/news/feature/2016/03/15/reaping-the-benefits-of-digital-technology-in-central-asia.