DIGITAL AUTHORITARIANISM 'MADE IN CHINA': INSTALLING A DIGITAL DYSTOPIA

Pregledni rad (Review Paper)
Received: 22 November 2021
Accepted: 14 January 2022
DOI: https://doi.org/10.37458/nstf.23.1.7

Andrew N. Liaropoulos*

Abstract:

The COVID-19 pandemic has magnified the use of digital technologies in the name of public health and safety and vividly illustrated how societies, even democratic ones, can tolerate the expansion of executive power and accept restrictions on liberties. In China,

* Dr. Andrew N. Liaropoulos is Assistant Professor in University of Piraeus, Department of International and European Studies, Greece. His research interests include international security, intelligence reform, strategy, foreign policy analysis, European security policy and cyber security. Dr. Liaropoulos is also a senior analyst in the Research Institute for European and American Studies (RIEAS) and a member of the editorial board of the Journal of Information Warfare (JIW) and of the Journal of European and American Intelligence Studies (JEAIS).

the pandemic justified the use of such technologies and policies to a further extent, but also served as a proof by the government, that its model of digital control succeeded in handling the coronavirus crisis. This paper reviews the Chinese model of digital authoritarianism and highlights its implications for democracy and civil liberties, since China is aiming to export its model around the globe. It manifests the rationale and techniques of this model, but also China's position on internet governance and techno-nationalism. China is leading the way on AI and surveillance technology and is exporting its model abroad, via the Digital Silk Road, the technology component of the Belt and Road Initiative. The exportation of the digital authoritarianism model is targeting mainly states in East Asia, Africa and Latin America, but its implications are global, if digital surveillance and social credit systems become the new normal.

Keywords: COVID-19, digital technologies, China, digital authoritarianism Bel and Road Initiative

Introduction

Information and communication technologies (ICTs) enable the exchange of a vast amount of data and thereby bridge social and economic inequalities all over the world. The rapid and low-cost exchange of information has enabled the political, economic, and social participation of citizens, thus promoting the spread of human rights and democracy, even within authoritarian states. Social media platforms and messaging applications have been used to mobilize citizens in defending their rights and in assisting human rights activists to gather

and disseminate information to the general populace. Nevertheless, the same technologies that are used to emancipate people are also used by repressive regimes to limit human rights and exercise control. Over the past years, we have witnessed the retreat of Internet freedom and the rise of digital authoritarianism (Kamasa, 2020).

Digital surveillance, development of content filtering tools, online censorship, interference with service providers and paying micro-bloggers to spread positive information about the government, are only some of the means at the disposal of states (Morozov, 2011). The use of digital technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations is affecting civil liberties and democracy worldwide. This technology-enabled authoritarianism involves online censorship and mass surveillance using cameras, facial recognition programs, drones, GPS tracking, algorithms, and other technologies, that strengthen authoritarian control and enable social engineering[1].

Although many states have developed digital tools to conduct censorship and surveillance, the case of China is a rather unique one for two reasons. First, China has established by far, the most sophisticated model of digital authoritarianism. Under Xi Jinping's leadership, the Chinese Communist Party (CCP) has established a population-wide digital surveillance system that includes internet service providers, data analytics companies and social media websites. It can be argued that in China, the ominous metaphors of Big Brother and Panopticon, have become a reality. Second, China is aggressively exporting surveillance and monitoring systems to several countries in East Asia, Africa and Latin America (Polyakova & Meserole, 2019). The Digital Silk Road (DSR) - a key component of the Belt and Road Initiative (BRI) - is critical in influencing the development of cyber norms and standards regarding global Internet governance. The type of development model that China is exporting to the developing world - capitalism with Chinese char-

[1] For a balanced analysis on global Internet freedom, online censorship, and digital surveillance, see selectively the annual reports of Freedom House https://freedomhouse.org/.

acteristics - is accompanied by a model of digital surveillance and societal control, which poses significant constraints on domestic liberties (Crosston, 2020, p. 151). China is not only engaged in building the digital infrastructure of developing nations, but also in advancing censorship and opinion-shaping technologies. The purpose of this paper is to analyze the means and methods that China has used, in order to establish a digital surveillance state and export its model of digital authoritarianism in the developing world.

1. China's Digital Authoritarianism

Over the past two decades, authoritarian regimes have invested on digital means to monitor and suppress opposition. They have developed a variety of measures, which violate freedom of expression and the right to privacy, like targeting dissident voices, internet filtering practices and disconnecting access to ICTs (Liaropoulos, 2016, p. 35, Keremoğlu & Weidmann, 2020). The social revolutions that took place in Iran, Tunisia, Egypt and other countries during the so-called Arab Spring, vividly illustrated how social media can function as a force multiplier, but also alarmed authoritarian regimes to utilize the same means in order to secure their political survival (Liaropoulos, 2013).

China is a tech-enabled autocracy, but to become one, it first had to rise as a digital power. The CCP does not view digitalization, as an opportunity for China to become more open and liberal, but rather as an opportunity to strengthen its regime (Ingster, 2016). China's digitalization process is driven by both private companies and by the state's strategic initiatives, including social governance. Indicative of this process in both the private sector and society are the following two policies, the 'Social Credit System' and the 'Made in China 2025'. The 'Social Credit System' that was originally announced in 2014, aspires to develop a system that encourages its citizens to protect social trust in every aspect of their lives. The CCP realized that by exploiting surveillance technology and big data, it can create a

comprehensive system for monitoring individual and organizational behavior, and thereby ensure compliance and trust within the society. In the private sector, social credit is seen as a framework to enhance transparency and to ensure increased compliance with government regulations. On the individual level, such an integrated system is seen as a mechanism for ensuring lawful behavior and maintaining social order. By rewarding and punishing citizens based on the morality of their actions, the CCP has introduced a point-system that aims to maintain high levels of public trust and safeguard harmony within the country (Lilkov, 2020, p. 33).

The 'Made in China 2025' is an industrial policy that aims to increase the ratio of China's domestic core technologies and essential industries through subsidies and investment funds by 2025 (Ito, 2019, p. 54). It points out ten priority sectors, including robotics, information technology, aerospace technology and pharmaceuticals, in which Beijing is aspiring to dominate by 2025 by combining protectionism, import substitution and state financing (Sinkkonen & Lassila 2020, p. 6). This policy is in accordance with Beijing's techno-nationalism that intents to reduce dependence on imports of vital digital and communications hardware. Bearing in mind that the US is one of the key exporters of microchips and tech equipment to China, Washington's decision in 2018 to ban US companies from selling microchips to ZTE - China's second biggest telecoms company - served as a wake-up call for Chinese decision-makers (Lilkov, 2020, p. 24).

Reducing dependence is only one aspect of Beijing's techno-nationalism. Banning foreign big tech companies and social media platforms from entering the Chinese market and thereby influencing Chinese society is another form of techno-protectionism. China has banned among others Google, Wikipedia, YouTube and Facebook, but at the same time created similar digital products that are state controlled. By banning foreign competition, the CCP strategically offered China's huge domestic market for exploration, only to national companies - Baidu, search engine, Tencent, entertainment platform, Alibaba, electronic commerce, Weibo, social media plat-

form and WeChat, text messaging services (Lilkov, 2020, p. 22).

Chinese technological giants are a crucial part of China's digital authoritarianism. Chinese big tech companies (Alibaba, Tencent, Baidu, etc.) are required by law to cooperate in matters of national security and intelligence, by aiding surveillance and making available their expertise, products, and data for the government's objectives. Vast amounts of data are transferred from private companies to government authorities systematically since the former are legally compelled to provide a backdoor for authorities to access any encrypted data. Since the government can access such information on broad scale, its big data analytics and thereby predictive analytics become more accurate (Khalil, 2020, p. 9).

From the early days of the Internet development in China, Beijing aimed to block online content. The 'Great Firewall' - meaning a system of software and hardware that determines the acceptable and prohibited content - allows China to seal off the Chinese internet from the rest of the global Internet and thereby practice its version of cyber sovereignty (Creemers, 2020).[2] Elements of this system are internet protocol blocking, deep packet inspection that examines network traffic[3], keyword filtering and banning the use of virtual private networks. The 'Great Firewall' also blocks foreign internet tools and mobile apps, and stresses foreign companies to adapt to domestic regulations. The purpose of the 'Great Firewall', is not only to create a closed internet, but also to control its users (Griffiths, 2020). Adding to that, the Cyberspace Administration of China (CAC) which serves as the central internet regulator, censor, oversight, and control agency for the Chinese government, forces digital platforms to invest in their own technology to censor

[2] In relation to the global Internet governance, China promotes a multilateral model of governance, where states are able to regulate their web within their borders and not the multi-stakeholder model, where civil society, the private sector and governments collectively manage the rules of Internet.

[3] Data that is transferred via the Internet is broken down into smaller packets. Deep packet inspection is able to check the content of the packets, know where it came from and where it is going, and can either block it or redirect its final destination. Deep packet inspection is regarded as a sophisticated way to examine and manage network traffic.

content. If these companies do not comply, they face fines, or even loss of their licenses (Khalil, 2020, p. 10).

China operates the world's largest surveillance network, which consists of more than 200 million closed-circuit television (CCTV) cameras in public spaces across the country. The vast amounts of data that are collected on Chinese citizens, include among others, online communications, travel and health data, as well as facial scans and biometric data (Khalil, 2020, pp. 10-11). The collected data is contextualized and synthesized by AI algorithms in order not only to monitor citizens, but also to predict behavior. This omnipresent and fully networked surveillance system is operationalized by two major monitoring systems, 'SkyNet' and 'Sharp Eyes' (Polyakova & Meserole, 2019, p. 4, Wang, 2020). The former is a police video system that collects data from surveillance cameras placed in all public transportations, shopping malls, theaters and public places that jointly empower real-time monitoring. 'SkyNet' is promoted by the Chinese governments as a crime control mechanism, but in reality, assisted by crowd analysis and AI, it functions as a mechanism of state control. 'Sharp Eyes' is a broader surveillance system, since it links cameras that are installed in smartphones, vehicles, televisions and other smart appliances with public surveillance cameras. Practically 'Sharp Eyes' has adjusted to the Internet of Things (IoT) and thereby strengthens the monitoring capabilities of the surveillance state (Khalil, 2020, p. 11).

The surveillance toolkit does not only include smart cameras, but also portable facial-recognition glasses, voice-recognition software that trace phone call and drones that resemble birds to avoid suspicion (Lilkov 2020, p. 27). Adding to all the above, the CCP also use high-tech censorship systems and social media platforms like Weibo and WeChat to increase its ideological propaganda. The toolkit includes censoring information, distorting facts, and constructing favorable to the regime narratives. Many social media accounts are directly set up by the government and use deceptive digital tools,

such as bot and trolls (Wang 2020). A dystopian example of China's surveillance state can be found in the Xinjiang province, where the Muslim minority of Uighurs is heavily monitored and controlled. At the click of a mouse, available data from numerous surveillance cameras is retrieved and contextualized in order to identify citizens that pose a threat to 'national security' or 'social trust'. In many cases, non-violent online activities are deemed as harmful and thus citizens attend indoctrination camps, where they are 'transformed' into secular citizens that do not challenge the CCP and social harmony (Leibold, 2020).

It is fair to argue that China has institutionalized a sophisticated mass surveillance system that exploits digital technology to exercise massive societal control and prevent political rebellion. The Chinese model of digital authoritarianism encapsulated the CCP's philosophy on Internet governance, techno-nationalism and societal management and control. The latter is a rather Orwellian development that expands the state's control over its citizens, but has also broader implications, outside China.

2. Social Credit Systems: A digital dystopia under construction

Since 2014, the CCP has been gradually developing a national social credit system that promotes trustworthy behavior, to shape a harmonious society. Despite what media reports have frequently stated in the recent past, the social credit system is not yet fully operational and citizens in China have not been assigned a national score yet. Contrary to popular imagination, a single and all-powerful numerical score for every Chinese citizen, is still missing (Matsakis, 2019). So far, the CCP has not been able to construct a gigantic database that integrates all the available information from its various sources, governmental agencies and private companies. Due to technological constraints and lack of coordination between all the different parts of this enterprise, the implementation of the social credit system is still under construction. There are 47 institutions engaged in the system, among them the State Council, the National De-

velopment and Reform Commission, the People's Bank of China and several ministries and security agencies. Adding to that, there is growing number of laws and regulations that relate to social credit like the Foreign Investment Law, the Vaccine Administration Law and the Biosecurity Law. As a result of the plethora of regulations and bureaucracies that are involved in the social credit ecosystem, a central and integrated data-sharing structure is still absent (Drinhausen, K. & Brussee, 2021, p. 6).

Nevertheless, there are social credit systems that are run by local governments and the private sector, along with those employed by the central government. The National Credit Information Sharing Platform serves as a repository of all social credit systems' data (Khalil, 2020, pp. 8-9). The rationale behind these systems is to offer incentives and disincentives to steer social behavior. These systems rate, reward and punish citizens and businesses based on the morality of their social actions. Violators are named and shamed and eventually blacklisted. The social credit system also publishes a red list to reward compliant behavior (Khalil, 2020, p. 9, Drinhausen, K. & Brussee, 2021, p. 10).

In 2016, a memorandum of understanding was issued, where public institutions and government agencies, clarified their respective roles in enforcing these punishments/rewards. This memorandum is known as the Joint Punishment System. Based on this punishment system citizens and businesses can be blacklisted, limiting their access to services and resources. The punishments/rewards involve limited/privileged access to education, travel, housing employment, hospitals and internet access (Lilkov, 2020, p.38). In the private sector, the penalties include restricted access to government subsidies and loans, limited opportunities to make investments, issue bonds or purchase property. Likewise, at the individual level, citizens are not allowed to leave the country, buy airplane and railway tickets and make economic investments (Lilkov, 2020, p.39).

As stated above, China have strengthened its surveillance apparatus, to ensure social order and stability and build a harmonious society. China has already devel-

oped a sophisticated social credit system that ranks citizens' online and offline behaviour (Botsman 2017, Kobie 2019). This Orwellian sounding control system, ranks citizens' and businesses' behaviors, based on their online social interactions. Online purchases and posts are ranked to restrict access to jobs, travel, and credit (Deibert 2019, p. 35). IT companies, even western technological giants like Apple and Google, operating in China must comply with China's regulations, which requires them to allow governmental authorities to surveil their networks, sensor private chats and public posts and extract data (Deibert, 2019, p. 35). China's Cybersecurity Law that was passed in 2017, requires access to foreign companies' data and extends data localization to all critical information infrastructure.

Apart from the domestic implications of the social credit system, projects like China's DSR and Huawei's 'Safe Cities' are developments that disseminate authoritarian norms and advance state control at the expense of civil liberties (Polyakova & Meserole, 2019). The Chinese model of digital surveillance is spreading well beyond China's borders.

3. Exporting authoritarianism via the Digital Silk Road project

The DSR project aims to strengthen digital connectivity in the participating countries, with China as the key player of this process. This digital infrastructure project includes among others terrestrial and underwater data cables, 5G cellular networks, data storage centers, surveillance networks and the launch of global satellite navigation systems (Recorded Future, 2021 p. 4). But the DSR is far more than just a digital infrastructure project, it is part of a broader strategy that encapsulates Beijing's views on techno-nationalism, cyber sovereignty and its ambition to shape a more Sino-centric - and less American-centric global (digital) order (Ghiasy & Krishnamurthy, 2021). The later can be achieved by opening new markets for Chinese tech giants like Alibaba, Tencent and Huawei and by fostering the digital connectivity of the developing countries with China – or rather their

digital dependence from China. The DSR is in line with the 'Made in China 2025', which aims to enhance China's domestic tech innovation and thereby ensure greater autonomy in the digital technology sector.

By building the digital backbone of many developing countries, China is gaining in many ways, far from the economic one. The global economy is largely data driven. Therefore, the one who controls the data flows will also control the economy. By controlling data, Chinese companies can understand how the market works, identify local and international competitors and conduct commercial research and development (Kadi 2020). By dominating these new markets and by limiting the ability of local or Western companies to gain a share of the market, China is making these countries dependent on any future software or hardware that is critical to their national digital infrastructure and thereby security. Adding to the above, taking for granted China's habit to conduct espionage, it will be a great surprise if Beijing is not tempted to collected covert intelligence via these means (Lilkov, 2020, p. 49). China's digital colonialism is a direct threat to democracy and human rights. Nevertheless, it is worth questioning whether a more digitalized world would benefit China in the long term. In many of the developing countries, if digitalization is accompanied by economic growth and a certain degree of liberalization of the market, this would offer investment opportunities for non-Chinese companies too.

China has constructed data centres in North Africa, Egypt, and Algeria, as well as underground and underwater fibre-optic cables in Pakistan, Vietnam, Indonesia and the Philippines (Kadi, 2019, Harding, 2019, Lilkov, 2020, p. 49). One of the areas that China has exported aggressively over the last years is that of surveillance technology (Feldstein, 2019, p. 8). Bearing in mind that China is nowadays an economic giant who also succeeded in keeping if not expanding its authoritarian characteristics, it is no wonder that states with similar characteristics turned to Beijing for assistance. A quick survey demonstrates that over the past years China has marketed and transferred surveillance technology to countries like Vietnam, Pakistan, Uzbekistan, the United

Arab Emirates, Ecuador, Venezuela, Bolivia, Angola, Ethiopia, Nigeria, Zambia, Kenya and Zimbabwe (Freedom House 2018, Lilkov 2020). As of January 2021, forty-one African countries have agreed to join China's BRI. Thirteen of them have acquired surveillance capabilities and nine of them - Botswana, Côte d'Ivoire, Ghana, Kenya, Mauritius, Morocco, South Africa, Uganda, and Zambia - are implementing 'safe city' systems produced by Huawei (Recorded Future, 2021, p. 7). The latter is China's tech champion, or otherwise a trojan horse to enter and dominate foreign markets.[4] Huawei has signed a 'smart city' contract with Kenya, a cloud data center contract with Pakistan, a 4G high-speed wireless internet contract with Canada and a 5G high-speed wireless internet contract with Thailand. Huawei has also launched a Cloud and AI Innovation Lab in Singapore and is building Latin America's largest public Wi-Fi network in Mexico (Freedom House, 2018, p. 8, Recorded Future, 2021, p. 4). Huawei is not only providing advanced equipment but also offering ongoing technological support to set up, operate, and manage these systems.

China does not only offer the necessary technology to censor and steer public opinion, but also advices authoritarian regimes on how to develop the necessary data and privacy protection legislation, utilize the available data and steer its relations with the media regarding information management (Freedom House, 2018, p. 8). Apart from providing tailored seminars to government officials and media elites, China is accessing overseas data and fostering alliances with like-minded states, in relation to global internet governance (Recorder Future, 2020, p.4). We should bear in mind that such alliances are important in international organizations and fora like the UN, the International Telecommunications Union (ITU) and regional ones like the Shanghai Cooperation Organization (SCO) and the Association of Southeast Asian Nations (ASEAN), where China promotes a multilateral model of cyberspace governance.

[4] The other Chinese tech giants, although with a smaller share of the global market on 5G technology and smartphones include ZTE and Hikvision.

China's intense marketing of surveillance technologies is not simply filling a gap in the global market. The transfer of surveillance technologies, accompanied by legal advice and media-training courses, will not be limited to fight home-grown terrorism and domestic criminal activities in the developing countries. Rather this toolkit will also be used, or mainly be used to suppress political opposition and limit the rise of democracy in these countries (Crosston 2020, p. 165). The byproduct of the DSR is the spillover of unauthorized surveillance, the suppression of universal human rights and the collapse of democratic standards. The international community must urgently recognize these developments and develop a comprehensive strategy to deter the rise of digital authoritarianism (Lilkov, 2020, p. 50-51). Keeping in mind that China will host a mega-security event, the 2022 Winter Olympics, Beijing will be in the spotlight. It will be critical to see, whether the CCP will succeed in displaying the effectiveness of its domestic surveillance program, or whether the global media will broadcast the suppression of protests and human-rights activists.

4. Conclusions

The digitalization of the economy in China during the 2000s, gradually led to the digitalization of the authoritarian state. In the hands of the CCP, digital technology has become a powerful and oppressive tool for surveillance and control of the society. By establishing a comprehensive system that monitors behavior, the government is 'objectively' measuring trustworthiness. Points are gained and lost based on the citizen's social behavior, resulting to a score that determines the citizen's level of access to resources and privileges. But these digital surveillance technologies are not limited inside China. On the contrary, they consists a tool of China's grand strategy. China has achieved to increase its influence by entering new markets in Asia, the Middle East, Africa and Latin America and export surveillance technology. Many of the countries that receive Chinese digital surveillance products, are human-rights violators and would

otherwise be unable to access such technology. Chinese technology enables these repressive regimes to exercise population control, surveillance and censorship and thereby expand the authoritarian rule around the globe. Since Beijing dominates the construction and management of telecommunications and data centers in these countries, it gains access to data and capabilities that will enable it to conduct influence operations in these societies and as a result draw them closer to China and away from the US and the West.

Chinese digital authoritarianism is a reality and obviously an ominous one. As China aspires to become a global leader, it will weaponize its digital authoritarianism toolkit, to control the developing countries. This entails the danger that digital authoritarianism will become the new normal, with obvious implications to global democracy, freedom and internet governance. Uninstalling this digital dystopia is not easy task and demands coordinated efforts by states, tech companies and civil society.

Literature:

1. *Botsman, R. (2017). Big data meets big brother as China moves to rate its citizens. Wired, available at https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion*
2. *Creemers, R. (2020). China's Approach to Cyber Sovereignty. Konrad-Adenauer-Stiftung, available at https://www.kas.de/en/single-title/-/content/china-s-approach-to-cyber-sovereignty*
3. *Crosston, M. (2020). Cyber Colonization: The dangerous fusion of artificial intelligence and authoritarian regimes. Cyber, Intelligence, and Security, 4(1). 149-171.*
4. *Deibert, R. (2019). The Road to Digital Unfreedom: Three Painful Truths about Social Media. Journal of Democracy, 30 (1), 25-39.*

5. *Drinhausen, K. & Brussee, V. (2021). China's Social Credit System in 2021. From fragmentation towards integration. MERICS China Monitor, available at https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration*
6. *Feldstein, S. (2019). The Global Expansion of AI Surveillance. Garnegie Endowment for International Peace, available at https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847*
7. *Freedom House, (2018). Freedom on the Net. The Rise of Digital Authoritarianism, available at https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism*
8. *Ghiasy, R. & Krishnamurthy, R. (2021). China's Digital Silk Road and the Global Digital Order. The Diplomat, available at https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/*
9. *Griffiths, J. (2020). The Great Firewall of China: How to build and control an alternative version of the Internet. Bloomsbury Publishing.*
10. *Harding, B. (2019). China's Digital Silk Road and Southeast Asia. Center for Strategic and International Studies, available at https://www.csis.org/analysis/chinas-digital-silk-road-and-southeast-asia*
11. *Ingster, N. (2016). China's Cyber Power. The International Institute of Strategic Studies, Adelphi Series, 456.*
12. *Ito, A. (2019). Digital China: A Fourth Industrial Revolution with Chinese Characteristics. Asia-Pacific Review, 26(2). 50-75.*

13. *Kadi, E. (2019). The Promise and Peril of the Digital Silk Road. Chatham House, The Royal Institute of International Affairs, available at https://www.chathamhouse.org/2019/06/promise-and-peril-digital-silk-road*
14. *Kamasa, J. (2020). Internet Freedom in Retreat. CSS Analyses in Security Policy, no.273, available at https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse273-EN.pdf*
15. *Keremoğlu, E. & Weidmann, N. (2020). How Dictators Control the Internet: A Review Essay. Comparative Political Studies, 53 (10-11). 1690-1703.*
16. *Khalil, L. (2020). Digital Authoritarianism, China and COVID. Lowy Institute Analysis, available at https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid*
17. *Kobie, N. (2019). The Complicated Truth about China's Social Credit System. Wired, available at https://www.wired.co.uk/article/china-social-credit-system-explained*
18. *Leibold, J. (2020). Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement. Journal of Contemporary China, 29(121). 46-60.*
19. *Liaropoulos, A. (2013). The Challenges of Social Media Intelligence for the Intelligence Community. Journal of Mediterranean and Balkan Intelligence, 1(1). 5-14.*
20. *Liaropoulos, A. (2016). Reconceptualizing Cybersecurity: Safeguarding Human Rights in the Era of Cyber Surveillance. International Journal of Cyber Warfare and Terrorism, 6(2). 33-41.*

21. *Lilkov, D. (2020). Made in China. Tackling Digital Authoritarianism. Wilfried Martens Centre for European Studies, available at https://www.martenscentre.eu/publication/made-in-china-tackling-digital-authoritarianism/*
22. *Matsakis, L. (2019). How the West Got China's Social Credit System Wrong. Wired, available at https://www.wired.com/story/china-social-credit-score-system/*
23. *Morozov, E. (2011). The Net Delusion. The Dark Side of Internet Freedom. New York: Public Affairs.*
24. *Polyakova, A. & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. Brookings Institution, available at https://www.brookings.edu/research/exporting-digital-authoritarianism/*
25. *Recorded Future, (2021). China's Digital Colonialism: Espionage and Repression Along the Digital Silk Road. Cyber Threat Analysis China, available at https://www.recordedfuture.com/china-digital-colonialism-espionage-silk-road/*
26. *Sinkkonen, E. & Lassila, J. (2020). Digital Authoritarianism in China and Russia. FIIA Briefing Paper, no.294.*
27. *Wang, D. (2020). China's Digital Authoritarianism. Medium, available at https://medium.com/swlh/chinas-digital-authoritarianism-beccfa8daab0*