USING AND EXPORTING DIGITAL AUTHORITARIANISM: CHALLENGING BOTH CYBERSPACE AND DEMOCRACIES

Claudiu Mihai CODREANU, PhD Student
National University of Political Studies and Public Administration
Bucharest/Romania

Abstract
Over the last two decades, views regarding cyberspace and the usage of digital means by governments shifted from hopes of cyber-utopias to fears of cyber-dystopias, fuelled by increasingly heavy limitations imposed on Internet freedoms and online privacy rights worldwide, a tightening grip of authoritarian regimes on cyberspace, disinformation campaigns, censorship, internet shutdowns, digitally-enabled mass surveillance both online and offline and so on. Thus, the discussion will be centred on Russia's and China's usage and export of digital authoritarianism, while also considering steps taken by liberal democracies to counter such actions, focusing on the role of the US and of the EU and its member-states. This paper will start with a literature review regarding digital authoritarianism and an exploration of how Russia and China are using and exporting it. States such as Russia and China are using digital means to bolster and expand their authoritarian regimes, while also exporting digital authoritarianism to other like-minded governments around the world, creating an unignorable challenge for liberal democracies and civil society groups everywhere. Finally, the paper will also address potential courses of action and policies that liberal democracies and international organisations can take for countering digital authoritarianism. For instance, they should promote an alternative model for digital governance and governance through digital means, starting by promoting digital liberties and privacy rights instead of trying to limit them for national security purposes (e.g., the case of encryption).

Thus, liberal democracies should respond to digital authoritarianism by further bolstering democracy.

Keywords
China; cyberspace; democracy; digital authoritarianism; Russia.

1. INTRODUCTION

The Internet, cyberspace and digital tools were firstly seen as means to enhance democracy and unite people all over the world, from marginalised people from democratic states to people living in autocracies. Cyber tools have been rather successfully used by social movements and protest movements in the 2000s and the early 2010s, as online messaging services and social media platforms facilitated the organisation and spread of the protests part of the Arab Spring or the Moldovan protests of 2009 (Feldstein 2019). However, the Internet and new digital tools proved to be double-edged swords, as the tide turned in favour of autocrats, who started exploiting digital tools in order to keep themselves in power and to reassert or maintain control over the people (Pytlak 2020). Thus, from the point of being used by citizens to uncover human rights abuses or to circumvent censorship, now digital tools are increasingly used by authoritarian governments to curtail human rights and consolidate public surveillance and censorship actions. Together with the growing trend of autocratization all over the world, democratic governments, civil society and academia need to closely study and monitor digital authoritarianism and to find ways of countering it and develop a democratic alternative to internet governance.

Therefore, in this paper I shall discuss explore the current state of digital authoritarianism around the world, focusing on the Chinese and Russian models, and also on their export of digital authoritarian technologies and practices to other like-minded countries. Russia and China export digital authoritarian models, practices and technologies to authoritarian states, and even to illiberal and electoral democracies (Polyakova and Meserole 2019; Yayboke and Brannen 2020). However, the research will also look into some

examples of digital authoritarian practices used by liberal and electoral democracies in Europe and the United States. The US, United Kingdom and European Union member-states have their own digital authoritarian practices, albeit far less stringent and impactful than their Chinese and Russian counterparts. Western companies also export digital authoritarian tools to authoritarian states (e.g., Saudi Arabia) (Allen and La Lime 2021; Council on Foreign Relations 2022). In the end, the study of digital authoritarianism will be followed by a series of recommendations for countering digital authoritarian models and practices, as democracies need to find an alternative model of internet and technology governance in order to counter authoritarian models promoted by China or Russia. In order to do this, I shall consult relevant academic literature on this topic, as research looking into these areas is consistent and constantly developing. Moreover, the study will focus more on the digital authoritarian models for China and Russia and their efforts to export them abroad and less on controversial actions of liberal democracies in cyberspace.

2. DIGITAL AUTHORITARIANISM, CYBERSPACE AND THE GLOBAL TREND OF AUTOCRATIZATION

2.1. Digital authoritarianism – models, tools and practices

New developments in digital technologies allow authoritarian and illiberal governments tools to easily monitor and track opponents, while also keeping down dissent or protests. Technological advances provide such regimes both a wider set of tools to quell dissent and also a reduction in the cost of repression. Thus, authoritarian governments use technological means to abuse human rights and protect their regime. (Dragu and Lupu 2021, 992-996)

Instead of enabling activists and civil society to organise and bypass authoritarian controls in countries around the world, new technologies and digital tools have actually contributed more to allow governments to consolidate their authoritarian rule and control and enact widespread surveillance. Initially,

ICTs (Information and Communications Technology) and social media platforms (including messaging services) were used by citizens and civil society groups to organise and promote anti-government protests and keep leaders, authoritarian or not, in check (e.g. the cases of the Arab Spring and the Moldovan protests of 2009). However, such events were followed by various measures implemented by authorities to gain stricter control over the internet and social media. (Feldstein 2019; Pytlak 2020, 66-67)

According to Freedom House (2021), the main countries rated as 'not free' regarding their internet controls are China, Russia, Iran, Cuba, Venezuela, Ethiopia, Belarus, Kazakhstan, Myanmar, Saudi Arabia, Thailand, Turkey, United Arab Emirates, Uzbekistan, Vietnam. The US, UK, EU, Japan, South Korea, Taiwan and Australia are part of the bloc of states that promote digital freedoms internationally, China, Iran, Russia and Saudi Arabia are part of the states that promote digital authoritarianism and a strict internet governance, whilst other countries such as Brazil, India and Indonesia are in the middle (Deibert 2015, 70; Knake 2020, 2). Furthermore, global internet freedom declined for the eleventh consecutive year in 2021, and Freedom House highlighted in 2018 that digital authoritarianism had been already on the rise around the world (Shahbaz 2018; Freedom House 2021, 1).

Digital authoritarianism is defined by Polyakova and Meserole (2019, 1) as the use of digital technology by authoritarian regimes to "surveil, repress, and manipulate domestic and foreign populations". Digital authoritarianism, or tech-enabled authoritarianism, represents the use of technology by authoritarian governments to control and shape the behaviour of its citizens, using surveillance, censorship, manipulation and repression, in order to retain and expand control and power (Khalil 2020, 6). It is also defined by Yayboke and Brannen (2020, 2) as the usage of the Internet and digital technologies by governments (especially authoritarian ones) to increase social and political control and undermine civil liberties, curtailing the rights to privacy, freedom of speech or freedom of movement.

Digital authoritarianism is consolidating in authoritarian states such as China, Russia, Iran and Saudi Arabia, but digital authoritarians are also exporting their models and tools to like-minded regimes. Moreover, tools and practices of

digital authoritarianism are also being used inside democratic countries, either by political parties or private companies (Yayboke and Brannen 2020, 2). The main threats for citizens emerging from authoritarian and illiberal practices in cyberspace are arbitrary surveillance, restricting the freedom of expression and the prevalence of secrecy and disinformation (Glasius and Michaelsen 2018, 3796). Digital tools and the internet can be used to disrupt both democracies and dictatorships (Shahbaz 2018).

In addition to this, an increasing number of states are using advanced artificial intelligence technology for surveillance tools in order to efficiently monitor and track their citizens, and a significant part of these states use such tools to curtail human rights, even if others may use it lawfully. In 2019, more than 40% of the world's countries were using AI technologies for surveillance tools. More than 50% of liberal democracies use AI surveillance systems, from facial recognition cameras to safe city platforms, but this does not imply that they are also abusing the systems. Furthermore, almost half of competitive autocratic states and illiberal democracies use AI surveillance technology and more than a third of closed authoritarian states, and these types of regimes are the most prone to abuse the systems. (Feldstein 2019, 1-2)

Another tool of digital authoritarians is implementing partial or total internet shutdowns, with the former entailing only the blocking of specific websites or social media platforms. Such measures were used over the years in various countries all around the world, including Russia, Iran, Myanmar or Venezuela. For instance, Cuba's internet shutdown during the 2021 anti-government protests lasted several days and it involved blocking access to communication and social media platforms such as Facebook or WhatsApp. (Newman 2021)

Ron Deibert (2015) differentiates between three generations of information and internet controls and digital authoritarianism. First-generation controls are measures taken to raise borders in the global cyberspace and restrict citizens' access to information from other countries, the most eloquent example being the Great Firewall of China (a system for filtering web information and URLs to control all internet traffic accessed from the country). The efficiency and stringency of the Great Firewall was more or less matched by few countries (e.g. Iran, Pakistan, Saudi Arabia and Vietnam), but Internet filtering became

widespread in most countries, even though in liberal democracies it was used mainly against websites perceived or accused to offer illegal content (e.g. digital piracy). According to Deibert, second-generation controls refer to a consolidation of information controls through laws and regulations and a stricter approach to private tech companies and network operators, including the requirement of providing backdoors to software and comply to surveillance and censorship requests. Furthermore, third-generation controls involve targeted espionage, surveillance and disruptions in cyberspace (e.g., cyberattacks, cyber espionage), their main element being that this kind of controls are offensive in nature, and not only defensive such as the first two. Consequently, in the 2010s a fourth generation emerged, as digital authoritarians adopted a more assertive position at the international level, promoting such measures worldwide. (Deibert 2015, 65-70)

2.2. Cyberspace – less open and less global

Cyberspace is a "complex socio-technical system", consisting of interactions between humans and technology and interaction between humans facilitated by technology (Dunn Cavelty and Wenger 2022, 2). Consequently, cybersecurity is a "multifaceted set of practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access" (Balzacq and Dunn Cavelty 2016, 183), encompassing policies, strategies and actions to protect networks, infrastructure and cyberspace. Despite the rise of various non-state actors, from cybersecurity firms, big tech companies to hacking groups and so on, the state still maintains a central and key role in cyberspace, both as the owner of networks and as the main actor that must address and solve issues of cybersecurity (Dunn Cavelty and Egloff 2019, 48).

Cyberspace, starting as a Western and Western-centric medium and set of technologies, is now more non-western than ever. Non-western countries and tech companies are becoming some of the most important players in cyberspace, especially Asian companies. Moreover, the majority of internet users are from Asian countries, taking into account China's or India's large populations.

Furthermore, China seems to be taking a leading role in the development and implementation of new technological advances, such as 5G and artificial intelligence. (Barrinha and Renard 2020, 756)

2.3. A new wave of autocratization is undergoing

According to the V-Dem Institute (2022), the global level of democracy in 2021 reached 1989 levels, before the democratic revolutions in Central and Eastern Europe. Now, authoritarian regimes are increasing and encompass a total of 70% of the world population and closed autocracies now number 30 countries with 26% of the world population, whilst the most common regime type is electoral autocracy (44% of the world population). Furthermore, 2021 set a negative record for the last 50 years as 33 countries are autocratizing and 20% of EU member-states are autocratizing. (V-Dem Institute 2022)

V-Dem Institute (2022) differentiates between four different types of regimes: liberal democracies (full democracy), electoral democracies (hybrid regime tilting toward democracy), electoral autocracies (hybrid regime tilting toward authoritarian) and closed autocracies (full authoritarian). Most of China and Russia's recipients of digital authoritarian tools and models are closed autocracies and electoral autocracies, even though a number of electoral democracies import such tools (such as Ecuador).

The main type of authoritarian regime in the current world is the competitive authoritarian regime (or electoral autocracy), in which formal democratic institutions exist, but incumbents of power abuse and manipulate them against the opposition in order to maintain their rule. The regime is competitive because opposition parties exist and use democratic institutions to contest for power, but the competition is unfair and heavily balanced in favour of the incumbents. Furthermore, elections are held regularly and the opposition can organise and participate, even though it has little chance of actually winning. However, regimes where there are no real channels for opposition to contest legally for power are taken into account as full authoritarian regimes. Full authoritarian regimes include closed regimes where democratic institutions do not exist, such

as China, Cuba or Saudi Arabia and regimes where democratic instructions exist only formally and as a façade. (Levitsky and Way 2010, 5-7)

Moreover, illiberal regimes are characterised by the implementation of institutional reforms that reduce that reduce the protection of minority and human rights, judicial independence, media independence and civil society. Furthermore, illiberal regimes are reasserting national sovereignty against multilateral instructions (e.g., against the EU). The main efforts of illiberal regimes have the goals to restrain judicial oversight, curtail political opposition, weaken independent media and demonize civil society groups. The main European examples of illiberal regimes over the last years are Hungary, Poland, Turkey and Serbia, but other European countries have experienced illiberal trends or inclinations, such as Czechia, Slovakia or Romania. (Polyakova et al. 2019, 5-7)

Conversely, liberal democracy's main feature is the strive to secure individual freedom and protect society from the threat of majority tyranny, as they are governed by laws, hence the crucial role of the rule of law principle, ensuring that the government can also be held accountable (Hague and Harrop 2004, 39). Furthermore, according to Robert A. Dahl (1998, 37-38), there are five standards for a governing regime to be taken into account as democratic: effective participation, voting equality, enlightened understanding, control of the agenda and inclusion of all adults.

3. TWO MAIN USERS AND EXPORTERS OF DIGITAL AUTHORITARIANISM: CHINA AND RUSSIA

3.1. The Chinese model of digital authoritarianism – unescapable surveillance, censorship, big data, personal data and AI

China is regarded by Freedom House as the worst abuser of internet freedom, whilst its government is supplying technology and software for facial recognition and data analytics tools to like-minded countries that have poor human rights records. China promotes and spreads its digital authoritarianism

over the world through providing trainings and seminars for governments, exporting tools for AI surveillance and building and installing telecom infrastructure (Shahbaz 2018). Furthermore, the emergency situation created by the COVID-19 pandemic allowed China to boast their use of digital tools to track and monitor their citizens, and also to expand the use of digital authoritarian means, using the need of preventing the spread of COVID-19 as a pretext (Khalil 2020, 14).

Moreover, China's government-hackers intensified their cyber espionage operations after the Ministry of State Security gained a leading role in 2015. For instance, in 2021, the US, UK, EU, NATO and Japan accused Chinese government agencies of a series of significant and disruptive hacking campaigns, compromising thousands of public and private organisations around the world by exploiting a vulnerability in Microsoft's Exchange Server software (Greenberg 2021).

Since the enactment of the 2016 cybersecurity law, the Chinese government legally requires companies to facilitate data access and state control, such as increasing surveillance of their networks or censoring content and reducing online anonymity by requiring users to provide their real names for registration (Qiang 2019, 55). China's largest tech companies work alongside the country's government and intelligence agencies (Wang 2021). In this context, China's internet traffic filtering system, the Great Firewall, blocks over 1.300 websites, including Google, Youtube, Facebook, Twitter or Wikipedia, while also heavily limiting the possibility of using virtual private networks (VPN) by individual users (Qiang 2019, 56).

China's video-surveillance network is the largest in the world, numbering more than 200 million cameras, many of them equipped with AI technologies for facial recognition, and Chinese tech companies Hikvision and Dahua control more than 40 percent of the global market of surveillance cameras. Moreover, the government also makes use of voice-recognition software and even DNA databases, comprised mostly with DNA samples from individuals with criminal convictions, alongside dissidents and members of the Uyghur ethnic community or migrant workers. Besides video surveillance and data collection, China is also

implementing the Social Credit System. (Qiang 2019, 56-59; Polyakova and Meserole 2019, 5; Khalil 2020, 10; Kovachich and Kolesnikov 2021)
China's law enforcement agencies collect a massive amount of data about people in order to monitor them. The Chinese government collects large amounts of data from its citizens, including online communication, health and education records, travel logs and biometric data. The data is then stored and analysed by AI systems. These actions are the most noticeable in the Xinjiang province, home to over 13 million Turkic Muslims (the Uyghurs). In Xinjiang, Chinese authorities use mandatory mobile apps, artificial intelligence, big data and even biometric collection to control the people of the Muslim minority. Uyghurs are frequently required by law-enforcement to have their DNA collected, eyes scanned and to install spyware apps on their phones to track all of their digital activity. In addition to this, video-surveillance has gone so ubiquitous in Xinjiang that authorities even use surveillance drones to cover areas that cannot be reached by cameras. (Wang 2021; Polyakova and Meserole 2019, 5; Khalil 2020, 10)

3.2. Chinese export of digital authoritarianism – all over the world, but mostly in Africa, South Asia and Latin America

In 2015, China launched the Digital Silk Road, as part of the Belt and Road Initiative. Agreements and memorandums of understanding were signed with dozens of countries from Africa, South Asia, Latin America, Middle East or Eastern Europe, especially developing countries that need high-quality and inexpensive technology for expanding internet and wireless infrastructure. However, there are also some developed countries that signed agreements, such as South Korea, Hungary, Poland, Czechia, Estonia or the UK. Other states that participate in the Digital Silk Road are Pakistan, Myanmar, Kazakhstan, Turkey, Serbia, Ethiopia, Venezuela, Cuba, Peru, Ecuador or Zimbabwe. Nevertheless, China may use the Digital Silk Road to export its model of digital authoritarianism, even though this is not the main aim of the initiative. (Council on Foreign Relations 2022)

At the international level, besides the Shanghai Cooperation Organisation or UN discussions, Beijing is also promoting its digital authoritarian model and practices at an international level through annual meetings of the World Internet Conference held in Wuzhen, China. The conference brings together leaders of large tech companies (including Facebook, Amazon, Google, Apple, Alibaba and Tencent), members of research communities and world leaders, promoting both Internet sovereignty ideas and the Chinese tech industry. (McKune and Ahmed 2018, 3845)

China's model of Internet sovereignty, where the state delimits and controls cyberspace within its borders, is inspiring illiberal and authoritarian governments around the world. Chinese technology is functional, affordable and offers similar features or levels of quality as its Western counterparts (Wang 2021). Chinese companies such as Alibaba, TikTok, or Tencent's WeChat have gone global and the first two are widely used all over the world, while WeChat is mainly used by the Chinese diaspora (Wang 2021). In addition to this, China's Huawei and ZTE are the largest companies in the telecommunications sector worldwide and Tencent is a dominant social media platform and an increasingly large video game publisher (Knake 2020, 19). Some of the tech companies are owned directly by the Chinese state, but others are private companies heavily controlled by the authorities (Wang 2021). China exported surveillance technologies (especially camera systems, facial-recognition software and AI tools) to over 18 countries, such as Malaysia, Singapore, Ethiopia, Zimbabwe, Angola, UAE, Ecuador and Venezuela (Polyakova and Meserole 2019, 6). In addition to this, over 80 countries, most of them from Africa, Asia and Latin America, adopted Huawei's safe city systems and other tools of surveillance technology supplied by Chinese-based companies (Khalil 2020, 26).

For instance, China's Huawei signed partnerships with Serbia to expand internet infrastructure and cooperate on smart cities projects, alongside opening a data storage site in the country. In addition to this, Huawei will also install surveillance cameras around the country, including in Belgrade, whilst Serbian opposition accused the government that the technology was used to monitor anti-government protests. Consequently, even though the EU remained the largest donor in Serbia, Chinese investment there is strengthening authoritarian

rule in the country in the face of reforms required for EU funding. (Council on Foreign Relations 2022; Brandt and Taussig 2019, 142)

Furthermore, China is a major supplier and driver of AI surveillance technologies, as Chinese companies such as Huawei, Hikvision, Dahua and ZTE supply AI tools for surveillance purposes in more than 60 countries (Huawei supplies such tools to over 50 countries). However, AI surveillance technology is also supplied from companies based in liberal democracies. The largest non-Chinese supplier of AI tools for surveillance is Japan-based NEC Corporation, supplying to over 14 countries. Furthermore, US-based companies (e.g. IBM, Palantir, Cisco) supply AI surveillance technology to over 32 countries, and there are also some firms in this sector in France, Germany and Israel. Most of the world's countries that use AI surveillance tools us a mix of Chinese and US technology, including Russia, Germany, France, Spain, Romania, Turkey, China or US. However, according to 2019 data, several countries rely only on Chinese technology, such as Serbia, Italy, Argentina, Chile, Venezuela or the Netherlands, for instance. (Feldstein 2019, 2-3)

3.3. The Russian model of digital authoritarianism – surveillance, web filtering, censorship and legal threats

Russia's digital authoritarianism is less stringent than China's, one of the main dissimilarities being that Russian internet had originally developed in line with the Western model. Moscow started adopting a more authoritarian approach to internet governance especially after the 2011-2012 protests. The Russian model of digital authoritarianism stands as a lower-tech and less-expensive alternative to the Chinese one. The Russian model is characterised by highly restrictive laws on public expression and speech, state capture and corporate capture of ISPs (internet service providers), state manipulation of the market and internet filtering. The Russian model of Internet filtering is less draconian from a technical point of view, but similar when it comes to intimidation, fear of prosecution or fines and self-censorship. However, Russia constructed its own technology for internet surveillance, known as SORM (System for Operative

Investigative Activities), or the SORM network, storing and intercepting all Internet traffic inside the country, which is analysed or investigated by the Federal Security Service (FSB). (Morgus 2019, 89-91; Kerr 2018, 3821; Polyakova and Meserole 2019, 8; Kovachich and Kolesnikov 2021)

For digital surveillance, Russia relies on both Chinese and Western technologies, and Russia is actually a receiver of China's export of digital authoritarian tools and policies, their strong partnership in this regard starting as early as 2015. However, Moscow's digital infrastructure for its smart city surveillance system was provided by Western tech companies such as Cisco, Dell or HP. (Kirilova 2021; Kovachich and Kolesnikov 2021). Moscow and Beijing view their dependence on US or European technology as a significant vulnerability, but Moscow will encounter serious difficulties to replace Western technology in critical areas, especially compared to China's ability to do so (Kovachich and Kolesnikov 2021).

Russia and China also have different perceptions and strategies towards Europe and the EU. Russia views European democracy, security and prosperity as threats to its authoritarian regime, and so it makes efforts to undermine them and to destabilize countries. In contrast, China prefers a stable Europe with which it can freely trade, but a divided Europe that would trade on Beijing's terms. However, both countries have used information operations (including disinformation campaigns) and cyber operations (including cyberattacks and cyber espionage) against European states (Brandt and Taussig 2019, 133-140).

Moreover, Russia uses its own technology in sensitive areas for defence and national security, leaving out both Western and Chinese providers. For instance, Russia was far from eager to use Chinese equipment for the construction of Russian 5G infrastructure, opting for using only Russian telecommunications companies' equipment, the main concern being that Chinese telecoms companies might leave backdoors into Russian networks which Beijing could use for spying. (Kovachich and Kolesnikov 2021)

Nevertheless, international sanctions imposed against Russia by the US, UK or EU after Russia's renewed invasion of Ukraine in 2022 will hamper Russia's plans in this area, as sanctions against technology companies and export bans of US technology will weaken Russia's digital authoritarianism and it will likely

make it more dependent on Chinese technology (Rappeport 2022). As a result, Russian telecom companies were cut off from acquiring new equipment and services from Cisco, Nokia or Ericsson and even Taiwan, home to the world's largest maker of semiconductors, halted deliveries (Satariano and Hopkins 2022).

Furthermore, after the renewed Russian invasion of Ukraine started on 24 February 2022, Russia started to cut itself from the global or Western internet, whilst US or European companies began suspending their operations in Russia. Western tech companies such as Apple, Samsung, Microsoft, Oracle or Cisco fully or partially pulled back from Russia, Netflix and Spotify suspended their services and Twitter, Facebook, Instagram and Youtube or partially or fully blocked. In addition to this online isolation, Russia strongly tightened the control of the internet and significantly increased the level of online censorship, especially regarding events or information regarding its war against Ukraine. (Satariano and Hopkins 2022)

However, international backlash caused by Russia's war against Ukraine and the need to quell domestic dissent against the invasion were only incentives to intensify ongoing processes of tightening control over cyberspace. In 2021, the Kremlin was already backing laws for expanding online censorship and also allowing Russian intelligence services to break encryption of online messages and even to require companies and software developers to provide law enforcement agencies full access to encrypted information (Kirilova 2021). Furthermore, similar to China's Great Firewall, Russia was also testing its Runet, a closed 'sovereign' internet that would cut off traffic from other states, helped by China's providing of know-how in this area (Knake 2020, 4).

3.4. Russian export of digital authoritarianism – cheaper and low-tech alternative to the Chinese model

The Russian model of digital authoritarianism is mainly appealing to countries from the area of the former Soviet Union, mainly because most of them have similar legal frameworks to Russia. Thus, Russia predominantly exports digital

authoritarian tools in its near abroad, exporting SORM-like systems to Belarus, Kazakhstan, Kyrgyzstan and Uzbekistan through two Russian companies, Protei and Peter-Service. However, the two companies also have clients in other parts of the world, such as the Middle East and North Africa (Bahrain, Iraq, Qatar, Tunisia or Yemen) and Latin America (Cuba, Mexico and Venezuela). Russia's model of digital authoritarianism offers a low-tech and low-cost alternative to the Chinese model. Even though the main receivers of Russian digital authoritarian tools have been countries of Russia's near abroad (former Soviet states), its technology has also been exported to the global south. (Morgus 2019, 92-95; Kerr 2018, 3821-3823; Polyakova and Meserole 2019, 7-8)

Moreover, the Collective Security Treaty Organisation (CSTO) and the Shanghai Cooperation Organisation (SCO) are used by Russia (and China, in the case of SCO) to facilitate regional coordination and internationally promote digital authoritarianism and a unified approach to control of the Internet and of information. (Kerr 2018, 3825; McKune and Ahmed 2018, 3845)

China and Russia are also promoting their views and models of internet governance and digital authoritarianism at the level of the UN (Knake 2020, 5).

4. DIGITAL AUTHORITARIAN PRACTICES IN DEMOCRACIES AND DEMOCRATIC ALTERNATIVES TO DIGITAL AUTHORITARIANISM

4.1. Digital authoritarian practices in the US, UK and EU member-states

Mass surveillance is not a practice specific to authoritarian states such as China or Russia, as large US or Western tech companies have adopted a surveillance-based business model, gathering people's data in exchange for free services. Moreover, the US, UK, Australia, Canada and New Zealand, part of the Five Eyes intelligence coalition, is seeking to undermine encryption by pressuring software developers and companies to provide governments backdoor access to encrypted communications. For instance, government ministers of the Five Eyes alliance called on companies to provide backdoors to encrypted content,

otherwise intelligence agencies could make attempts to break their systems of encryption. (Wang 2021; Shahbaz 2018)

Intelligence services exploit vulnerabilities and security gaps in common operating systems and software, ensuring much-needed backdoors inside networks that can enable access for deploying disruptive actions, surveillance or espionage. However, vulnerabilities found or directly created by intelligence services in software and networks reduce the level of security for everyone, as the backdoors can be exploited by other state and non-state actors for malicious purposes. Thus, no matter the purpose of the government that created or exploited security gaps in parts of cyberspace, such actions affect the security of every user, including the state which created the vulnerabilities. Nevertheless, intelligence services are making cyberspace more insecure directly and indirectly, in order to gain access to more data, even if the purpose may be preparing for potential conflicts. (Dunn Cavelty and Egloff 2019, 47; Dunn Cavelty 2014, 710)

Furthermore, there was also the recent case of the Pegasus spyware scandal, uncovered by human rights groups and media. The Pegasus spyware, a type of malicious software (malware) used to spy individuals or organisations online, was uncovered by an investigation done by several organisations, such as Amnesty International, and published by a consortium of media organisations. The spyware was developed by the NSO Group, an Israeli-based surveillance company, and according to a data leak published in 2021, it was used to target human rights activists, journalists, business executives, academics, government officials (including presidents and prime ministers) and opposition politicians by authoritarian and illiberal government around the world. The malware, which the Israeli company said its scope was to be used against terrorists or criminals, infects mobile devices (running either Google's Android or Apple's iOS operating systems), allowing the extraction of messages, email and photos, whilst it can also be used to activate microphones or record calls. At least 10 governments used NSO tools, including Azerbaijan, Kazakhstan, Mexico, Morocco, Saudi Arabia, Hungary or India, targeting individuals from over 45 countries, including France, Spain, the UK or Turkey. (Kirchgaessner et al. 2021)

Furthermore, more than a dozen world leaders were targeted using Pegasus and the majority of them were government officials of African states, including the presidents of South Africa and Morocco and prime-ministers of Egypt or Algeria. However, Israeli-based NSO Group is not the only major player in the industry of digital surveillance in Africa, where China's Huawei has a great role and even Western companies such as French-based firm Amesys, UK-based Gamma Group or Italy-based group Hacking Team. Nonetheless, Western tech companies also exported their services for surveillance or espionage, including US-based Gatekeeper Systems, which sold facial recognition technologies to Saudi Arabia and other authoritarian states. (Allen and La Lime 2021; Council on Foreign Relations 2022)

In addition to this, even EU member-states used the spyware. Hungary's government used Israeli-made Pegasus spyware against independent journalists and opposition politicians, and the same spyware was also used by Poland (Walker 2021; Chapman 2022). This shows that threats do not come exclusively from Chinese or Russian technology, as even digital tools created and exported from democracies can be used maliciously or in an authoritarian way. Thus, the export of digital authoritarianism can be regarded as more about the spread and implementation of a model and not exclusively of technology or software.

Other instances of illiberal or authoritarian practices in cyberspace used by or inside democracies are the cases of Cambridge Analytica (which emphasised the dangers of exploiting big data for political goals) and the leaks and claims made public by American whistleblower Edward Snowden regarding the US intelligence agency NSA (National Security Agency), which highlighted the sometimes negative role played by intelligence agencies in cyberspace (Glasius and Michaelsen 2018, 3806-3808). Thus, the governments' and companies' collection and usage of big data for various political or market purposes can be characterised as a form of capitalist accumulation, which Shoshana Zuboff described as 'surveillance capitalism' (2015, 75).

4.2. Democracies' search for a democratic model of internet governance – EU's model of digital sovereignty focused on privacy

The European Union's model of internet governance represents a 'third way' between China's model of digital authoritarianism and US's model of unrestricted free markets and freedom of speech (Freedom House 2021, 15). EU's model of technological sovereignty entails preserving European autonomy and leadership in crucial technological sectors in order to avoid dependencies (Csernatoni 2021). For the EU, the notion of digital sovereignty mainly refers to the need of protecting users' privacy and personal data. Digital sovereignty entails that the EU should build a strong, innovative and secure technology sector, preserving the EU and its member states to keep a central role in cyberspace and still be regulators and legislators, or 'rule-makers' (Burwell and Propp 2020, 5-6). Accordingly, in its 2020 cybersecurity strategy, the European Union sets the goal of working with international partners to promote globally a model of cyberspace based on the respect of human rights, democratic values, fundamental freedoms and the rule of law, keeping cyberspace global, secure, stable and open (European Commission 2020, 19).

EU institutions are working on promoting or preserving Europe's role in key areas such as cybersecurity, quantum technology or artificial intelligence. For instance, in October 2020 the European Union enacted regulation on screening foreign direct investments, after fears of security threats stemming from foreign states providing 5G equipment through state-controlled companies (such as China and Huawei), an action that could enable interference of foreign states inside EU networks and communications. Thus, the European Commission has called on member states to exclude high-risk vendors from sensitive or critical parts of their 5G networks, including core networks that manage data traffic. In addition to this, the European Union is also targeting practices of large US-based tech companies with its focus on protecting user privacy and requirements for moderating online content. (Csernatoni 2021; Burwell and Propp 2020, 3-7; Knake 2020, 1)

Furthermore, EU's General Data Protection Regulation (GDPR), implemented during 2018, can become a good practices example for privacy regulations

worldwide, especially in democracies. GDPR sets forth significant mechanisms through which citizens gain rights over their online data. Another significant aspect of the regulation is that GDPR is extraterritorial, and so it applies to any business or country holding data of European citizens at a global level. (Knake 2020, 4)

4.3. Countering digital authoritarianism by promoting a model of techno-democracy

Digital authoritarian practices are spreading in both autocracies and democracies, along with the global trend of autocratization. China and Russia are solidifying their domestic digital authoritarian rule, whilst also exporting digital authoritarian models, practices and technologies to authoritarian states, and even to illiberal and electoral democracies (Polyakova and Meserole 2019). However, China's model and digital tools are spreading faster and farther than Russia's, along with the rapid increase of its tech industry. Furthermore, as autocratization trends all over the world (V-Dem Institute 2022), even in Europe, democracies need to concentrate their efforts to counter digital authoritarianism, including their own practices. 'Softer' digital authoritarian practices in democracies can be used as justifications for their own digital authoritarian models, even though surveillance is not exclusively an abuse of digital technologies.

Thus, there is a serious need of developing an alternative, democratic model of internet governance and approach to cyberspace and digital technologies that should counter digital authoritarianism. A democratic model of internet governance should firstly protect both offline and online freedoms, freedom of speech and the right to privacy. Consequently, democracies should implement measures and regulations that promote the internet's egalitarian nature and emancipatory potential, protecting the freedom of expression online, sharing information across borders and holding leadership to account (Freedom House 2021, 1). Democracies should promote and defend internet freedom, digital rights and human rights and also enact and enforce significant data privacy

legislation (Freedom House 2021, 25-27). In addition to this, they should ensure that measures implemented to protect cybersecurity and national security maintain and do not restrict internet freedom and human rights, offering digital authoritarian models a democratic alternative (Yayboke and Brannen 2020, 8).

Another important aspect of a democratic alternative to digital authoritarianism is respecting and promoting the right to encryption (both of communications and personal data) and also increasing the amount of encrypted data in cyberspace. Moreover, governments and intelligence agencies should work on finding an alternative to the idea of using pre-installed backdoors in software or networks. Freedom of speech and the right to privacy, including the right to data and communication encryption should be seen as beneficial to cybersecurity, as less encrypted data could lead to reduced cyber espionage and cybercrime (Dunn Cavelty 2014, 711). Thus, democracies should protect and promote the protection data and communications encryption, focusing on the protection of digital rights everywhere in the world (Freedom House 2021, 25; Yayboke and Brannen 2020, 8). Moreover, liberal democracies should make efforts to ensure the security of cyberspace, and this also means that governments must limit some actions of their intelligence agencies, such as efforts to create and exploit vulnerabilities and security gaps in software and networks (Dunn Cavelty 2014, 711).

In order to contain the spread and usage of digital authoritarianism, a coalition of democracies should work together to impose sanctions against states that use digital authoritarianism, that export it and on companies that export such tools, especially if they export them to authoritarian countries, so countries that will abuse them and use them to curtail human rights. Furthermore, democracies should promote a global and open cyberspace, transparency, clear laws and regulations which should also prevent abuses of digital tools, monitor and regulate the extensive collection and use of personal data and of surveillance tools. The US, UK, EU and other democracies (e.g., Japan, Australia) should sanction regimes using and exporting digital authoritarianism and companies that supply such tools, tighten export controls on technologies related to this sector, whilst making efforts to develop a democratic model of digital governance as an alternative to digital authoritarianism (Polyakova and

Meserole 2019, 11). Liberal democracies should also tighten import and export controls and impose sanctions on tech companies that enable human rights abuses (Shahbaz 2018; Knake 2020, 14). Sanctions should be applied not only to Russian or Chinese companies that supply digital authoritarian tools, but also to companies based in the US, Europe, Israel or elsewhere that provide and sell surveillance technologies to authoritarian regimes (Polyakova and Meserole 2019, 11).

In addition to this, democracies should also regulate the usage of surveillance systems and the collection of personal data and information by government agencies, whilst also restricting the export of such technologies to abusers of digital tools and authoritarian regimes (Freedom House 2021, 25). The US must first work on reforming its own surveillance and data-gathering practices (countered even by allies such as the EU) and on protecting its citizens' online privacy in order to showcase an alternative model to digital authoritarianism, a model that should protect privacy, promote civic participation and meet human rights standards (Wang 2021). At the same time, the United States and its allies should make efforts to establish and promote global standards for countries and tech companies that respect human rights and internet freedoms (Wang 2021).

Finally, these efforts should also include raising public awareness and aiding citizens of digital authoritarian countries, as for instance democratic governments, civil society networks and/or private companies could work on facilitating Internet and information access to people living in autocracies (e.g., promoting and enabling the use of virtual private networks, encrypted and safe communications or developing digital tools to protect online privacy).

5. CONCLUSIONS

As new technologies continue to be developed and as more and more people, businesses and public institutions are dependent on digital tools and the Internet, digital authoritarianism will only get more powerful and will only spread even farther and further if left unchecked. Even though China and Russia are the main abusers of digital technologies and the main exporters of

digital authoritarian tools, similar practices are increasingly common in democracies, even though democracies are more transparent in their actions and citizens can hold leadership accountable for abuses (Wang 2021; Shahbaz 2018). However, if liberal and electoral democracies continue to adopt domestic or imported models of digital authoritarianism, the threshold for what counts as abuses of digital tools will lower significantly for digital authoritarians, at the cost of consolidating autocracies around the world and contributing to the curtailing of human rights. Digital authoritarians threaten democracies by exporting their practices and also by getting into an offensive, using cyberattacks and information operations against democracies in order to weaken their rule (Deibert 2015; Brandt and Taussig 2019), all the more reason to accelerate the development of an alternative. Furthermore, the new challenges spurred by the ongoing pandemic period were exploited by governments to embolden and condone various digital authoritarian practices in both democracies and autocracies, such as individual tracking, increased surveillance or information control (Khalil 2020).

Thus, democracies should strive to both keep their own actions in cyberspace in check and scrutinise the actions of digital authoritarians, even by promoting models of democratic governance of the internet or by sanctioning states and private companies that engage in the usage and export of digital authoritarianism. Furthermore, the United States, United Kingdom and the European Union should lead the way of promoting an alternative model to digital authoritarianism, or even alternative models, such as EU's idea of 'digital sovereignty'.

REFERENCES

- Allen, Nathaniel, and Matthew La Lime. 2021. "How digital espionage tools exacerbate authoritarianism across Africa". *Brookings*, November 19. Accessed April 20, 2022. https://www.brookings.edu/techstream/how-digital-espionage-tools-exacerbate-authoritarianism-across-africa/

- Balzacq, Thierry and Myriam Dunn Cavelty. 2016. "A theory of actor-network for cyber-security". *European Journal of International Security* 1, no. 2: 176-198.
- Barrinha, André, and Thomas Renard. 2020. "Power and diplomacy in the post-liberal cyberspace". *International Affairs* 96, no. 3: 749-766.
- Brandt, Jessica, and Torrey Taussig. 2019. "Europe's Authoritarian Challenge". *The Washington Quarterly* 42, no. 4: 133-153.
- Burwell, Frances G., and Kenneth Propp. 2020. "The European Union and the Search for Digital Sovereignty". *Atlantic Council*, June 2020. Accessed April 20, 2022. https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf.
- Chapman, Annabelle. 2021. "Poland's Pegasus Gate: Digital Authoritarianism in the EU?". *CEPA*, January 20. Accessed April 20, 2022. https://cepa.org/polands-pegasus-gate-digital-authoritarianism-in-the-eu/.
- Council on Foreign Relations. 2021. "Assessing China's Digital Silk Road Initiative". Accessed April 20, 2022. https://www.cfr.org/china-digital-silk-road/.
- Csernatoni, Raluca. 2021. "The EU's Rise as a Defense Technological Power: From Strategic Autonomy to Technological Sovereignty". *Carnegie Europe*, August 12. Accessed April 20, 2022. https://carnegieeurope.eu/2021/08/11/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134.
- Dahl, Robert A. 1998. *On Democracy*. New Haven & London: Yale University Press.
- Deibert, Ron. 2015. "Cyberspace Under Siege". *Journal of Democracy* 25, no. 3: 64-78.
- Dragu, Tiberiu, and Yonatan Lupu. 2021. "Digital authoritarianism and the future of human rights". *International Organization* 75, no. 4: 991-1017.

- Dunn Cavelty, Myriam, and Andreas Wenger. 2022. *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation"*. London and New York: Routledge.
- Dunn Cavelty, Myriam, and Florian J. Egloff. 2019. "The politics of cybersecurity: Balancing different roles of the state". *St. Antony's International Review* 15, no. 1: 37-57.
- Dunn Cavelty, Myriam. 2014. "Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities". *Science and engineering ethics* 20, no. 3: 701-715.
- European Commission. 2020. "The EU's Cybersecurity Strategy for the Digital Decade". Joint Communication to the European Parliament and the Council. Brussels, 16.12.2020. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.
- Feldstein, Steven. 2019. "The Global Expansion of AI Surveillance". *Carnegie*, September 2019. Accessed April 20, 2022. https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.
- Feldstein, Steven. 2020. "Digital Democracy Struggles". *Carnegie*, September 9. Accessed April 20, 2022. https://carnegieendowment.org/2020/09/09/digital-democracy-struggles-pub-82532.
- Freedom House. 2021. "Freedom on the Net 2021: The Global Drive to Control Big Tech". *Freedom House*. https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech.
- Freedom House. 2021b. "Key Internet Controls 2021". Accessed April 20, 2022. https://freedomhouse.org/report/freedom-net/2021/key-internet-controls.
- Glasius, Marlies, and Marcus Michaelsen. 2018. "Illiberal and Authoritarian Practices in the Digital Sphere – Prologue". *International Journal of Communication* 12: 3795-3813.

- Greenberg, Andy. 2021. "How China's Hacking Entered a Reckless New Phase". *Wired*, July 18. Accessed April 20, 2022. https://www.wired.com/story/china-hacking-reckless-new-phase/.
- Hague, Rod, and Martin Harrop. 2004. *Comparative politics and government: an introduction*. New York: Palgrave Macmillan.
- Kerr, Jaclyn A. 2018. "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region". *International Journal of Communication* 12: 3814-3834.
- Khalil, Lydia. 2020. "Digital Authoritarianism, China and COVID". *Lowy Institute*, November 2. Accessed April 20, 2022. https://www.lowyinstitute.org/sites/default/files/Khalil%2C%20Digital%20Authoritarianism%2C%20China%20and%20Covid_web_print_021120.pdf.
- Kirchgaessner, Stephanie, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani, and Michael Safi. 2021. "Revealed: leak uncovers global abuse of cyber-surveillance weapon". *The Guardian*, July 18. Accessed April 20, 2022. https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus.
- Kirilova, Kseniya. 2021. "Russian Authorities Seek Total Control Over Internet". *Jamestown*, September 15. Accessed April 20, 2022. https://jamestown.org/program/russian-authorities-seek-total-control-over-internet/.
- Knake, Robert K. 2020. "Weaponizing Digital Trade: Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity". *Council on Foreign Relations*, September 2020. Accessed April 20, 2022. https://cdn.cfr.org/sites/default/files/report_pdf/weaponizing-digital-trade_csr_combined_final.pdf.
- Kovachich, Leonid, and Andrei Kolesnikov. 2021. "Digital Authoritarianism With Russian Characteristics?". *Carnegie*, April 21. Accessed April 20, 2022. https://carnegiemoscow.org/2021/04/21/digital-authoritarianism-with-russian-characteristics-pub-84346.
- Levitsky, Steven, and Lucan A. Way. 2010. *Competitive authoritarianism: Hybrid regimes after the cold war*. New York: Cambridge University Press.

- McKune, Sarah, and Shazeda Ahmed. 2018. "The contestation and shaping of cyber norms through China's internet sovereignty agenda". *International Journal of Communication* 12: 3835-3855.
- Morgus, Robert. 2019. "The Spread of Russia's Digital Authoritarianism". In *Artificial Intelligence, China, Russia, and the Global Order*, ed. Nicholas D. Wright, 89-97. Maxwell: Air University Press.
- Newman, Lily Hay. 2021. "Cuba's Social Media Blackout Reflects an Alarming New Normal". *Wired*, July 13. Accessed April 20, 2022. https://www.wired.com/story/cuba-social-media-blackout/.
- Polyakova, Alina, and Chris Meserole. 2019. "Exporting digital authoritarianism: The Russian and Chinese models". *Brookings*, August 2019. Accessed April 20, 2022. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.
- Polyakova, Alina, Torrey Taussig, Ted Reinert, Kemal Kirişci, Amanda Sloat, James Kirchick, Melissa Hooper, Normand Eisen, and Andrew Kenealy. 2019. "The anatomy of illiberal states: assessing and responding to democratic decline in Turkey and Central Europe". *Brookings*, February 2019. Accessed April 20, 2022. https://www.brookings.edu/wp-content/uploads/2019/02/illiberal-states-web.pdf.
- Pytlak, Allison. 2020. "In search of human rights in multilateral cybersecurity dialogues". In *Routledge Handbook of International Cybersecurity*, ed. Eneken Tikk and Mika Kerttunen, 65-78. London and New York: Routledge.
- Qiang, Xiao. 2019. "The road to digital unfreedom: President Xi's surveillance state". *Journal of Democracy* 30, no. 1: 53-67.
- Rappeport, Alan. 2022. "The U.S. imposes sanctions on Russian technology companies and evasion networks". *The New York Times*, March 31. Accessed April 20, 2022. https://www.nytimes.com/2022/03/31/world/europe/us-sanctions-russia.html.
- Satariano, Adam, and Valerie Hopkins. 2022. "Russia, Blocked From the Global Internet, Plunges Into Digital Isolation". *The New York Times*, March 7. Accessed April 20, 2022.

https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html.

- Shahbaz, Adrian. 2018. "Freedom on the Net 2018: The Rise of Digital Authoritarianism". *Freedom House*. Accessed April 20, 2022. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.
- V-Dem Institute. 2022. "Democracy Report 2022: Autocratization Changing Nature?". Accessed April 20, 2022. https://v-dem.net/media/publications/dr_2022.pdf.
- Walker, Shaun. 2021. "Viktor Orbán using NSO spyware in assault on media, data suggests". *The Guardian*, July 18. Accessed April 20, 2022. https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests.
- Wang, Maya. 2021. "China's Techno-Authoritarianism Has Gone Global". *Foreign Affairs*, April 8. Accessed April 20, 2022. https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritarianism-has-gone-global.
- Yayboke, Erol, and Sam Brannen. 2020. "Promote and Build: A Strategic Approach to Digital Authoritarianism". *CSIS Briefs*, October 2020. https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism.
- Zuboff, Shoshana. 2015. "Big other: surveillance capitalism and the prospects of an information civilization". *Journal of Information Technology* 30, no. 1: 75-89.