



**FIGHTING FOR
DEMOCRACY**
IN THE ERA OF DIGITAL
AUTHORITARIANISM



Contents

GLOSSARY	4
<hr/>	
1. INTRODUCTION	8
<hr/>	
1.1. Understanding the essence of authoritarian regimes	9
1.2. Instruments of digital authoritarianism	11
<hr/>	
2. THE RISE OF SOCIAL MEDIA IN THE DIGITAL AGE	14
<hr/>	
3. AUTHORITARIAN REGIMES AND SOCIAL MEDIA	18
<hr/>	
4. METHODES AND TECHNIQUES	21
<hr/>	
4.1. Propaganda and disinformation	21
4.2. Surveillance	26
4.3. Censorship	27
4.4. Harassment, intimidation, discrediting	31
<hr/>	
5. IMPACT ON DEMOCRACY: REASONS FOR CONCERN	32
<hr/>	
5.1. Preserving democracy and democratic values	33
5.2. Protection of human rights and freedoms	33
5.3. Security	34
5.4. Information integrity	34
5.5. Social cohesion	34
<hr/>	
6. RESPONDING TO THE CHALLENGE	35
<hr/>	
7. CONCLUSION	39
<hr/>	
8. REFERENCES	41
<hr/>	

GLOSSARY

B **BOT NETWORKS** – interconnected network of automated, semi-automated, or manually controlled accounts that, through temporal and content coordination, disseminate specific information, narratives, disinformation, and propaganda.

C **CONFIRMATION BIAS** - tendency to seek, interpret, favor, and recall information confirming one's beliefs or hypotheses. People exhibit this bias when they selectively gather or present information in a biased manner or interpret it in a non-objective way. The effect is stronger for issues triggering emotional reactions and deeply ingrained beliefs.

COORDINATED INAUTHENTIC BEHAVIOR – activities and campaigns involving groups, accounts, and pages that coordinately seek to deceive people about who they are and what they do, relying on fake accounts. Facebook coined the term to describe the use of multiple accounts that work together to present a false image of themselves, artificially boost the popularity of content, or engage in behavior that violates community standards.

D **DEEPPFAKE** – a technology that uses artificial intelligence to create hyper-realistic fake videos, photos, and audio materials. It is often used to replace one person's face with another person's, creating convincing fake scenes.

DIGITAL AUTHORITARIANISM – the use of digital information technologies for the purpose of surveillance, repression, and manipulation of both domestic and foreign populations.

DISINFORMATION – a combination of true, partially true, and false content/information.

DOXXING – the process of gathering someone's personal data and information, and publicly disclosing it on the Internet without their consent, exposing the victim to discomfort, risks, and even potentially dangerous situations.

E ECHO CHAMBER – an environment in which participants encounter information that reinforces or confirms their preexisting beliefs through communication and repetition within a closed system, isolated from disapproving and opposing views.

.....

F FAKE NEWS – an original article/media report containing completely inaccurate information and content not based on facts.

.....

G GLOBAL VILLAGE – a term that describes the phenomenon of increasing interconnectedness of the world as a result of the spread and advancement of technology. The term was coined by Canadian media theorist Marshall McLuhan in 1962.

.....

I INFORMATION INFLUENCE OPERATIONS (IIO) – intentional and organized efforts to manipulate or influence public opinion, perceptions, beliefs, or behaviors. It involves the strategic and planned use of various communication channels to shape narratives, spread disinformation, undermine democratic processes within and outside of a country, promote specific political, economic, and ideological interests or agendas, and degrade the integrity of the information space.

.....

M MICROTARGETING – a form of online targeted advertising that analyzes personal data to identify the interests of specific audiences or individuals and influence their actions. Microtargeting can be used to deliver personalized messages to an individual or audience using online services such as social media.

.....

N NARRATIVE – the lens through which people perceive themselves and the world around them, connecting personal experiences with an understanding of how the world functions. The stronger the narrative, the more likely it is to be retained and remembered. The power of a narrative depends on several factors: coherence (how one event logically connects to another), simplicity (immediately understandable and spreadable), resonance, and adaptability.

S

SURVEILLANCE CAPITALISM – refers to the widespread collection and commercialization of personal data by corporations. This phenomenon is distinct from state surveillance, although the two can reinforce each other. Companies profit by collecting and analyzing data about consumers. These data are then used to create personalized advertisements or sold to other companies for the same purpose. This economic model is often associated with technology companies such as Google and Facebook. The issue of surveillance capitalism has raised concerns about privacy and the power these companies have to influence the behavior of individuals and society as a whole.

SOCIAL MEDIA ALGORITHMS – a set of computer rules and processes that determine which content is shown to users and in what order, based on various factors such as user behavior, interactions, and personal preferences. Its goal is to provide each user the most relevant and engaging content, encouraging interaction and time spent on the platform.


T

TROLLS – in the context of social media, it refers to individuals or accounts that intentionally provoke discord, controversy, or negative reactions by posting inflammatory, polarizing, or provocative content.

TROLL FARMS – an entity that conducts information influence operations on the Internet. These activities are often disguised under inconspicuous names, such as a public relations agency, internet research center, etc. Troll farm operations are typically focused on the political or economic sphere. The objectives of these operations may include, for example, attacking political opponents, supporting a specific candidate or option, or other related activities. Troll farms achieve their goals by utilizing, among other tactics, fake news, and hate speech.

U

USEFUL IDIOT – in political jargon, it refers to someone who supports an idea or propagates propaganda without being aware.



Global freedom faces a dire threat. Around the world, the enemies of liberal democracy—a form of self-government in which human rights are recognized and every individual is entitled to equal treatment under law—are accelerating their attacks.

Freedom House 2022 Report



1. Introduction

The institutionalized logic of liberal democracy, in which democratic governments and officials prioritize the voters' interests, has been increasingly challenged by the logic of authoritarianism for some time now. This entails centralized power that, under the guise of democracy, promotes sharp divisions based on religion or moral, geography or race, and ethnic identity. Emphasizing these differences justifies the authoritarianism of centralized authority, with the underlying premise that the political elite knows best how to protect the people and the state from all perceived threats.

The emergence of social media platforms at the beginning of the 21st century marked a global shift in how people communicate, exchange information and engage in political mobilization. However, while these platforms have the potential to support democratic processes, they also provide authoritarian regimes with new opportunities for control, manipulation, and repression. Consequently, the misuse of social media by authoritarian regimes has become an acute problem for democracies worldwide.

With the rise of digital technology, many people, drawing from the experience of the Arab Spring, believed that the Internet and social media could be a force for democratization, potentially undermining the power of authoritarian regimes. In countries with limited media freedom and freedom of expression, social media served as an alternative source of news and information, providing a counterbalance to state-controlled media and narratives.

However, despite technology's positive role in strengthening civil society and democratic values, the initial premise has proven somewhat utopian. The same tools that enable people to communicate, organize, and resist, and spread information about the abuses of their rights, are now being misused by governments that are at odds with democratic values and ideals.

The projection of strategic goals by authoritarian regimes through social media has become an increasingly common phenomenon, involving information control, censorship, disinformation, propaganda, citizen surveillance, mobilization of supporters, spread of ideology, and establishment of control mechanisms.

Tactics include spreading disinformation both domestically and beyond the country's geographical borders, monitoring citizens, harassing dissenters online, and manipulating public opinion. These activities have profound implications not only for the individual rights of citizens within these regimes but also for the integrity of democratic processes and institutions at a global level.

Algorithms regulating social media content can be manipulated to suppress or promote certain views, information, or disinformation. The public

availability of convincing deepfakes and other forms of online manipulations based on artificial intelligence further complicates the situation.

Understanding the misuse of social media by authoritarian regimes is crucial for protecting democratic integrity in the digital era, as the world becomes more of a global village, while internet freedoms are declining. At the same time, two-thirds of internet users worldwide live in countries where authorities punish citizens for expressing their personal views in the online space, and certain governments have started building their own digital space for easier control and surveillance, where state narratives dominate, and independent media and critics are marginalized.¹ In this regard, citizens, media, and decision-makers must be ready and capable of anticipating, recognizing, mitigating, and countering the phenomena imposed by digital authoritarianism, ensuring that social media serve as a tool for democratic empowerment rather than a weapon for authoritarian control, repression, manipulation, and surveillance.

This study aims to highlight the phenomenon of digital authoritarianism and the misuse of social media by authoritarian regimes, demonstrating the tactics they employ and how they impact democratic processes and institutions. The goal is to contribute to the development of awareness, strategies, and policies that can protect democratic and liberal values that Montenegrin society, at least declaratively, aspires to uphold.

1.1. Understanding the essence of authoritarian regimes

Authoritarian regimes are political systems in which power is centralized and maintained through political repression, extensive censorship, and limited political pluralism. In such a system, the ruling structures hold strong, and sometimes absolute power, often without the consent of the citizens and with little regard for public opinion or individual freedoms. This regime type is typically characterized by one leader or a small group of leaders who possess disproportionate political control. The power of individuals or groups is directly subordinate to the ruling system, creating the illusion of institutional functioning while fundamentally establishing a power pyramid consisting of loyalists with the clear task of preserving the authoritarian order or regime. The pretense of democracy becomes crucial for the survival of such a regime, so at a conceptual level, institutions in authoritarian regimes have a dual role - protecting the current social order and creating the illusion that they are independent.

Civil liberties are often limited in an authoritarian regime, and basic human rights are regularly violated. The regime maintains power through propaganda, mass surveillance, censorship, and the suppression of political opposition. Society is often characterized by restricted freedom of expression, the suppression of dissent, and limited media freedoms. Elections, if held at all, are usually not free and fair and are often manipulated to ensure the continuous dominance of the ruling group.

In the case of Russia, one such mechanism is control over the education system, including the revision of history and historical facts to find justification for current policies in history and historical events and to provide a foundation for present and future domestic plans and projections. One example of this historical revision is Putin's attitude towards Stalin, where there is a relativization of a period characterized by crimes, camps, and revenge.²

Economic elites often serve as a crucial link between authoritarian regimes and power consolidation models, as seen in the case of Russia, where oligarchs gained control over key natural resources following the collapse of the Soviet Union. In return, they leveraged their economic power to build infrastructure for regional loyalists.



Authoritarian regimes can arise for various reasons, such as economic instability, social unrest, or a perceived need for rapid modernization.

They can also come into power in cases of power vacuums, often resulting from coups, revolutions, or the collapse of previous political orders.

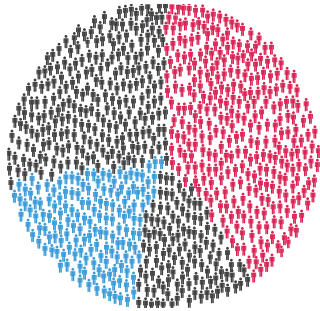
Some authoritarian regimes may show stability and efficiency, particularly in the short term, due to their ability to make quick decisions and implement policies without the delays inherent in democratic processes. However, these advantages often have a negative impact on human rights and freedoms.

On the domestic front, the primary fear of authoritarian regimes is a democratic change of power and power transition. To act preventively, hybrid regimes create internal hybrid threats, provoke artificial crises, manipulate the information space, and employ coercion to maintain internal power organization. They adopt a similar approach to external threats, perceiving democratic states and governments as the greatest danger and viewing the democratization process in neighboring countries as a threat to the survival of their own value system. Perhaps the most striking example is Russia's approach to Ukraine, undermining democracy, interfering in electoral processes, engaging in information and media operations, and exerting hybrid pressure to exploit weaknesses within democratic governments and democratic processes in those countries.

There is a broad spectrum of authoritarian regimes, ranging from absolute monarchies to military juntas and one-party states. Their specific characteristics can vary widely depending on cultural, historical, and geopolitical factors. Not all authoritarian regimes are entirely devoid of certain democratic elements. For example, some may organize elections, albeit with significant restrictions. Authoritarian regimes utilize the results of such unfree and undemocratic electoral processes as a basis for further undermining liberal values, all under the guise of a convincing electoral victory. An example of the erosion of democratic principles and liberal values can be seen in Hungary, where democratic standards are deteriorating, and the main justification for this is cited as the preservation of independence and protection of national interests.

According to the report by Freedom House, 38% of the world's population lives in not-free countries, the highest percentage since 1997. Only around 20% currently reside in free countries.³

Depending on the typology, authoritarian regimes create processes that superficially resemble those in free democracies, and one of these processes is the establishment of pseudo-opposition parties that serve as examples of vibrant democracy in the country, while essentially being a facade for internal use of power. The underlying process that always occurs in parallel with pseudo-democracy is the consolidation of long-term power, achieved through changes in legal or constitutional frameworks that allow for the longevity of the regime or ruler. The example of Vladimir Putin in Russia is striking. Through amendments to the constitution, the Russian president enabled himself to run for presidential elections twice, thereby creating conditions to remain in the position of the President of Russia until 2036. The role of the pseudo-opposition in such situations is clear, as the constitutional amendments were adopted unanimously. Genuine opposition in Russia, activists, and citizens, are intimidated and discouraged from any form of activism, access to media is denied to them, and often any form of action is sanctioned as internal extremism.



38%

THE WORLD'S
POPULATION LIVES IN
NOT-FREE COUNTRIES

20%

POPULATION THAT
CURRENTLY RESIDE IN
FREE COUNTRIES

*Freedom in the World 2022 Report
(Freedom House)*

After the invasion of Ukraine, the Russian Duma adopted a series of laws that characterize any opposition to the special military operation as treason, with the threat of imprisonment. The intentions of authoritarian regimes and their strategic plans are reflected in their treatment of genuine opposition leaders and activists within the country. Following the annexation of Crimea in 2014 and the building of support for expansionist plans, Boris Nemtsov, an opposition leader and activist from the PARNAS party, was assassinated in Moscow in 2015. Authoritarian regimes perceive any form of independent action as a threat to their rule and brutally suppress any form of political or civic disobedience at its roots.

1.2. Instruments of digital authoritarianism

The term digital authoritarianism has become prevalent in the scholarly literature addressing the misuse of digital information technologies by authoritarian regimes. It refers to the use of digital information technologies for the purpose of surveillance, repression, and manipulation of both domestic and foreign populations. The digital sphere provides new tools for maintaining power, including sophisticated surveillance systems, automated content control, and targeted disinformation campaigns. The rise of digital authoritarianism is also fueled by advancements in artificial intelligence, enabling more efficient and pervasive control than ever before.

Although these efforts take place in the digital space and are deeply interconnected, they are not limited to activities on social media alone. Digital authoritarianism utilizes all elements of the information space, including ownership of media and technological platforms, exerting pressure on business and advertising, and employing traditional censorship techniques. However, due to the scope of this material, the focus will be on the activities of authoritarian regimes conducted on social media platforms to achieve various strategic goals.

Regimes can monitor the activities of their citizens, especially those who are politically active or critical of the government, and use this information to suppress dissent and criticism. This can involve monitoring individuals' online activities and utilizing artificial intelligence to analyze posts on social media.

Moreover, these online platforms can be used to spread propaganda or disinformation, shape narratives, and create an atmosphere of fear. This can involve using fake identities on social media, automated bot accounts, and troll farms to amplify specific messages or narratives, creating and spreading fake news, or employing targeted advertising (microtargeting) to reach specific demographic groups with tailored messages.

Manipulation of public opinion on platforms takes various forms and has different names. Numerous terms have been used to describe various activities in the information space, such as hybrid warfare, psychological warfare, active measures, fake news, disinformation, propaganda, coordinated inauthentic behavior, and information/influence operations. While not synonymous, all these terms describe a range of interconnected malicious activities aimed at misleading or deceiving in the local or global information space.⁴

For the purposes of this study, we will use the term information influence operations (IIO). IIOs refer to deliberate and organized efforts to manipulate or influence public opinion, perceptions, beliefs, or behaviors of the audience. These operations typically involve the strategic and planned use of various communication channels to shape narratives, spread disinformation, undermine democratic processes within and beyond a country, promote specific political, economic, and ideological interests or agendas, and degrade the integrity of the information space.

Finally, digital authoritarianism on social media can also involve the punishment of dissenting individuals and groups. This can include online harassment, doxxing (publicly disclosing private information), and more severe measures such as arrests or violence.

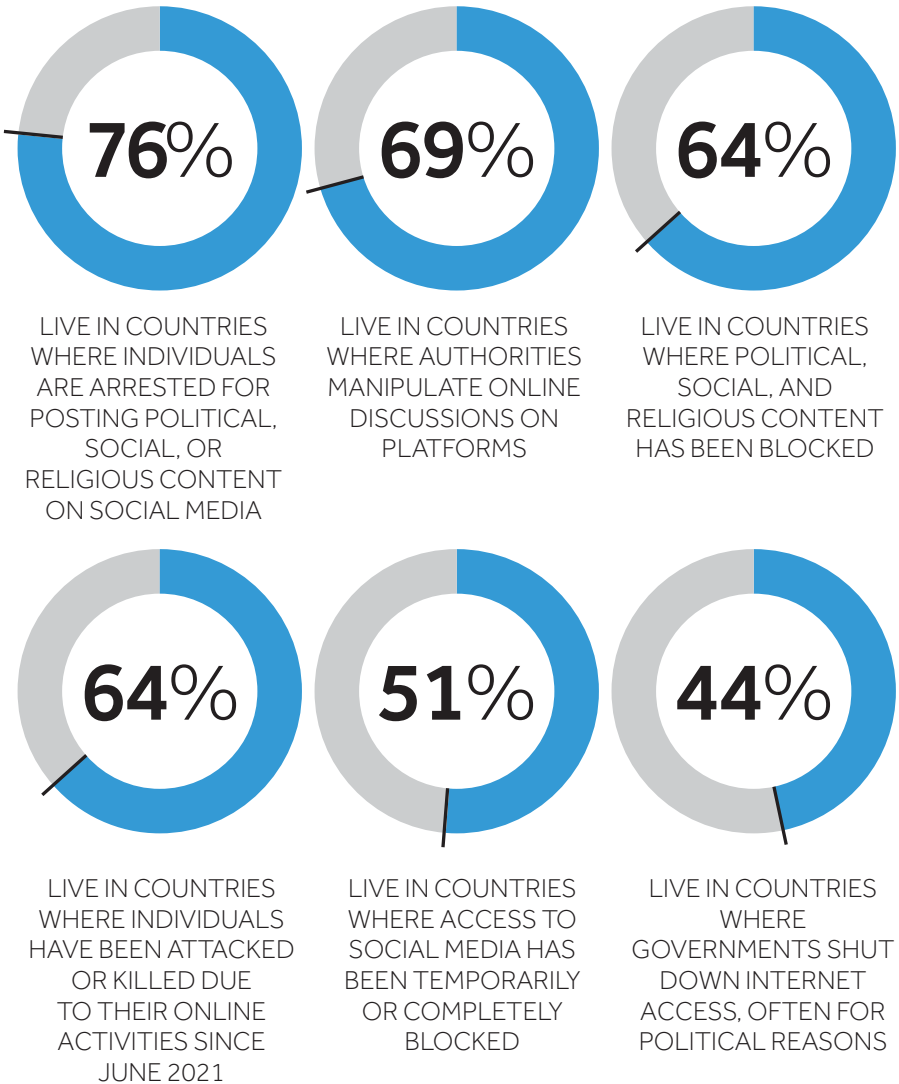
Certain governments strive to create an online space that can be controlled. According to the latest Freedom House report, a record number of national governments blocked websites with political, social, or religious content in 2022, undermining the right to freedom of expression and access to information. The majority of these blockings were targeted at websites hosted outside the respective countries.⁵

In that regard, certain national laws and solutions threaten the free flow of information through the centralization of technical infrastructure and the ap-

plication of repressive regulations on social media platforms and user data, enabling censorship and data filtration. Beijing's efforts to build and maintain the Great China Firewall⁶ have raised numerous concerns about privacy violations, cyber security, false propaganda content, and social media censorship. On the other hand, the Russian government has demonstrated particular proficiency in spreading propaganda and disinformation through the use of bot and troll networks. Authoritarian regimes also employ AI solutions to monitor their citizens, facilitating identification, tracking, and targeting of those who oppose them. The possibilities for utilizing new technologies for digital surveillance and censorship continue to develop.

Digital authoritarianism on social media is a cause for growing concern due to the pervasiveness and influence of social media in contemporary life, with platforms such as Facebook, Twitter, Instagram, and others playing a central role in shaping public opinion and facilitating public discourse.⁷

According to the Freedom House 2022 report⁸ over 4.5 billion people have access to the Internet. Among them:





2. The rise of social media in the digital age

The continuous growth of social media platforms in the last decade has made them an integral part of everyday life globally. Platforms like Facebook, Instagram, and Twitter are no longer solely used for entertainment and communication but play significant roles, among others, in information creation and dissemination, marketing, business networking, and political communication.

The COVID-19 pandemic has further accelerated the shift towards a more digital and mobile media and information environment, with potential far-reaching implications for journalism. However, according to research, traditional media in Montenegro and around the world still enjoy the highest level of trust among citizens and have managed to withstand the pervasive influence of social media.⁹

Facebook is a globally popular social network with the largest number of users. Still, there is a clear emigration trend, especially among Generation Z, to more visual platforms like Instagram and TikTok in the last three years. Telegram has also seen significant growth in some markets, providing a more flexible alternative to WhatsApp.¹⁰

The COVID-19 pandemic has further accelerated the shift towards a more digital and mobile media and information environment, with potential far-reaching implications for journalism. However, according to research, traditional media in Montenegro and around the world still enjoy the highest level of trust among citizens and have managed to withstand the pervasive influence of social media

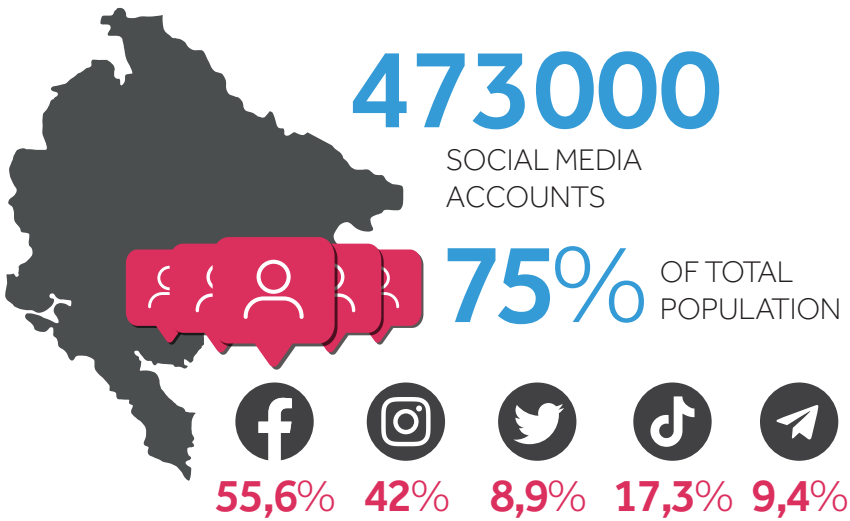
As of 2023, there are estimated to be around 4.76 billion social media users worldwide, which is 137 million more than the previous year. According to DataReportal data for 2023, 47% of users state that they primarily use social networks for communication, 36% for filling their free time, while every third user, 34% of them, uses social networks for informing and reading news.¹¹

In January 2023, there were approximately 473,000 social media accounts in Montenegro, equivalent to 75% of the total population. According to research, 55.6% of Montenegrin citizens have an account on Facebook, 42% on Instagram, 17.3% on TikTok, 9.4% on Telegram, and 8.9% on Twitter. Research¹² shows that the citizens of Montenegro have the highest level of trust in news

and information from traditional media, with 57.8% expressing trust in this source. On the other hand, 16.7% trust news and information obtained through social media, with Facebook and Instagram enjoying the highest level of trust as sources of information.¹³

In the business world, social media has become an essential tool for marketing and advertising. Companies use these platforms to interact directly with their customers, promote products and services, and gather consumer insights through various analytical tools. The rise of marketing services on these platforms is another evidence of the significant role of social media in shaping consumer behavior.

From a socio-political perspective, these platforms also play a significant role. They have been used to mobilize social movements, from the Arab Spring to the *Black lives matter* movement. These platforms have allowed citizens to express their views, gather support, and organize protests. At the same time, governments and other actors can also use them to spread disinformation, propaganda, manipulate public opinion, interfere in elections, and control the flow of information.



Furthermore, the algorithms of social media platforms reinforce confirmation bias while limiting exposure to diverse and opposing viewpoints, resulting in echo chambers that amplify existing ideas while restricting exposure to alternative perspectives. This can further polarize public opinion and political discourse and contribute to distrust in institutions and democratic processes.

In democratic countries, the use of social media in political processes has become commonplace. Politicians, parties, and activists use these platforms to connect with voters, share their views, and generate support. In Montenegro, since the end of 2020, there has been a proliferation in the use of Twitter by politicians and public figures, who use the platform for direct communication with the public, either through textual or audio formats, through popular threads or spaces.

Contrary to that, in many authoritarian regimes, social media platforms are heavily censored and controlled to suppress dissident voices and maintain power by ruling structures. For example, in China, the government has replaced Google and Facebook with domestic services like Baidu and WeChat, which Beijing can regulate information and cut off access to international platforms. In Russia, the legislation increases control over the Internet and online content, thus restricting the free flow of information.

Parallel to the rise of authoritarian practices on social networks, major technology platforms like Facebook monetize attention (attention economy)¹⁴ and increasingly gather data from individual users, a phenomenon referred to as surveillance capitalism¹⁵. in academic theory. Both models can have strong negative implications for individual privacy and create space for authoritarian practices. As Ronald Deibert summarized, attention-grabbing algorithms at the core of social media platforms encourage authoritarian practices that aim to spread confusion, ignorance, prejudice, and divisions, thereby facilitating manipulation and undermining democracy.¹⁶

Attention-grabbing algorithms at the core of social media platforms encourage authoritarian practices that aim to spread confusion, ignorance, prejudice, and divisions, thereby facilitating manipulation and undermining democracy

Ronald Deibert

Using algorithms to provide media and other services through online social platforms has direct implications for democratic processes. A healthy democracy is one in which citizens participate and make free decisions based on accurate information grounded in verified facts and reliable evidence. The role of social media as intermediaries between users and the media positions them as de facto media content providers. Given the frequent presence of unprofessional, false, and dangerous social media content, users become exposed and particularly vulnerable to online disinformation.



The research conducted by Cambridge and Stanford Universities, published in 2015 in the Proceedings of the National Academy of Sciences of the United States of America, indicated that Facebook's algorithm only needs 10 likes from a person to assess them better than a coworker, 70 likes to assess them better than a roommate, 150 likes to assess them better than their parents, siblings, or close relatives, and 300 likes to assess them better than their spouse.¹⁷

After the recent revelations by whistleblower Frances Haugen, it is clear that Facebook's sorting and news feed algorithm favored content that provokes anger, making it five times more visible than content that elicits happiness. The theory was simple: posts with a high number of Wow, Angry, Sad, and Haha reactions tended to keep users more engaged and present on the platform, and user engagement was key to Facebook's business. Thus, prioritizing controversial and polarizing posts opened the door to more undesirable

content, violating Facebook's terms of service. Internal company documents that leaked to the public in 2019 confirmed that posts that elicited any of the aforementioned emoticon reactions more often included disinformation, harmful news, and low-quality or questionable content. Despite the public significance of the issue, changing the algorithm was deemed impractical, as it would ultimately lead to less usage, fewer ad clicks, and consequently lower profits for the company.¹⁸

Furthermore, when considering the issue of transparency, the problematic nature of content personalization comes into play. When combined with user profiling and micro-targeting, it contributes to the creation of so-called filter bubbles. In these filter bubbles, people are exposed to an excessive amount of news or opinions that align with their existing beliefs. This further results in a hermetic closure of users within a circle of personalized information based on their interests and beliefs. In this way, exposure to alternative viewpoints is limited, creating what are commonly known as echo chambers.



*In the analysis titled **Social media and journalism in Montenegro conducted by the Media Self-Regulation Council (MMS) with the support of UNESCO and the EU**, it was found that neither journalists nor editors had a clear understanding of the significance and role of algorithms. Out of a total of 20 interviewees, the majority of them did not comprehend the functioning principles of social networks, nor were they able to access guidelines or instructions on how to use them effectively.*¹⁹

While authoritarian regimes can often be a source of information influence operations, the success of a disinformation campaign does not solely depend on them. There needs to be a demand for misleading or false information that aligns with the offered content. Therefore, the emotional, values-based, or ideological validation needs of individuals and groups are paired with social media algorithms, which are the most sophisticated information delivery systems that meet our preferences. Understanding the broader dynamics of disinformation spread in the digital environment requires recognizing the importance of these paired needs and algorithms.

Research shows that deeply polarized societies with low trust in traditional media may be more susceptible to the psychological drivers behind consuming disinformation and fake news in all geographical contexts.²⁰



3. Authoritarian regimes and social media

All governments, including democratic ones, tend to shape public opinion, although different regimes do so differently depending on the circumstances. Democratically elected governments resort to this during health or economic crises or in efforts to maintain public support for certain sensitive policies or issues. In contrast, authoritarian regimes regularly employ censorship, surveillance, and manipulation of public opinion across a wide range of issues, with the primary goal of staying in power. According to the Freedom House 2022 report, officials in at least 53 countries have accused, arrested, or detained internet users in response to critical posts on social media, while authorities in at least 22 countries have blocked access to social media and communication platforms.²¹

Social media platforms are often misused, and people are exposed to distorted information, most commonly without their knowledge. Examples of such practices range from global disinformation campaigns (e.g., about the coronavirus) led by countries like China and Russia.²² to Belarus where the government intensified arrests of bloggers, online activists, and other users in the context of Russian aggression in Ukraine, imposing prison sentences²³. These practices also extend to interference in the electoral processes of other countries.



*In recent years, there has been an increase in the availability of scientific and expert literature and reports that study and highlight the prevalence of information operations for political purposes. This includes the use of political bot networks to amplify hate speech or other forms of manipulated content, illegal data collection or micro-targeting, or the use of trolls to suppress political activism or press freedom.*²⁴

The Oxford Internet Institute's report on organized social media manipulation emphasizes not only the growing ability of authoritarian regimes to exploit the information space within their borders but also the emergence of several states capable of sophisticatedly employing information influence operations beyond their geographical boundaries. These states include China, India, Iran, Pakistan, Russia, Saudi Arabia, and Venezuela, with five of them

being classified as not free and two as partly free, according to the Freedom House 2023 report.²⁵

The story of institutionalizing modern and high-tech efforts to carry out information influence operations begins with Russia's long-term investments in nationalist youth camps, where teams were organized to direct disinformation campaigns toward Russian citizens using the popular Russian blogging platform LiveJournal. These efforts served as a precursor to the Internet Research Agency (IRA - Агентство интернет-исследований).²⁶ The IRA, a Russian company based in St. Petersburg, was established and funded by Yevgeny Prigozhin (the leader of the Wagner Group) and is involved in online propaganda and influencing Russian business and political interests both domestically and internationally. Since 2013, the agency has utilized fake accounts registered on mainstream social media platforms, forums, and media websites worldwide to promote Kremlin's interests in domestic and foreign policies, including Ukraine, the Western Balkans, and the Middle East. However, it was only after 2016, during the investigation into allegations of Russian interference in the US presidential elections, that the public gained detailed insights into the modus operandi of this troll factory.

To understand Russia's actions as an authoritarian regime on social media, it is necessary to reflect on the Soviet media-propaganda doctrine, specifically the propaganda intelligence system known as active measures. By definition, active measures were an intelligence product of the Soviet KGB aimed at spreading fake news, disinformation, and propaganda through illegal radio stations, newspapers, and magazines to make the views and current policies of the USSR acceptable and generate affirmative attitudes among the population in the West. Building upon this doctrine and in new geopolitical circumstances, Valery Gerasimov, the Chief of the General Staff of the Armed Forces of the Russian Federation, articulated a modern Russian operations strategy known as the Gerasimov Doctrine. This doctrine encompasses hacking services, instrumentalizing media, creating fake news, leaking information, and conventional and asymmetric military means.

Social media is seen as a new battlefield where the misuse of information, intelligence-driven strategies, bot and troll farms, fake news, and narrative creation are utilized to manipulate domestic and global public opinion regarding any operation or policy that may provoke dissent. These tactics are

Although it is difficult to provide a complete list, it is known that a number of other authoritarian systems have begun developing their own internet teams aimed at manipulating public opinion online over the past decade. Some of these countries include China and the so-called 50 Cent Army, Venezuela i Iran. Similar systems have also been established in the Western Balkans region, while private agencies actively conduct disinformation campaigns for the purpose of various governments worldwide, most often during electoral processes

employed to shape and manipulate domestic and global public opinion regarding any operation or policy that may provoke discontent.

Despite the perception that information influence operations for political purposes solely rely on the spread and dissemination of falsehoods, the reality is somewhat different. According to a study by Stanford²⁷, one of the key tactics used by the Russian military intelligence agency (GRU) and the Internet Research Agency (IRA) involves narrative laundering, which entails placing a story in a lesser-known media outlet and then picking it up and repeatedly reinforcing it in state-controlled media to gain popularity. This tactic is closely related to boosting, which aims to legitimize content through its constant repetition in mainstream media and on social media, creating the perception that a particular narrative represents the popular viewpoint of the majority. The underlying principle of influence operations is that information does not necessarily have to be accurate; it just needs to be convincing.

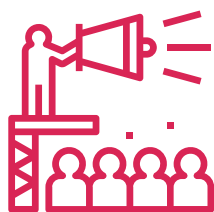
Although it is difficult to provide a complete list, it is known that a number of other authoritarian systems have begun developing their own internet teams aimed at manipulating public opinion online over the past decade. Some of these countries include China and the so-called *50 Cent Army*²⁸, Venezuela²⁹ i Iran³⁰. Similar systems have also been established in the Western Balkans region³¹, while private agencies actively conduct disinformation campaigns for the purpose of various governments worldwide, most often during electoral processes.³²

In a 2020 study titled *Tracking Online Influence Efforts*³³, conducted by Princeton University, researchers presented a dataset covering 76 foreign and domestic information influence operations from 2011 to 2020. These operations were initiated by state actors or ruling parties in autocracies and were carried out in 30 countries. The results showed that during that period, 64% of the information influence operations targeting foreign countries originated from Russia, reaching its peak in 2017 with the implementation of 34 different campaigns. China, Iran, Saudi Arabia, and the United Arab Emirates were responsible for the remaining activities.

4. Methodes and techniques

Authoritarian regimes use various tactics on social networks to spread propaganda, disinformation, and fake news, i.e., to model reality according to their own interests. Methods can vary from the use of bot and troll networks, spreading fake or misleading information to shape public opinion and suppress dissenting voices, to ad hominem targeting and harassment.

4.1. Propaganda and disinformation



Control of information and narratives is considered key to the regime's security. In an authoritarian world, controlling the information environment is crucial, as it directly shapes citizens' willingness to join opposition groups, participate in protests, and engage in anti-regime activities. This is an area where Russia, along with China, plays a leading role. The Kremlin floods the controlled online space with pro-regime narratives, diverting

attention from the regime's actions, spreading the news, and fostering confusion and uncertainty by promoting alternative narratives about events, as was the case following the invasion of Ukraine, in order to convince the domestic public of the correctness and justification of the special military operation.

Many authoritarian regimes share an interest in enhancing their image on an international level, as well as fostering distrust in democracy and the rule of law in general. Discrediting democracy as a governance model is a goal shared by all authoritarian regimes, and the possibilities have significantly increased with the emergence of networks. In this regard, it is indicative that China and Russia have become closer in the information space after the Russian aggression against Ukraine, leading to frequent repetitions of Russian narratives by Chinese media and officials, aimed at discrediting the West and raising the question of Chinese neutrality in the conflict.³⁴ In an empirical study conducted by the Alliance for Securing Democracy in 2023, it was presented that each of the 50 tweets from Chinese diplomats and media with the highest number of shares on that platform mentioned NATO exclusively in a negative context.³⁵ However, there are also previous reports and extensive documentation about secret meetings between officials of these two

countries between 2017 and 2019, aimed at sharing methods and tactics for monitoring dissidents, critics, and controlling the Internet.³⁶

The development of generative technologies will likely further increase the capacity for manipulation through the broader availability of deepfake solutions, making it harder to distinguish between true and false digital content. Micro-targeting will enable autocrats to tailor content to specific individuals or segments of society, similar to how the business world uses demographic and behavioral characteristics to customize advertisements and achieve commercial effects. A suitable illustration of how deepfakes can be used for political purposes is the example of the misuse of the Russian opposition's identity in 2021.³⁷ Currently, we encounter realistic AI-generated images much more frequently than video materials, which are predominantly used for creating fake identities and accounts on social media platforms.

In the mass dissemination of propaganda and disinformation, regimes often resort to astroturfing – a tactic aimed at creating a false perception of widespread support for a person, organization, idea, or political action through the use of trolls and bot networks. These methods involve bombarding networks with pro-government comments, posts, and hashtags that align with the government's narrative, while simultaneously discrediting or attacking those who oppose it. The reach and effectiveness of the content spread by these accounts can be enhanced by social media algorithms, which often promote popular or engaging content, regardless of its veracity. However, many platforms have systems in place to detect and remove such accounts, although the effectiveness of these measures is often questioned.

In addition to automated bot accounts, whose complexity varies, there is an increasing use of accounts created and managed by real people to participate in conversations, post comments or tweets, or send private messages to individuals.



*After Elon Musk took over Twitter, the problem of bot and troll accounts related to Russian and Chinese state propaganda on the platform intensified. This happened because the new owner disbanded the team responsible for tackling information influence operations and coordinated campaigns. This unit worked to combat information operations and coordinated campaigns by countries such as Russia, China, and Iran, to influence public opinion and undermine democracy. The absence of this team now leaves Twitter vulnerable to foreign manipulation and abuse of this kind, even though Musk claims that under his leadership, there is significantly less disinformation on the platform.*³⁸

In 2020, the DFC (Digital Forensic Center) exposed a large pro-China bot network connected to the ruling party in Serbia. The network aimed to promote Chinese medical assistance during the COVID-19 pandemic and highlight the friendship between the two countries.³⁹ Additionally, in the same year, Twitter publicly announced that they had removed over 8,000 accounts linked to the Serbian Progressive Party from their platform.⁴⁰

In the final quarterly report of Meta for the year 2022, it is stated that over 5,000 Facebook accounts, 12 groups, and a certain number of Instagram ac-

How to spot a bot?

Just because it acts like a bot doesn't mean it is a bot. These indicators of automated or co-ordinated online activity can help, but look for a combination of signs, not just one.

ACCOUNT:

- Recent creation date
- Lack of personal information
- Profile photo is ambiguous, stolen or nonexistent
- Divisive words, hashtags, URLs or emojis in bio
- Suspicious handle e.g. lots of numbers

CONTENT:

- Tweeting in more than one language
- Engaging in multiple international narratives
- Signs of automation or account management software like buff.ly
- Posting inflammatory memes and GIFs
- Hashtag spamming
- Occasional off-brand retweets
- Very few reliable news sources
- Awkward turns of phrase

ACTIVITY:

- High volume of tweets (more than 100/day)
- High percentage of retweets (more than 80%)
- Posting persistently day and night
- Posting only at specific times of day
- Sudden spike in activity or change in interests

NETWORK:

- Followers and following is high and almost identical
- High number of following and no followers
- Following a suspicious mix of sources
- Connected to other suspicious accounts
- Duplicated account
- Previously circulating suspicious content
- Previously identified by other organisations as suspicious



counts were removed due to violations of the rules on coordinated inauthentic behavior. This network, controlled by the Serbian Progressive Party, aimed to portray the President and ruling party's widespread popularity across the country in an apparently organic manner. It also aimed to support the government's actions while discrediting opposition actors in the political scene. At least \$150,000 was spent on these activities.⁴¹

On the other hand, the term troll in the context of social media refers to individuals or accounts that intentionally provoke discord, controversy, or negative reactions by posting inflammatory, polarizing, or provocative content. In authoritarian regimes, state-sponsored trolls are often used to harass, intimidate, and discredit critics and opposition figures. This is typically achieved by forming armies of trolls or troll farms that act in coordination and post specific content with the aim of eliciting a reaction from the audience. Examples of such activities can be found in countries like China⁴² and Iran⁴³.

As mentioned before, information influence operations and coordinated campaigns are not limited to domestic spheres; they often target foreign audiences in an attempt to shape international perception and advance the regime's geopolitical interests. Chinese global information influence operations, for example, aim to promote a positive image of the country and its government, downplay the significance of Uyghur human rights issues, and push narratives that align with Beijing's foreign policy objectives.

ProPublica has uncovered over 10,000 fake Twitter accounts associated with the Chinese Communist Party (CCP) and involved in a campaign of coordinated information influence. The report revealed that these accounts targeted Chinese dissidents and sought to discredit the protests in Hong Kong, while continuously spreading disinformation about the COVID-19 pandemic.⁴⁴

During 2019, massive protests took place in Hong Kong against the proposed Chinese extradition law, police brutality, and authoritarian rule. These protests immediately sparked a social media disinformation campaign aimed at undermining the protests, as indicated by Twitter's statement.⁴⁵ Twitter removed 936 accounts originating from the People's Republic of China that were engaged in coordinated efforts to create polarization in society and undermine the legitimacy and political position of the Hong Kong protests. Since Twitter is blocked in mainland China, many of these accounts accessed Twitter using VPNs. However, some accounts accessed Twitter from specific unblocked IP addresses originating from mainland China. The removed accounts represented the most active participants in the mentioned campaign and were part of a larger network of approximately 200,000 accounts.

However, one of the most famous examples comes from Russia. The Internet Research Agency (IRA), a Russian troll factory based in St. Petersburg, has been linked to the Russian government. It employs hundreds of paid trolls who flood social media platforms with pro-Russian content posted under fake identities.⁴⁶

Between 2013 and 2018, the IRA's campaigns on Facebook, Instagram, and Twitter reached tens of millions of users in the United States. According to publicly available information, the IRA spent a total of around \$100,000 over



THE MODUS OPERANDI OF THE INTERNET RESEARCH AGENCY (IRA) IS BASED ON FOUR PILLARS⁵⁰:

1.

DISCREDITING AND ATTACKING: *American institutions; critics of Trump; the Democratic Party in the US presidential elections (2016) and the midterm elections (2018); Emmanuel Macron in the French elections of 2017; Hillary Clinton in the US presidential elections in 2016; Theresa May; US military operations in various locations worldwide.*

2.

POLARIZATION: *American society (for example, simultaneously supporting the Black Lives Matter and White Lives Matter movements), Australian politics, Brazilian politics.*

3.

SUPPORT: *Right-wing movements in the United States; Alternative for Germany (AfD) in the German federal elections (2017); Brexit referendum; Catalan independence vote; Donald Trump in the 2016 US presidential election.*

4.

UNDERMINING AND DIMINISHING SUPPORT:
the case of Angela Merkel.

two years on advertisements—an insignificant amount considering that the operational costs of the IRA were approximately \$1.25 million per month. Nearly 3,400 Facebook and Instagram ads purchased by the IRA are also minor compared to over 61,500 Facebook and 116,000 Instagram posts, along with 10 million tweets spread under the guise of authentic user activity. Over 30 million users, between 2015 and 2017, shared one of the fake posts from Facebook or Instagram with their friends and family. As stated in reports based on Facebook's data, the IRA's activities that spread disinformation about the electoral process and exacerbated societal divisions reached far more people organically than through paid advertisements.⁴⁷

Content is often disseminated through a process where state-controlled alternative or mainstream media outlets or bloggers create disinformation and narratives, which are then spread by bot and troll profiles across various channels, including social media platforms. Eventually, individuals and groups in the digital sphere, whether ideologically aligned with those narratives or simply falling into the category of useful idiots, share the propagated content, organically amplifying the reach of the propaganda and exposing a large number of people to the same content. Depending on their personal or group ideological or value positions, whether they are far-right or far-left, bloggers or theorists, they align themselves with the served narrative and add their own claims or theses, further amplifying the propaganda in favor of the creators.

According to the data provided by Facebook to the United States Senate Select Committee on Intelligence (SSCI) in 2019, one of the pages created by the IRA was the Crna Gora News Agency, which targeted the Montenegrin audience. The articles published on this page primarily aimed to discredit pro-Western entities and NATO.⁴⁸

When it comes to Montenegro, there is a strategic use of bot accounts (controlled by humans) and trolls by political parties, with an estimated 80% of political content on social media and news portals being their work.⁴⁹

4.2. Surveillance



Social media platforms provide an abundance of data about individuals' activities, online presence, and opinions, which became evident to the general public after the Cambridge Analytica scandal.⁵¹

In April 2018, Facebook's founder and CEO Mark Zuckerberg testified at two congressional hearings about his company's role in the Cambridge Analytica scandal, when it was revealed that Facebook had exposed the data of nearly 87 million users to political exploitation. The case is a blatant example of how personal data is increasingly being used to influence election outcomes.

One of the primary surveillance methods involves tracking public posts and private communications on social media platforms. Given the abundance of personal data and opinions shared on these networks, these platforms provide a rich source of information for regimes that want to monitor their citizens. This varies from tracking public sentiment and identifying citizens' dissatisfaction to singling out individuals who express disagreement or opposition to the regime. Research shows, for example, that the Chinese government uses digital tools to predict events that could create hotspots for unrest, then preemptively applies repression to reduce disagreement before dissatisfaction spreads.⁵²



However, the most ambitious mass surveillance and control project is the Chinese social credit system, or rating system, according to which every citizen has a numerical value reflecting their contribution and usefulness to society, in all spheres of life. The system is based on a large amount of personal data, and the process is made possible thanks to citizens' reliance on numerous online and mobile services. Scores can affect access to certain privileges such as travel, obtaining loans, employment, and education.

SORM (System for operative investigative activities), the Russian government's surveillance system, was initially developed by the KGB to monitor telephone calls. Surveillance expanded to the Internet to track the content of emails, internet browsing activity, and other digital data as part of a new version known as SORM-2. By 2015, an updated version — SORM-3 — encompassed all telecommunications. According to Russian law, internet service providers are required to install SORM equipment that allows the Russian Federal Security Service (FSB) access to all data shared on the network without the companies' knowledge or control over which data is shared and with whom. SORM essentially copies all data flows on the Internet and telecom networks — sending one copy to the government and the other to the intended destination.⁵³

In April 2018, Facebook’s founder and CEO Mark Zuckerberg testified at two congressional hearings about his company’s role in the Cambridge Analytica scandal, when it was revealed that Facebook had exposed the data of nearly 87 million users to political exploitation. The case is a blatant example of how personal data is increasingly being used to influence election outcomes

With the help of artificial intelligence and machine learning, this process can be automated and carried out on a large scale, enabling the regime to build comprehensive profiles of its citizens’ political views, personal connections, and daily routines.

In this regard, there are numerous reservations about the use of the TikTok application outside the geographical boundaries of China. Data collection is the norm for almost all social networks, but the question arises: who has access? When it comes to TikTok, allegations and claims⁵⁴ are often made that data from global users end up in the hands of the Chinese Communist Party (CPC). However, the company has repeatedly denied this.⁵⁵

Besides content data, geolocation data remains when publishing content on social networks, which is significant for authoritarian regimes. Through this, the movement of individuals or groups of dissenters can be tracked, and it is handy for identifying participants in protests or political rallies.

4.3. **Censorship**



Regimes often control social media platforms, censoring content critical of the government or challenging the official narrative. This can include blocking certain users, removing posts, or even completely shutting down platforms.

Internet censorship is perhaps the most obvious way authoritarian regimes use digital tools for repression. China, for example, operates what is known as the Great Firewall – currently the most extensive censorship system in the world, a joint venture of the government, technology, and telecommunications companies working together to filter content that the regime deems harmful.

China has been the most repressive state regarding internet freedom for the eighth consecutive year. Censorship was increased during the 2022 Beijing Olympic Games and after tennis star Peng Shuai accused a high-ranking official of the Communist Party of China of sexual assault. The government continued to tighten control over the country’s tech sector, including new rules that require platforms to use their systems to promote the CPC’s ideology. Journalists, human rights activists, religious and ethnic minority group members, and other users were detained for sharing online content, with some facing harsh prison sentences.⁵⁶

Particular attention is paid to reports from public gatherings, party meetings, as well as news about major holidays. In fact, any large gathering is considered risky, so information about them is under special control. Chinese censors are particularly sensitive to attempts to connect to foreign social networks such as Facebook, Instagram or Twitter and posting photos or videos with political connotations.

Chinese WeChat implements real-time automatic censorship over images exchanged via chat. When a message is sent from one user to another, it passes through a server managed by Tencent (the parent company of WeChat), which detects whether the message contains blacklisted keywords before the message is sent to the recipient.⁵⁷

The course of history itself can be altered by such filtering, and particularly censored are sensitive historical events that do not agree with the official state narrative. Information about the Tiananmen Square protest in 1989 cannot be found on Baidu Baike, the Chinese equivalent of Wikipedia. On a search for “1989”, there are only two results: the number between 1988 and 1990 and the name of a computer virus. All other events from 1989 have been erased from the records, including the moment when soldiers of the People’s Liberation Army of China opened fire on civilians in Beijing after several months of student protests at Tiananmen Square.⁵⁸



In 1996, when only 150,000 Chinese were online, State Council Decision No. 159 explicitly aimed to place the Internet under state control. Over the last twenty years, Beijing’s legal and technical architecture for web censorship and surveillance has dramatically increased. Even though Chinese President Xi Jinping centralized control over the Internet in 2013 (mostly through the creation of a Cyber Space Administration that reported directly to him), over sixty agencies with enormous legal and technical capabilities to regulate online activities now oversee Chinese cyberspace.⁵⁹

In addition to China, Iran and Russia are striving to isolate their citizens from the rest of the world. Since adopting the sovereign internet law in 2019, Russia has consolidated its control over infrastructure and intensified the blocking of foreign platforms, VPNs, and international websites. It remains to be seen how successful the government will be in achieving this goal – due to a combination of political and especially technical factors.⁶⁰ In Iran, the National Information Network centralizes infrastructure under state control, enabling the blocking of almost all major international platforms and control of domestic communication channels.⁶¹

Certain states are increasing pressure on technology companies to remove content and share user data, as seen in transparency reports published by large online platforms. Publicly available data shows that Facebook, Google, and Twitter most often receive requests for content removal for national security reasons, criticism of authorities, and religious offenses. Between January 2019 and June 2020, only three countries in the top ten in terms of the number of requests for content removal have full internet freedom and are rated as democracies – the UK, France, and Germany.⁶²

Twitter received 971 requests from governments and courts, from October

In 2016, on the day of parliamentary elections in Montenegro, access to WhatsApp and Viber communication applications was shut down due to the widespread dissemination of fake negative messages about an alleged election theft by the then-ruling party, originating from numbers in China and the United Kingdom⁶⁹

27, 2022, to April 27, 2023. The requests ranged from removing controversial posts to providing private data to identify anonymous accounts. Twitter reported that it fully complied with the requests in 808 cases and partially in 154 cases. As for the nine requests, Twitter did not report any specific response.

Elon Musk took over Twitter, promising a new era of freedom of speech and independence from political pressure. However, data shows that the company has complied with numerous requests for surveillance and censorship under Musk's leadership, particularly in countries like Turkey and India. In India, where the media, journalists, and critical voices have been suppressed for

months, Twitter complied with government requests to censor content related to a BBC documentary highly critical of Prime Minister Narendra Modi, which the Indian government had blocked in January. The company justified this action by citing Indian laws.⁶³ According to the non-governmental organization Reporters Without Borders, press freedom in India has significantly declined by eight points in the past year, and the country ranked 150th on the international list.

On the other hand, in May 2023, two days before the elections in Turkey, Twitter censored Erdogan's critics, which sets a serious precedent. Turkey threatened to block access to Twitter in the country if the platform did not remove content from several accounts.⁶⁴

In the year before Musk's takeover, the compliance rate with government reports and requests was around 50%. After Musk's takeover, that percentage increased to 83% (808 out of a total of 971 requests). The orders vary greatly in scope and subject, but they all involve the government asking Twitter to either remove content or disclose information about a user.



Although Facebook, Google, and Twitter often receive requests for content removal due to national security or criticism of authorities, there are often instances of wrong steps by the platforms themselves, resulting in direct human rights violations. Facebook (now Meta) has confessed making mistakes in removing content related to the 2021 protests against the forced eviction of Palestinians from their homes in the Sheikh Jarrah neighborhood of Jerusalem. In an external report commissioned by Meta, it is stated that the content removal actions taken by Meta had a negative impact on the rights of Palestinian users to freedom of expression, freedom of assembly, political participation, and non-discrimination, thereby affecting the ability of Palestinians to share information and insights into their experiences as they truly happened. The report also mentions that Meta removed far more Arabic posts about the specific case than in Hebrew. Furthermore, last year's Amnesty International report high-

*lighted that these platforms' algorithms amplified the spread of harmful content against Rohingya Muslims in Myanmar, contributing to real-world violence.*⁶⁶

With AI's advancement, autocracies' ability⁶⁷ to implement such censorship has improved. AI can analyze images and text in sophisticated ways, allowing regimes to filter and block undesirable content.

Even if such censorship fails to yield results, autocracies have an additional line of defense: they can shut down internet access – either entirely or in specific areas – to prevent citizens from communicating, organizing, or sharing messages. There are numerous examples of this tactic. We can recall instances when the Russian government used targeted mobile internet shutdowns during anti-government protests in Moscow in 2019, or when the Iranian government successfully shut down internet access across the country amid widespread protests in November 2019.⁶⁸

Within a few weeks after the invasion of Ukraine, the Kremlin blocked Facebook, Instagram, and Twitter, citing extremism, thereby preventing the population from accessing reliable information about the war and limiting their ability to connect with users in other countries. The platforms were blocked after Meta stated that it would allow social media users in Ukraine to post messages inciting violence against Russian President Vladimir Putin and the Russian army and glorify the Azov Battalion. This represents the establishment of double standards and a violation of their own rules and policies regarding hate speech. Major social media and technology companies like Facebook (or its parent company, Meta), Twitter, and Google joined EU sanctions against Sputnik and RT and removed the accounts of these media outlets from their platforms. While many have applauded such moves, freedom of speech advocates, even within Russia, have warned of the dangerous consequences of these decisions, citing increased censorship in other non-democratic countries while simultaneously blocking access to independent sources of information. At the time of writing this study, the accounts of these two Russian state media outlets are still accessible on Twitter.

The blocking of platforms has resulted in greater use of domestic networks – VK and Odnoklassniki. According to publicly available information, Yandex, a popular Russian search browser and Google's equivalent, has prioritized disinformation and reduced search results for websites criticizing the invasion. The government also blocked over 5,000 websites, forced the media to call the invasion a special military operation, and introduced a law prescribing up to 15 years in prison for those spreading fake information about the conflict.⁷⁰

Although internet censorship has captured the digital space, millions of Russians have opted for VPN services and the dark web to bypass government restrictions. Surfshark, a VPN company from Lithuania, reported that the use of their VPN server increased by 3500% since the start of the invasion on February 24, 2022. The biggest leap occurred on March 5 and 6 of that year, the company announced, when Russia announced it would take steps to block access to Twitter and Facebook.⁷¹

During the period of the coronavirus epidemic (2020-2021), numerous authoritarian regimes introduced laws under the guise of fighting against disin-

formation and infodemics.⁷² Countries such as Iran, Russia, Egypt, Venezuela, Belarus, China, and Cambodia have taken steps to combat opposition and those disagreeing with the state narrative.⁷³ Thus, a blogger from Rwanda was sentenced to 10 years in prison on charges of inciting civil disobedience and spreading rumors, and in Bangladesh, a media activist faced a prison sentence of up to seven years for allegedly spreading fake news against the government.⁷⁴

Following the adoption of a new restrictive law in 2020, companies such as Facebook, Twitter, and YouTube were forced to open offices in Turkey that would comply with government requests for content removal. Additionally, in October 2021, the Turkish Parliament passed a law introducing a prison sentence of up to three years for individuals believed to be promoting fake information on social networks.⁷⁵ Besides allowing the state to be the arbiter of truth, the law requires social networks to hand over the personal data of users suspected of spreading fake news.⁷⁶

4.4. Harassment, intimidation, discrediting



Regimes can use social media to harass, intimidate, or threaten critics. This can include doxxing (publicly revealing private information about an individual), online harassment, or even threats of violence. A 2020 report from the Oxford Internet Institute states that evidence was found in fifty-nine countries that trolls are used to attack, dox, and harass political opponents, activists, or journalists on social media.⁷⁷

Besides being created for spreading disinformation and boosting the reach of state propaganda, bot and troll networks can be directed to target individuals or groups who are critics of the regime.

Through network surveillance tools, dissident voices can be identified, who can then be targeted for harassment both online and offline. Such surveillance often goes hand in glove with intimidation, where regimes use laws to suppress freedom of speech and punish critics with deprivation of liberty, physical, and online violence.



5. Impact on democracy: reasons for concern

One of the fundamental pillars of democracy is the free flow of reliable and accurate information. Today, it mostly occurs online, on social media platforms, which have become the backbone of the digital information ecosystem. Since 2016, through multiple documented cases, it has become evident that technological development can be effectively and efficiently used to degrade democratic systems, values, and societies.

The algorithmic dynamics relied upon by content recommendations on social media platforms largely enable information operations of influence. These prioritize emotional content likely to attract user attention, promoting sensationalist, often inaccurate information while simultaneously locking users into echo chambers, where touch with reality is lost.⁷⁸ The development of generative technologies based on artificial intelligence, which enable the creation of realistic audio, photo, and video content, will only accelerate this trend.

The previous year, 2022, marked the sixteenth consecutive year of global democratic decline.⁷⁹ With the spread of methods, techniques, and approaches for digital authoritarianism, new technologies have breathed new life and strengthened authoritarianism and leaders who maintain their rule on these values.

Understanding and confronting digital authoritarianism is vital for protecting individual freedoms and preserving the integrity of democratic institutions and processes.

5.1. Preserving democracy and democratic values

Digital authoritarianism presents a significant threat to democracy, as evidenced by numerous documented cases of authoritarian regimes interfering in elections in democratic countries, disseminating disinformation, and creating divisions via social media platforms. Such practices can not only undermine trust in democratic institutions and processes but also potentially influence the outcome of elections. Some authoritarian regimes export their practices of digital authoritarianism to other countries, thereby impacting global norms and standards related to internet governance and digital rights.

Understanding these tactics and developing effective countermeasures is crucial for preserving democracy. The tools, techniques, and strategies of digital authoritarianism are adopted in democratic countries by political parties, interest groups, and private companies to the detriment of public trust, personal privacy, and other civil liberties.

In both subtle and direct ways, authoritarian governments use the global information space to undermine the values and institutions that are the basis of a rule-based international order, discrediting the idea of democracy while seeking to weaken essential democratic norms. For authoritarian regimes, targeting democracy is a matter of survival for their governance mechanisms and the values they believe should underpin the international system in the future.⁸⁰ The infodemic associated with the COVID-19 pandemic has provided further opportunities for these systems to further fuel divisions and mutually support each other in spreading narratives when it is strategically useful to weaken democratic cohesion. In spreading conspiracy theories about the virus's origin, Chinese, Iranian, and Russian officials and media have retweeted content put out by organizations, media, and accounts associated with their governments.⁸¹ On the other hand, a wave of populist or il-

Freedom of speech, freedom of assembly, and the right to privacy are fundamental human rights that can be threatened by digital authoritarianism

liberally inclined political parties and leaders in hybrid regimes and democracies are increasingly adopting the approach to politics from autocratic regimes. They undermine institutions, reject critics, and exploit digital platforms to spread propaganda and disinformation. They manipulate public political opinion and do not hesitate to seek support from extreme groups and actors within and outside the state.

5.2. Protection of Human Rights and Freedoms

Freedom of speech, freedom of assembly, and the right to privacy are fundamental human rights that can be threatened by digital authoritarianism. The Internet has long served as a platform for freedom of speech and the free exchange of ideas. However, digital authoritarianism threatens this freedom, as regimes can manipulate online discourses, debates, and suppress dissenting

voices. With the advent of sophisticated surveillance technologies, authoritarian regimes can monitor the activities of their citizens. This violates the right to privacy and can have severe consequences for freedom of expression, leading to self-censorship out of fear.

Moreover, through the misuse of social networks, regimes can manipulate public opinion and data, violating individuals' rights to access accurate and unbiased information. Advances in AI have also enabled more effective methods of control. The risk of using new technologies for suppression or control is increasing, especially during times of socio-political tensions, elections, protests, demonstrations, armed conflicts, or other types of crises, such as a pandemic. The most vulnerable are human rights defenders and other civil society activists, whistleblowers, independent journalists, political opposition, as well as racial and ethnic minorities.

5.3. Security

The tactics used by digital authoritarian regimes, including hacking campaigns, surveillance, and disinformation, can present significant security risks. This can have implications not only for individuals, but also for companies, organizations, and even governments. Authoritarian regimes are expanding the reach of their digital tools abroad, openly increasing surveillance over their own citizens and those of other countries.

5.4. Information integrity

In the era when we largely receive information via social media, the spread of disinformation can have serious consequences: deceiving the public, disrupting fact-based decision-making, and fueling existing societal divisions. The use of social media to spread disinformation can significantly impact public discourse in democracies and society at large, as it undermines the integrity of decision-making. This can lead to polarization and fragmentation of society, making it difficult to achieve consensus and directly affecting the ability of democratic societies to face challenges effectively.

5.5. Social cohesion

Digital authoritarianism often involves the use of inflammatory content to manipulate public opinion and create divisions. This can lead to increased polarization and conflict, undermining social cohesion. Authoritarian regimes can use digital tools to exert influence beyond their borders, shaping global narratives and norms in ways that serve their geopolitical interests. They can also export surveillance and censorship technologies to other countries, contributing to the global spread of authoritarian practices.



6. Responding to the challenge

Ensuring freedom of the Internet is crucial for protecting democracy, as technology should empower citizens to make decisions consciously, based on facts, without coercion or manipulation. Social networks have become significant public platforms with immense power and responsibility to serve the public good. However, over the years, alongside the crisis of the liberal democratic order, we encounter growing tendencies of authoritarian regimes to misuse technology for their own needs, both within and outside the country, directly undermining democratic processes worldwide.

To protect democracy in the 21st century, technology companies, governments, and civil society must cooperate to address manipulation, misuse, and data collection issues. This requires multilateral and cross-sectoral coordination to promote digital literacy, identify malicious actors, and prevent and expose their actions that violate human rights, the rules of digital platforms, and undermine processes within democracies.

In this regard, there is a widely held belief that technology companies must do more to prevent information influence operations, ensuring that their actions do not restrict freedom of speech or violate basic human rights.

Efforts to expose disinformation and reveal information influence operations on social media platforms have become increasingly robust in recent years, but this raises numerous questions regarding implementation, consistency, and transparency.⁸²

One of the primary strategies used by social media platforms involves the use of machine learning algorithms to identify and label potentially decep-

tive content.⁸³ These algorithms can analyze text, images, and videos for disinformation and conspiracy theories. Some platforms will entirely remove contentious content, while others may label it as potentially misleading and reduce its visibility. However, it will take some time for the algorithm to be sufficiently perfected and trained for all languages equally to recognize and remove content from our linguistic region efficiently.

In addition to automated detection, platforms like Facebook have also employed fact-checking teams, which review flagged content, often in collaboration with external fact-checking organizations. If the content is deemed false or misleading, it can be labeled as such, providing users with more context and helping to limit the spread of untruths.⁸⁴

Following documented cases where Facebook served as a tool for election interference, it and other platforms have paid more attention to the principle of transparency. In the context of political marketing, Facebook has disabled the placement of paid political ads outside the financier's home country. Additionally, the Facebook Ads Library has become publicly accessible. It allows anyone to search and view active and inactive ads on social issues, elections, or politics that have been launched on Facebook or Instagram. The library includes details such as ad content, who paid for it, the amount of money spent, the number of people reached, and demographic data about who is targeted. This feature is particularly useful for journalists, researchers, and all interested parties, for better insight into the extent and nature of political advertising and online campaigns. Also, it enables regulatory bodies and researchers to track money flows and identify associated trends.⁸⁵



Meta, TikTok, Twitter, and Google have been periodically publishing transparency reports for years. These documents provide insight into various aspects of their business, especially in content moderation, government requests for user data, content removal, and enforcement of their community standards or guidelines.

In this context, the measures by networks that treat coordinated inauthentic behavior and information influence operations are very significant, aiming for greater transparency and authenticity. False representation, use of fake accounts, artificially inorganic boosting of content popularity through the use of bot networks, or engaging in behaviors that lead to other violations of community standards or platform rules are not allowed. In this regard, in-

terested individuals, researchers, and media can find publicly available data in the quarterly reports that platforms publish.⁸⁶ The fact that the big three (Facebook, Instagram, and Twitter) are prone to manipulation is evidenced by the data that they have marked and removed over 350 coordinated efforts and information influence operations since 2018.⁸⁷ However, a big problem is the consistency and effectiveness of measures in the fight against manipulation and coordinated behavior, as buy-

Efforts to expose disinformation and reveal information influence operations on social media platforms have become increasingly robust in recent years

ing inauthentic support on platforms remains cheap and available, and the percentage of identified and removed accounts used for such operations is decreasing.⁸⁸

While social media platforms take steps to encourage transparency and accountability, the specifics and effectiveness of their measures can vary significantly from one company to another.⁸⁹ Since Elon Musk took over Twitter, many have accused him of promoting the spread of disinformation on the platform.⁹⁰ Criticism followed after Musk reinstated previously suspended or banned accounts, some of which had even been penalized for spreading disinformation, conspiracy theories, or hate speech. Often, Musk shares content of questionable credibility on his own account.⁹¹

In addition to social networks, Google is making efforts to combat disinformation, build journalists' capacities, and support fact-checking associations. After more than 80 fact-checking organizations sent a letter⁹² to YouTube in January, stating that this platform is one of the main channels for spreading disinformation and conspiracy theories, which enables the misuse of the platform, Google (who owns YouTube) announced a donation of 13 million dollars to the International Fact-Checking Network (IFCN). The grant will fund the establishment of a Global Fact-Checking Fund.⁹³

In addition, Google continuously updates its search algorithms to ensure that reliable information ranks higher in search results. Furthermore, when users search for an information that is incorrect, Google provides information from fact-checking organizations alongside search results. The company also collaborates with external organizations to provide training and resources for journalists and support media literacy programs.

Under the auspices of the European Union, a series of companies and platforms signed a strengthened 2022 Code of Practice Against Disinformation to prevent the proliferation of fake news, increase transparency, and curb the spread of bots and fake accounts.⁹⁴



In May 2023, led by Musk, Twitter reportedly withdrew from that Agreement,⁹⁵ significantly reducing moderation on Twitter. Research shows this has enabled an increase in the spread of disinformation. Twitter previously had a dedicated team working to combat coordinated disinformation campaigns, but experts and former employees note that most of them have resigned or been dismissed.⁹⁶

In addition to the voluntary code, the EU has also adopted the Digital Services Act (DSA). This law will legally oblige companies from August 2023 to do more to combat illegal online content. The Act aims to encourage more careful and transparent content moderation, increase platform accountability for the information they distribute, and reduce disinformation. Full implementation is expected by mid-February 2024. The document will bind all companies that provide services in the European Union, regardless of whether they are established on its territory or not. The DSA represents a significant step forward, as the EU has decided to take steps to address the problem of spreading disinformation, hate speech, and other illegal content via social networks and large communication platforms. To oversee the implementation of the

Act, a regulatory Commission will be established, which will be able to impose sanctions – from financial penalties of up to 6 percent of a company's global revenue, to a temporary suspension of platform access at the EU level.⁹⁷

At the same time, privacy and data protection will be in focus. Thus, the European Union's General Data Protection Regulation (GDPR) has influenced the establishment of new standards relating to data privacy and giving users more control over their personal data. Some social media companies have also changed their privacy settings and data practices in response to public pressure and regulatory control.⁹⁸

After two years of work and months of negotiations, European Union lawmakers reached an agreement and published a draft law on artificial intelligence called the Artificial Intelligence Act. Upon reviewing the Act's proposals, AI tools will be classified according to their perceived risk level: minimal to limited, high, and unacceptable. High-risk AI systems include those influencing voters during elections and AI systems of social networks for ranking and disseminating content.⁹⁹ In addition to the above, there are a number of other relevant EU instruments in the fight against disinformation

In addition to the internal efforts of companies and social networks, there are organizations dedicated to combating disinformation and online influence operations. These are non-profit organizations, research groups, and journalistic organizations. They monitor social media platforms for deceptive content, report their findings, and often work directly with platforms to solve problems. Facebook's partial data sharing with research organizations, such as the DFRLab and the Stanford Internet Observatory, has helped raise awareness about the impact, reach, and execution of information operations carried out by various authoritarian regimes and actors.

However, at the global level, there is a clear disparity in resources between those conducting influence operations and civil society trying to highlight them. These organizations lack resources for monitoring, analyzing, and opposing malign activities, and their actions are often slowed or hampered by local political elites who themselves spread disinformation. It's important to note that through enhanced cooperation, transparency, and data sharing with interested parties, social networks could more effectively and extensively shed light on the problem of network abuse in different geographical areas.

Network abuses remain a significant challenge despite all efforts, especially due to the disproportionate application of measures in non-English speaking areas.¹⁰⁰ The fact is that the amount of content, the global reach of platforms, and the speed at which disinformation can spread contribute to the complexity of this issue, which should obligate networks to take more proactive action.

It's still too early to say whether the EU's involvement and recognition of the problem will contribute to solving it on an international level, but the measures taken represent important steps, even though their implementation at the global level remains questionable.¹⁰¹



7. Conclusion

With the rise of global mass communication in the 21st century, there has been a shift in the way information is exchanged, its speed, and the possibilities it offers. Although at the beginning of the previous decade, there was a belief in the inevitable disintegration of authoritarian regimes after a few examples of social media being used to bring about significant socio-political changes, that premise has proven to be utopian and naive.

On the contrary, digital authoritarianism has demonstrated the ability of certain regimes not only to adapt but also to reshape the power balance between democracies and autocracies by exploiting social media and leveraging the inherent weaknesses of democracies in responding quickly and uniformly to growing challenges. Leaders of this trend include Russia, Iran, and China, which have developed modern methods of control, manipulation, surveillance, and censorship, first for domestic purposes within their geographical boundaries and then for information operations worldwide.

Propaganda and disinformation spread on the Internet and social media deepen social polarization, exacerbate ethnic tensions, fuel nationalism, undermine public trust in media, journalism, public institutions, democratic processes, and contribute to a crisis in liberal democracy. International reports witness this regression, highlighting that the Internet and democracy are becoming increasingly defensive and less free worldwide.

The motivation behind such actions is not only the consolidation, control, and strengthening of power but also the enhancement of authoritarian regimes' international image and the promotion of distrust in democracy, the rule of law, and the exploitation and exacerbation of existing social, political, and economic divisions. The discrediting of these values and principles is directly linked to the survival of these regimes in power. In this regard, there is growing evidence of coordination and collaboration between Moscow and Beijing in spreading anti-Western narratives and mutual adoption of tactics.

In an increasing number of countries, internet shutdowns and other repressive actions that disrupt access to online information have facilitated efforts to achieve sovereign control or a sovereign internet. Certain countries have adopted measures to control data flow and isolate their domestic Internet from the global network. Imposing new restrictions on cross-border data transmission and storage, as well as centralizing technical infrastructure, enables authorities to exert complete control over the information space and the content their citizens receive, especially in the context of domestic and international turmoil. Such practices create space for the violation of basic human rights, the expansion of surveillance, censorship, and easier access to user data through the adoption of stringent laws.

While it is often argued that social media platforms bear primary responsibility, they cannot be solely held accountable, despite their role in enabling digital authoritarianism. Despite inconsistencies, these platforms have become more proactive in identifying and removing coordinated inauthentic behavior originating from state or state-affiliated actors. In recent years, efforts to raise awareness about the existence and impact of network abuse have been made by promoting transparency principles, publicly available data, reports, and insights into advertising practices.

The European Union, as a geopolitically important actor, has actively engaged through several acts and laws in an attempt to contribute to problem-solving, primarily at the European level. However, it will require additional time for tangible results from the new legislative solutions. Additionally, an increasing number of civil society organizations play a significant role in exposing information operations of influence through OSINT research.

These activities should be accompanied by national governments proposing new laws on personal data protection, which would be updated for the digital age. This would make it more difficult for all actors to access individuals' data and use them for information influence operations. Furthermore, the security sector of each country could establish concrete cooperation and information exchange with platforms on authoritarian influence operations and other actions targeting democratic integrity within the states themselves.

Due to the complexity of the challenges, democracies have been unprepared and slow for years in devising comprehensive responses. As the trends leading to the information and crisis of liberal democracy have shown, the response must be multi-dimensional. Therefore, a combination of public-private partnerships, media, and the civil sector should play a decisive role in defining and implementing a unified response in the future. In the meantime, authoritarian regimes will continue to exert pressure regardless of whether democracies can find an effective response or not.¹⁰²

From everything presented, the conclusion is evident that the best way to counter any form of authoritarianism is to nurture, defend, and uphold democratic values, the rule of law, free and fair elections, freedom of speech, as well as media independence, and professionalism. If democracies fail to defend their own achievements, principles, and interests with the same determination with which authoritarian regimes attack and target them, digital authoritarianism will become the new normalcy.

8. References

- 1** Shahbaz, A, Funk, A, Vesteinsson, K, Freedom on the Net 2022 Countering an Authoritarian Overhaul of the Internet, Freedom House, available at: <https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf>
- 2** Putin calls for balanced assessment of Stalin, 03.12.2009, Reuters, available at: <https://www.reuters.com/article/idUSGEE5B21J6>
- 3** Repucci, S, Slipowitz, A, Freedom in the world 2022 The Global Expansion of Authoritarian Rule, Freedom House, available at: https://freedomhouse.org/sites/default/files/2022-03/FITW_World_2022_digital_abridged_FINAL.pdf
- 4** Kalathil, S, The Evolution of Authoritarian Digital Influence: Grappling with the New Normal, National Defense University Press, News Article View (ndu.edu), available at: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-1/prism_9-1_33-50_Kalathil-2.pdf?ver=D-JRX5DRHKfqeXbyt6et98w%3D%3D
- 5** Shahbaz, A, Funk, A, Vesteinsson, K, Freedom on the Net 2022 Countering an Authoritarian Overhaul of the Internet, Freedom House, available at: <https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf>
- 6** Trajković, I, Kineski digitalni zid za suvereni državni internet, 25.07.2022, Al Jazeera, available at: <https://balkans.aljazeera.net/news/technology/2022/7/25/kineski-digitalni-zid-za-suvereni-drzavni-internet>
- 7** Wong, B, Bottorff, C, Top Social Media Statistics And Trends Of 2023, 18.05.2023, Forbes, available at: <https://www.forbes.com/advisor/business/social-media-statistics/#:~:text=In%202023%2C%20an%20estimated%204.9,5.85%20billion%20users%20by%202027>
- 8** Shahbaz, A, Funk, A, Vesteinsson, K, Freedom on the Net 2022 Countering an Authoritarian Overhaul of the Internet, Freedom House, available at: <https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf>
- 9** EU citizens trust traditional media most, new Eurobarometer survey finds, 12.07.2022, European Parliament, available at: <https://www.europarl.europa.eu/news/en/press-room/20220704IPR34401/eu-citizens-trust-traditional-media-most-new-eurobarometer-survey-finds>
- 10** Newman N, Fletcher, R, Robertson, C, Eddy, K, Nielsen, R, Digital News Report 2022, Reuter Institute and University of Oxford, available at: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2022-06/Digital_News-Report_2022.pdf
- 11** Kemp, S, Digital 2023: Global Overview Report, 26.12.2023, Datareportal, available at: <https://datareportal.com/reports/digital-2023-global-overview-report>
- 12** Tradicionalni mediji dominantno oblikuju politička uvjerenja crnogorskih građana, 29.05.2023, CeMI, available at: <https://cemi.org.me/me/post/tradicionalni-mediji-dominantno-oblikuju-politicka-uvjerenja-crnogorskih-gradana-1090>
- 13** Medijska pismenost i građani Crne Gore Istraživanje javnog mnjenja, maj 2023, Digitalni forenzički centar, <https://dfcme.me/wp-content/uploads/Istrazivanje-javnog-mnjenja-2023-2.pdf>
- 14** The Attention Economy Why do tech companies fight for our attention?, 17.08.2021, Center for Humane Technology, available at: <https://www.humanetech.com/youth/the-attention-economy>

- 15** Kavenna, J, Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy', 4.10.2019, Guardian, available at: <https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-autonomy-digital-privacy>
- 16** Deibert, R, The Road to Digital Unfreedom: Three Painful Truths About Social Media, Januar 2019, Journal of Democracy, available at: <https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-three-painful-truths-about-social-media/>
- 17** Quenqua, D, Facebook Knows You Better Than Anyone Else, 19.01.2015, The New York Times, available at: <https://www.nytimes.com/2015/01/20/science/facebook-knows-you-better-than-anyone-else.html>
- 18** Algoritmom do informacije ili profita?, 15.11.2022, Digitalni forenzički centar, available at: <https://dfcme.me/algoritmom-do-informacije-ili-profita/>
- 19** Spaić, A, Vujović, R, Petričević, P, Jovičević, I, Društvene mreže I novinarstvo u Crnoj Gori, Medijski savjet za samoregulaciju, available at: https://www.medijskisavjet.me/images/sample-data/dokumenti/Drus%CC%8Ctvene_mrez%CC%8Ce_i_novinarstvo_u_CG.pdf
- 20** Woolley, S, Joseff, K, DEMAND FOR DECEIT: How the Way We Think Drives Disinformation, Januar 2020, National Endowment for Democracy, available at: <https://www.ned.org/wp-content/uploads/2020/01/Demand-for-Deceit.pdf>
- 21** Shahbaz, A, Funk, A, Vesteinsson, K, Freedom on the Net 2022 Countering an Authoritarian Overhaul of the Internet, Freedom House, available at: <https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf>
- 22** Standish, R, Study Shows How Russian, Chinese Disinformation About COVID-19 Evolved During The Pandemic, 02.12.2021, Radio Free Europe, available at: <https://www.rferl.org/a/russia-china-covid-disinformation-campaigns/31590996.html>
- 23** Freedom of the Net 2022. Belarus, Freedom House, available at: <https://freedomhouse.org/country/belarus/freedom-net/2022>
- 24** Bradshaw, S, Bailey, H, Howard, P, Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation, Computational Propaganda Research Project, Oxford Internet Institute, University of Oxford, available at: <https://demtech.oi.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report-2020-v.2.pdf>
- 25** Ibid.
- 26** Howard, P, Lie Machines How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives, Yale University Press, available at: <https://yalebooks.yale.edu/book/9780300250206/lie-machines/>
- 27** Diresta, R, Grossman, S, Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019, Stanford Internet Observatory Cyber Policy Center, available at: <https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/potemkin-pages-personas-sio-wp.pdf>
- 28** Lau, J, Who Are the Chinese Trolls of the '50 Cent Army'?, 07.10.2016, Voice of America, available at: <https://www.voanews.com/a/who-is-that-chinese-troll/3540663.html>
- 29** Kelly, S, Truong, M, Shahbaz, A, Earp, M, White, J, Manipulating Social Media to Undermine Democracy, Freedom House, available at: <https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy>
- 30** Khameneh, A, The Scorched-Earth Tactics of Iran's Cyber Army, 21.03.2023, Weird, available at: <https://www.wired.com/story/iran-cyber-army-protests-disinformation/>
- 31** Milivojević, A, Castle: Kako srpska vlast manipuliše razumom, a građani za to još i plaćaju, 18.06.2020, Balkan Insight, available at: <https://balkaninsight.com/sr/2020/06/18/castle-kako-srpska-vlast-manipulise-razumom-a-gradani-za-to-jos-i-placaju/>
- 32** Kirchgassner, S, Ganguly, M, Pegg, D, Cadwalladr, C, Burke, J, Revealed: the hacking and disinformation team meddling in elections, 15.02.2023, The Guardian, available at: <https://www.theguardian.com/world/2023/feb/15/revealed-disinformation-team-jorge-claim-meddling-elections-tal-hanan>

- 33** Martin, D, Shapiro, J, Ilhardt, J, Trends in Online Influence Efforts, 2020, Empirical Studies of Conflict, available at: <https://esoc.princeton.edu/publications/trends-online-influence-efforts>
- 34** Bodnar, J, Schafer, B, Soula, E, A Year of Disinformation: Russia and China's Influence Campaigns During the War in Ukraine, 24.02.2023, GMF Alliance for Securing Democracy, available at: <https://securingdemocracy.gmfus.org/a-year-of-disinformation-russia-and-chinas-influence-campaigns-during-the-war-in-ukraine/>
- 35** *ibid.*
- 36** Belovodyev, D, Soshnikov, A, Standish, R, Exclusive: Leaked Files Show China And Russia Sharing Tactics On Internet Control, Censorship, 05.04.2023, Radio Free Europe, available at: <https://www.rferl.org/a/russia-china-internet-censorship-collaboration/32350263.html>
- 37** Roth, A, European MPs targeted by deepfake video calls imitating Russian opposition, 22.04.2021, The Guardian, available at: <https://www.theguardian.com/world/2021/apr/22/european-mps-targeted-by-deepfake-video-calls-imitating-russian-opposition>
- 38** Atanesijan, G, Društvene mreže i lažne vesti: Ruske trollove nema ko da kontroliše na Twitteru, 19.04.2023, BBC News na srpskom, available at: <https://www.bbc.com/serbian/lat/svet-65285088>
- 39** DFC otkriva: Sa koronom stigla i mreža bot profila u Srbiju, 13.04.2020, Digitalni forenzički centar, available at: <https://dfcme.me/nova-mreza-bot-profila/>
- 40** Twitter Removes Thousands Of Accounts 'Promoting' Serbian Ruling Party, 02.04.2020, Radio Free Europe, available at: <https://www.rferl.org/a/serbia-twitter-vucic-sns-serbian-progressive-party/30526199.html>
- 41** Nimmo, B, Franklin, M, Agranovich, D, Hundley, L, Torrey, M, DETAILED REPORT: Quarterly Adversarial Threat Report, Februar 2023, Meta, available at: <https://about.fb.com/wp-content/uploads/2023/02/Meta-Quarterly-Adversarial-Threat-Report-Q4-2022.pdf>
- 42** Waddell, K, 'Look, a Bird!' Trolling by Distraction, 27.01.2017, The Atlantic, available at: <https://www.theatlantic.com/technology/archive/2017/01/trolling-by-distraction/514589/>
- 43** Deck, Andrew, A million-strong troll army is targeting Iran's #MeToo activists on Instagram, 29.06.2022, Rest of world, available at: <https://restofworld.org/2022/troll-army-targeting-irans-metoo-activists-instagram/>
- 44** Kao, J, Shuang Li, M, How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus, 26.03.2020, ProPublica, available at: <https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus>
- 45** Information operations directed at Hong Kong, 19.08.2019, Twitter blog
- 46** Maynes, C, Inside the Internet Research Agency: a Mole Among Trolls, 17.04.2018, Voice of America, available at: <https://www.voanews.com/a/inside-the-internet-research-agency-a-mole-among-trolls/4352107.html>
- 47** Howard, P, Ganesh, B, Liotsiou, D, The IRA, Social Media, and Political Polarization in the United States, 2012-2018, Computational Propaganda Research Project, available at: <https://www.intelligence.senate.gov/sites/default/files/documents/The-IRA-Social-Media-and-Political-Polarization.pdf>
- 48** DiResta, R, Grossman, S, Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019, 12.11.2019, Stanford Freeman Spogli Institute for International Studies, available at: <https://fsi.stanford.edu/publication/potemkin-think-tanks>
- 49** MREŽE BOTOVA I TROLOVA U CRNOJ GORI (1): VOJNICI NA ZADATKU, 21.09.2022, Centar za istraživačko novinarstvo Crne Gore, available at: <https://www.cin-cg.me/mreze-botova-i-trolova-u-crnoj-gori-1-vojnici-na-zadatku/>
- 50** Martin, D, Shapiro, J, Ilhardt, J, Trends in Online Influence Efforts, 05.08.2020, Scholar Princeton, available at: https://scholar.princeton.edu/sites/default/files/jns/files/trends_in_online_influence_efforts_v2.0_aug_5_2020.pdf
- 51** Klajmen, Z, Afera Fejsbuk-Kembridž analitika: Šta sve znamo do sada, 21.03.2018, BBC News na srpskom, available at: <https://www.bbc.com/serbian/lat/svet-43475183>

- 52** Qin, B, Strömberg, D, Wu, Y, Why Does China Allow Freer Social Media? Protests versus Surveillance and Propaganda, Journal of Economic Perspectives, available at: <https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.31.1.117>
- 53** Polyakova, A, Meserole, C, Exporting digital authoritarianism The Russian and Chinese models, August 2019, Brookings, available at: <https://www.brookings.edu/research/exporting-digital-authoritarianism/>
- 54** Milmo, D, TikTok's ties to China: why concerns over your data are here to stay, 8.11.2022, The Guardian, available at: <https://www.theguardian.com/technology/2022/nov/07/tik-toks-china-bytedance-data-concerns>
- 55** Shepardson, D, TikTok CEO: App has never shared US data with Chinese government, 22.03.2023, Reuters, available at: <https://www.reuters.com/technology/tiktok-ceo-app-has-never-shared-us-data-with-chinese-government-2023-03-22/>
- 56** Shahbaz, A, Funk, A, Vesteinsson, K, Freedom on the Net 2022 Countering an Authoritarian Overhaul of the Internet, Freedom House, available at: <https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf>
- 57** Kenyon, M, WeChat Surveillance Explained, 07.05.2020, The Citizen Lab, available at: <https://citizenlab.ca/2020/05/wechat-surveillance-explained/>
- 58** Moore, M, Tiananmen Massacre 25th anniversary: the silencing campaign, 18.05.2014, The Telegraph, available at: <https://www.telegraph.co.uk/news/worldnews/asia/china/10837992/Tiananmen-Massacre-25th-anniversary-the-silencing-campaign.html>
- 59** Polyakova, A, Meserole, C, Exporting digital authoritarianism The Russian and Chinese models, August 2019, Brookings, available at: <https://www.brookings.edu/research/exporting-digital-authoritarianism/>
- 60** Sherman, J, Reassessing RuNet: Russian internet isolation and implications for Russian cyber behavior, 12.07.2021, Atlantic Council, available at: <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/>
- 61** Iran's National Information Network, 9.11.2012, The citizen lab, available at: <https://citizenlab.ca/2012/11/irans-national-information-network/>
- 62** Clarke, L, Swindells, K, How social media companies help authoritarian governments censor the internet, 09.06.2021, The New Statesman, available at: <https://www.newstatesman.com/science-tech/2021/06/how-social-media-companies-help-authoritarian-governments-censor-internet>
- 63** India ban on BBC Modi documentary 'imperils press freedom', 25.12.2023, Aljazeera, available at: <https://www.aljazeera.com/news/2023/1/25/india-banning-bbc-documentary-on-modi-attack-on-press-freedom>
- 64** Kagubare, I, Klar, R, Twitter's restriction of Turkish election content sparks fear of precedent, 25.05.2023, The Hill, available at: <https://thehill.com/policy/technology/4019109-twit-ters-turkey-election-sparks-criticism/>
- 65** Biddle, S, FACEBOOK REPORT CONCLUDES COMPANY CENSORSHIP VIOLATED PALESTINIAN HUMAN RIGHTS, 21.09.2022, The Intercept, available at: <https://theintercept.com/2022/09/21/facebook-censorship-palestine-israel-algorithm/>
- 66** MYANMAR: FACEBOOK'S SYSTEMS PROMOTED VIOLENCE AGAINST ROHINGYA; META OWES REPARATIONS, 29.09.2022, Amnesty International, available at: <https://www.amnesty.org/en/latest/news/2022/09/myanmar-facebook-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/>
- 67** Brandom, R, Twitter is complying with more government demands under Elon Musk, 27.04.2023, Rest of world, available at: <https://restofworld.org/2023/elon-musk-twitter-government-orders/#:~:text=In%20its%20first%20six%20months,the%20previous%20twelve%20months%20combined.&text=The%20data%2C%20drawn%20from%20Twitter's,requests%20from%20governments%20and%20courts.>
- 68** Frantz, E, Kendall-Taylor, A, Wright, J, Digital Repression in Autocracies, Mart 2020, V – Dem

Institute, available at: <https://www.v-dem.net/media/publications/digital-repression17mar.pdf>

69 Vlada: Gašenje Vibera na dan izbora nije neustavno, 28.03.2017, FOS media, available at: <https://fosmedia.me/arhiva/infos/drustvo/vlada-gasenje-vibera-na-dan-izbora-nije-neustavno>

70 Shahbaz, A, Funk, A, Vesteinsson, K, Freedom on the Net 2022 Countering an Authoritarian Overhaul of the Internet, Freedom House, available at: <https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf>

71 Perrett, C, Russia's internet censorship is forcing citizens to turn to the dark web and VPNs for news and social media, 17.03.2022, Insider, available at: <https://www.businessinsider.com/what-happens-social-media-and-news-go-dark-in-russia-2022-3>

72 Wiseman, J, Rush to pass 'fake news' laws during Covid-19 intensifying global media freedom challenges, 3.10.2020, International Press Institute, available at: <https://ipi.media/rush-to-pass-fake-news-laws-during-covid-19-intensifying-global-media-freedom-challenges/>

73 Shahbaz, A, The Rise of Digital Authoritarianism, Freedom House, available at: <https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism>

74 *ibid.*

75 Freedom of the world 2023 Turkey, Freedom House, available at: <https://freedomhouse.org/country/turkey/freedom-world/2023>

76 Hubbard, B, Timur, S, Turkey Allows Jail Terms for What It Deems 'Fake News', 14.10.2022, The New York Times, available at: <https://www.nytimes.com/2022/10/14/world/europe/turkey-jail-fake-news.html>

77 Bradshaw, S, Bailey, H, Howard, P, Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation, Computational Propaganda Research Project, Oxford Internet Institute, University of Oxford, available at: <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report-2020-v.2.pdf>

78 Mantellassi, F, Digital Authoritarianism: How Digital Technologies Can Empower Authoritarianism and Weaken Democracy, 16.02.2023, Geneva Centre for Security Policy, available at: <https://www.gcsp.ch/publications/digital-authoritarianism-how-digital-technologies-can-empower-authoritarianism-and>

79 Freedom in the World 2022 The Global Expansion of Authoritarian Rule, Feburar 2020, Freedom House, available at: https://freedomhouse.org/sites/default/files/2022-02/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf

80 Kalathil, S, The Evolution of Authoritarian Digital Influence Grappling with the New Normal, National Defense University, available at: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-1/prism_9-1_33-50_Kalathil-2.pdf?ver=DJRX5DRHKfqeXby6et98w%3D%3D

81 *ibid.*

82 Kornbluh, K, Goodman, E, Weiner, E, Safeguarding Digital Democracy - Digital Innovation and Democracy Initiative Roadmap, Mart 2020, The German Marshall Fund of the United States, available at: https://www.gmfus.org/sites/default/files/Safeguarding%2520Democracy%2520against%2520Disinformation_v7.pdf

83 Mosseri, A, Working to Stop Misinformation and False News, 07.04.2017, Meta, available at: <https://www.facebook.com/formedia/blog/working-to-stop-misinformation-and-false-news#:~:text=lf%20the%20fact%2Dchecking%20organizations,appear%20lower%20in%20News%20Feed.>

84 Meta's Third-Party Fact-Checking Program, Meta, available at: <https://www.facebook.com/formedia/mjp/programs/third-party-fact-checking>

85 Ad Library, Meta, available at: https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=ME&media_type=all

86 Coordinated Inauthentic Behavior, Meta, available at: <https://about.fb.com/news/tag/coordinated-inauthentic-behavior/>

- 87** Pamment, J, Victoria Smith, *Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online*, Jul 2022, NATO Strategic Communications Centre of Excellence, available at: <https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244>
- 88** Fredheim, R, Sebastian Bay, Anton Dek, Martha Stolze, Tetiana Haiduchyk, *Social Media Manipulation 2022/2023: Assessing the Ability of Social Media Companies to Combat Platform Manipulation*, 03.03.2023, NATO Strategic Communications Centre of Excellence, available at: <https://stratcomcoe.org/publications/social-media-manipulation-20222023-assessing-the-ability-of-social-media-companies-to-combat-platform-manipulation/272>
- 89** Tobin, A, Varner, M, Angwin, J, *Facebook's Uneven Enforcement of Hate Speech Rules Allows Vile Posts to Stay Up*, 28.12.2017, ProPublica, available at: <https://www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes>
- 90** 'Stamp of approval': Twitter's Musk amplifies misinformation, 19.04.2023, France 24, available at: <https://www.france24.com/en/live-news/20230419-stamp-of-approval-twitter-s-musk-amplifies-misinformation>
- 91** Lee, K, *Elon Musk, in a Tweet, Shares Link From Site Known to Publish False News*, 30.10.2022, The New York Times, available at: <https://www.nytimes.com/2022/10/30/business/musk-tweets-hillary-clinton-pelosi-husband.html>
- 92** Milmo, D, *YouTube is major conduit of fake news, factcheckers say*, 12.01.2022, The Guardian, available at: <https://www.theguardian.com/technology/2022/jan/12/youtube-is-major-conduit-of-fake-news-factcheckers-say>
- 93** Ma, O, Feldman, B, *How Google and YouTube are investing in fact-checking*, 29.11.2022, Google blog, available at: <https://blog.google/outreach-initiatives/google-news-initiative/how-google-and-youtube-are-investing-in-fact-checking/>
- 94** *The 2022 Code of Practice on Disinformation*, European Commission, available at: <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>
- 95** Thierry Breton, *Twitter*, 26.05.2023, available at: <https://twitter.com/ThierryBreton/status/1662194595755704321?s=20>
- 96** Spring, M, *Twitter insiders: We can't protect users from trolling under Musk*, 06.03.2023, BBC News, available at: <https://www.bbc.com/news/technology-64804007>
- 97** *Pitanja i odgovori: Akt o digitalnim uslugama**, 25.04.2023, Evropska komisija, available at: https://ec.europa.eu/commission/presscorner/detail/hr/QANDA_20_2348
- 98** *Шта је Општа уредба о заштити података?*, Google, available at: <https://support.google.com/google-ads/answer/7687725?hl=sr>
- 99** *AI Act: a step closer to the first rules on Artificial Intelligence*, 11.05.2023, European Parliament, available at: <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence#:~:text=AI%20systems%20with%20an%20unacceptable,behaviour%2C%20socio%2Deconomic%20status%2C>
- 100** Marinescu, D, *Facebook's Content Moderation Language Barrier*, 08.09.2021, New America, available at: <https://www.newamerica.org/the-thread/facebook-s-content-moderation-language-barrier/>
- 101** Engler, A, *The EU AI Act will have global impact, but a limited Brussels Effect*, 08.06.2022, Brookings, available at: [The EU AI Act will have global impact, but a limited Brussels Effect \(brookings.edu\)](https://www.brookings.edu/research/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/)
- 102** Kalathil, S, *The Evolution of Authoritarian Digital Influence Grappling with the New Normal*, National Defense University, available at: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-1/prism_9-1_33-50_Kalathil-2.pdf?ver=DJRX5DRHKfqeXbyt6et98w%3D%3D



IMPRESSUM

PUBLISHER: Digital Forensic Center
EDITOR IN CHIEF: Azra Karastanović
AUTHORS: Milan Jovanović and DFC team
DESIGN AND LAYOUT: Ana Đurković
CIRCULATION: 80 copies
PRINTING: Piccolo Print Podgorica

СIP - КАТАЛОГИЗАЦИЈА У ПУБЛИКАЦИЈИ
НАЦИОНАЛНА БИБЛИОТЕКА ЦРНЕ ГОРЕ, ЦЕТИЊЕ

ISBN 978-9940-817-08-4
COBISS.CG-ID 22499332



This project is funded through a U.S. Embassy grant. The opinions, findings, and conclusions or recommendations expressed herein are those of the author(s) and do not necessarily reflect those of the Department of State.



www.dfcme.me  DFCMNE  DFCME  DFCMEDOTME

