STUDIA I ANALIZY NAUK O POLITYCE
2 (2023)

https://doi.org/10.31743/sanp.16411.14661

Armoured Information as a Promising Concept to Reduce Disinformation – a New Element of Armoured Democracy?

Informacja opancerzona jako obiecująca koncepcja ograniczająca dezinformację – nowy element demokracji opancerzonej?

Martinas Malužinas
Ph.D., Koszalin University of Technology, e-mail: martinasmaluzinas@gmail.com
https://orcid.org/0000-0002-2772-9534

Abstract: The aim of this article is to present the concept of armoured information, the primary task of which is to protect transmitted data (information). The article attempts to show the close relationship between the concept of armoured information and the category of armoured democracy or the recently developed category of armoured constitution. The common feature of the distinguished concepts is the aim to preserve the political order, especially its structural elements, which are democracy and its procedures. This is done by protecting reliable information showing a comprehensive, objective picture of the reality described, which in turn translates into a better quality of democracy and its protection in the respective country.

Keywords: information, armoured information, armoured democracy, democracy, authoritarianism

Streszczenie: Celem artykułu jest przedstawienie koncepcji informacji opancerzonej, której podstawowym zadaniem jest ochrona przekazywanych danych (informacji). Artykuł podejmuje próbę ukazania ścisłego związku idei informacji opancerzonej z kategorią demokracji opancerzonej czy z niedawno powstałą kategorią konstytucji opancerzonej. Cechą wspólną wyróżnionych koncepcji jest dążenie do zachowania porządku politycznego, a szczególnie jego strukturalnych elementów, jakimi są demokracja i jej procedury. Dokonuje się to poprzez ochronę rzetelnej informacji ukazującej całościowy, obiektywny obraz opisywanej rzeczywistości, co z kolei przekłada się na lepszą jakość demokracji i jej zabezpieczenie w danym państwie.

Słowa kluczowe: informacja, informacja opancerzona, demokracja opancerzona, demokracja, autorytaryzm

As many researchers point out, democracy in Europe has been under strong pressure for a long time. Examples of countries where the executive branch's respect for democratic values and constitutional order is declining are Hungary, Poland, Italy, Slovenia and the Czech Republic.

Reference is made to indicators on democracy and respect for political and civil rights, which confirm that these observations are part of a broader trend. When analysing the global Democracy Index[1] by region – as of 2022 – it should be noted that there are no countries in the Central and Eastern (CEE) region that fall into the full democracy category.

The fact is that two countries (Russia and Belarus) are considered "authoritarian regimes," two states (Ukraine and Hungary) are hybrid regimes, and nine countries (Lithuania, Latvia, Estonia, Romania, Bulgaria, Czech Republic, Poland, Slovakia and Slovenia) are considered countries with flawed democracy. As far as Hungary is concerned, it is emphasised that it has evolved from the category of a flawed democracy towards a hybrid democracy (see figure).

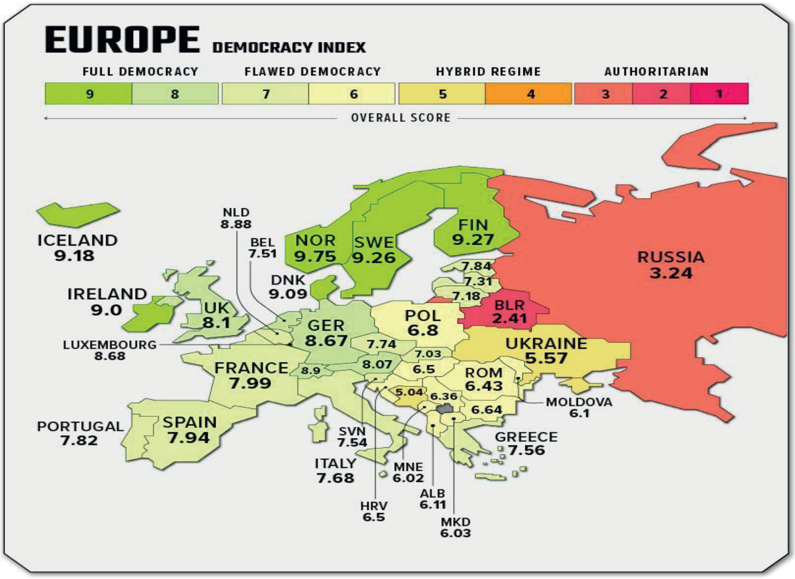

Figure. Democracy Index for European countries in 2022

Source: compiled from Visualcapitalist 2022.

[1] This year's Democracy Index report by the independent think-tank Economist Intelligence Unit (EIU) is one such attempt to implement an assessment of countries based on the extent to which they conform to democratic ideals.

The result for Ukraine fell to 5.57, which means that it has become a state with a hybrid regime. Russia's score also fell to 3.24, maintaining the status of the authoritarian regime. It should be noted that the developed EIU report was published before the start of Russia's invasion of Ukraine in February 2022, and the ongoing military conflict will certainly affect the results in next year's report.

In part, we can therefore agree with George Schopflin's thesis that post-communism is not only a transitional state but can be a key element of regional policy when trying to predict the future of states associated with it. This means that the CEE countries are still experiencing post-communism and even a retreat from democracy (Schopflin 1994: 128–130).

Comparing the groups of Western European countries with the CEE countries, it can be concluded that such countries as Norway, Finland, Sweden and Iceland meet the higher quality criterion of democracy. A significant deterioration in this region took place in Spain; the country is now considered a flawed democracy. The countries of Western Europe have a higher average in relation to the CEE, which testifies to the higher quality of democracy in this region.

Two years after the pandemic hit the world, it is noticeable that global democracy is in a deeper downward trend. However, it is often forgotten that populism is one of the factors that threaten and degrade the quality of democracy in many countries of the world. Also important is the growing role of *fake news* and disinformation, which have a destabilising effect on society and democracy.

Disinformation is information that is both false and harmful, intended to cause harm. In particular, CEE countries are increasingly the target of such campaigns. In recent years, dozens of carefully designed campaigns have posted millions of deliberately false and misleading posts on the CEE's online social spaces. The resulting confusion, and thus the problem of deciphering facts and separating them from fiction, has had a devastating effect on public trust, critical thinking and the ability of citizens to engage honestly in politics – the lifeblood of a functioning democracy.

The ever-increasing presence of fake news in everyday life is causing a decline in citizens' trust in the media in the region. In this context, it is worthwhile to systematize the types of disinformation. When classifying the nature of disinformation interventions, internal or external intervention is distinguished.

In the case of the first intervention may come from the country of the sender. Manipulated or falsified information is disseminated by haters and trolls, often for profit (e.g., increasing advertising revenue) or for propaganda and political purposes. The latter issue internally makes the appeal of disinformation to illiberal politicians or populists a convenient tool for extremist discourse to compete with and ultimately supplant rational, informed debate.

In the second case, the intervention can be considered in an external context, that is, its source can be foreign entities. In this context, Russia is the leading provider of disinformation campaigns in the group of the CEE states, conducting at least a few known operations in the subregion. Building on the historical Russian legacy (which coined the term *disinformatsyia*), targeted disinformation tactics in the CEE became an adaptation of the Russian military strategy of "hybrid war" (Świerczek 2019: 191–207). This strategy reinforces and exploits divisions in the target society, favouring fragmentation and polarisation. Often the goal is not so much to convince but to confuse citizens. By creating false equivalences between democratic and undemocratic political actors, it creates disillusionment and apathy. The special purpose of the Russian services is to undermine the credibility of election procedures, their organizing bodies and the political forces involved in elections. According to various post-election reports in the analysed countries, the false information aimed to discourage voters from participating in elections due to the threat of COVID-19, discredit political parties and the electoral administration apparatus and sow discontent with the functioning of Democracies in these countries (Fraszka 2020: 7–9). It is also noted that Russian disinformation campaigns are primarily aimed at a political goal. Moreover, the messages of these campaigns are anti-democratic, anti-Western and anti-UN. For example, the CEE states as a group of post-Soviet states are regular targets of pro-Kremlin disinformers. A particular example of disinformation was the Russian attacks during the parliamentary election campaign in Lithuania, Latvia, Estonia, Slovenia and the Czech Republic (Łukasik-Turecka, Malužinas 2023: 77). Many high-profile political events related to disinformation have shaken the trust of the citizens of the distinguished countries in the internet as a potential associated with the idea of democracy. This means that the democracies of the CEE countries are not immune to foreign or internal interference, and their governments do not have strategies to defend democratic processes.

Although there are other intervening states or political actors in the world, when it comes to foreign intervention, Russia is the actor that most people think of first. Quite a lot in this context is also known about Russian interference in the CEE, to which researchers are paying more and more attention (Bryjka 2022: 5; Legucka 2022: 24–29). Interference or intervention via social media and even traditional media has been much more talked about since 2014 when Russia's annexation of Crimea saw a marked deterioration in Russia-West relations.

In the above context, it is worth asking the research question: how can the **credibility of information (media)** be designed so that it is less susceptible to domestic and foreign interference in democratic (CEE) states, and could especially protect against malicious interference in an ever-evolving digital landscape and growing anti-democratic trends.

In the analysis presented here, the author does not focus on *strictly* cyber security issues, which are the subject of research by cyber defence experts. According to Paul Buther, distinguishing fact from fiction requires a lot of effort or specialized knowledge. Disappointed with the results, citizens may even lose faith in democracy itself (Buther 2019: 15). Instead, the author draws attention to a widespread trend and is interested in options for designing the information available to the public to be safeguarded from interventions, especially during electoral processes (especially during election campaigns), which can affect the conduct and outcome of elections and the state of a country's democracy.

The purpose of this article is to refer to any feature of an information project that aims to protect information as "armoured information" in order to document its close relationship to the idea of "armoured democracy" or the recently emerging idea of "armoured constitution."[2] Armoured information, in addition to the two mentioned concepts, has a common goal, which is to preserve the elements of the political order, that is, democracy and its procedures, respectively. Armoured democracy should be understood as any possible means to defend democracy against anti-democratic forces and ensure their survival in the new social environment (Bäcker, Rak 2019: 64).

However, the concepts cited differ in a number of important ways, such as their timing – armoured democracy seeks to prevent non-democratic forces from gaining power, while an armoured constitution seeks to limit the damage even if enemies of the rule of law have gained political power.

[2] No credit can be taken for formulating the term "armoured information" as such. In the scientific literature, however, the term is not widely used by researchers and has not yet gained notoriety in public discourse.

On the other hand, armoured information, which is a potential element of armoured democracy, will try to eliminate it at an early stage by fully identifying the threats, identifying these threats, and making them public. In a democratic system, you need to have well-informed citizens, actors responsible for their implementation (Government vs. actors far beyond government) and means to achieve the goal (prohibition of extremist parties, media accountability, as well as restrictions on freedom of assembly and protection of the constitution).

This article is an attempt to determine what media restrictions citizens could agree to in order to restrict politicians, foreign services, or other entities that seek to increase distrust of the institutions and principles of democracy in the country. **Pointing to trends – already prevalent – in which armoured information is being projected by many social networks, which contributes to providing increasingly reliable protection of its quality (the ability to limit its distortion) from would-be autocrats, populists or external interference, may sound like a lofty idea, but one worthy of scholarly exploration in further discussions of democratic theory and its consolidation.**

The analysis finds only limited empirical evidence that the rules of information censorship are able to systematically block politicians and external actors from distorting information in a given country. The following will be cited facts where such a practice is increasingly present in order to preserve the democratic system.

1. The concept of armoured democracy

The main demand of Karl Loewenstein, the creator of this concept, was to arm democracy with tools that can be used to combat its enemies so that it is not replaced by authoritarian governments (Loewenstein 1937a: 417–432). It is most often understood as a democratic system whose primary goal is to eliminate threats to its existence, both from internal and external enemies (Bäcker, Rak 2019: 64). Accepting this assumption leads to the conclusion of the appropriateness of translating the term "militant democracy" as an armoured democracy, i.e. a democracy with a defensive function – ready to defend itself against any possible threat – but also an offensive one, i.e. a democracy capable of attacking and destroying or overpowering an opponent if necessary.

The two most famous measures suggested by K. Loewenstein are the prohibition of extreme events and the restriction of freedom of assembly. Others include banning the formation of paramilitary units, precautions against the illegal use of firearms and other weapons, holding newspaper editors accountable for reports deemed "subversive propaganda," measures against incitement to violence or hatred against other groups, exclusion from public administration of persons with extremist tendencies, and the creation of political police to control anti-democratic and anti-constitutional activities (Loewenstein 1937b: 638–658).

2. Armoured information

It should be noted that many would-be autocrats (populists) or foreign actors (including Russian services and Kremlin elites) may wish to manipulate information in order to pursue their particular goals. Below, the author discusses how trends will emerge in the world that (unconsciously or consciously) project reality, including a long-term strategy contributing to the defence against disinformation threats and online information manipulation that destabilise the quality of democracy. As already noted, the author proposes to name such a global trend as a set of structural features of so-called "armoured information."

The focus of this publication is not on issues that are relevant to cybersecurity design for certain reasons, such as: combating fake news using computational intelligence techniques, detecting fake news online using machine learning techniques, systematic mapping research, etc. In other words, the so-called technical aspects were not taken into account. **In this part, the author discusses the current trends (phenomena) in which state and non-state actors, such as NGOs or social networks, contribute to protection against potential opponents of democracy. In a broader perspective, this can be called the effect of the ongoing processes of globalization.**

As Federica Liberini, Michela Redoano, Antonio Russo, Angel Cuevas and Ruben Cuevas note, social media such as Facebook, X (Twitter) and YouTube have recently become indispensable tools for political agitation (Liberini, Redoano, Russo, Á. Cuevas, R. Cuevas 2020: 2). According to several reports, these platforms could have played a decisive role in the outcome of the two decisive votes in 2016: the referendum in the UK on Brexit in the European Union (EU) and the presidential election in the United States.[3] The growing importance of social media shows that they are an effective channel of political communication that affects the quality of functioning of democratic institutions.[4] However, direct evidence of the impact of social media on voter behaviour during political campaigns is still limited.

Thanks to advances in technology and the widespread availability of user-generated data (including information on individual interests through so-called "cookie policy"), platforms such as Facebook, X (Twitter), Instagram, YouTube and even TikTok enable politicians to reach voters with a very high degree of precision that was probably not possible before. This phenomenon is generally referred to as microtargeting, which has contributed to the growing role of social media in the global political arena.

3. Constitutional options to restrict freedom of speech

Many CEE legislators recognise that the constitution can limit freedom of speech to a limited extent, eliminating only manifestations of its abuse in public places (or in virtual space) and only in relation to the most constitutionally relevant entities. However, it does not restrict this freedom in such a way as to prevent the issuing of assessments, opinions or even criticism of these entities, and therefore does not suppress public discourse. This means that the essence of freedom of speech is not violated, and the restriction imposed, justified by the premise of public order, does not violate the basic principles of democracy.

It is worth mentioning that the task of the legislator in a democracy is to create a legal order that allows relatively peaceful coexistence of individuals who differ in their views. On the other hand, an attempt to introduce amendments to the Constitution that would restrict freedom of expression

[3] E.g., The US Senate Special Committee on Intelligence has published the second volume of its report on Russian campaigning and interference in the 2016 US election (see (U)Report 2016).

[4] According to a report published in October 2018 by the UK Parliament's Digital, Culture, Media and Sport Special Committee investigating social media manipulation during the election, an unknown organisation spent more than £250,000 on Facebook adverts in 2018 that reached more than 10 million people in the UK and pushed for a much harsher Brexit than by then Prime Minister Theresa May.

would constitute a clear violation of the basic law and would provoke considerable opposition.

Introducing constitutional changes in this matter may sound like a panacea for the challenges described above. However, the attempt to introduce amendments in this matter is hampered by the complicated procedure for amending the constitution and the mechanisms for securing it. As a result, such actions can trigger one of two unintended legal and political consequences. The constitution may be exchanged in its entirety, as such an amendment need not comply with the formal rules of revision (Landau, Dixon 2015: 859–890), or it may lose its binding force and simply not be followed in practice (Contiades, Fotiadou 2013: 427–478). Therefore, the legislator must take into account the full range of factors that could impede or even threaten the constitutional legal order and the rule of law. Therefore, such a debate remains open to lawyers, whose goal is to find ways to optimize, rather than maximize, the difficulty of changing constitutional rules.

4. Restricting internet and social media freedom by authoritarian states

Facebook, Instagram, X (Twitter) and YouTube, despite their huge popularity, are not available everywhere in the world. Some countries restrict or block access to social media. The main reason is that social media offers many opportunities for actors, but in certain situations, it can pose a threat to the stability of the regime and its legitimacy. Their significant influence and the dynamic spread of the information contained in them make access to such services not always well received. Therefore, the authorities of some countries decide to restrict or block their use (in particular, this applies to the most popular platforms such as Facebook or X (Twitter), without which it is currently difficult to imagine communication). In most cases, the reason for such radical decisions is to protect the political system. For some regimes, it is inconvenient for photos or intra-state information to reach other users. Such regimes are in China, where residents are not allowed to use Facebook, X (Twitter), YouTube or Google. China is one of the most restrictive countries on the internet. The censors blocked well-known websites because, according to the regime, they were used to coordinate anti-government protests. In North Korea, access to the most popular social networks (Facebook, YouTube, X (Twitter)) is also blocked, which is justified by the fact that they are controlled by external entities. Incidents related to the blocking of Facebook, X (Twitter) and YouTube also occurred in Turkey. In the wake of various political events in Turkey, Recep Tayyip Erdoğan decided to obstruct access to websites for many hours, as the flow of information coming from Western countries could be detrimental to the local authorities. In Ukraine, access to sites such as VKontakte, the equivalent of Facebook, Odnoklassniki and Yandex, a search engine similar to Google, was blocked for three years by a decision of former President Petro Poroshenko in November 2016. The Ukrainian authorities have acknowledged that they serve Russian propaganda activities and the collection of information about Ukrainian citizens. The Middle East is also facing some restrictions. Iran's authoritarian government, in a bid to control the flow of information, has blocked access to popular sites including Facebook, X (Twitter) and Instagram. The case of Vietnam is also interesting in this regard. Officially, the authorities of this state do not block access to Facebook, but from time to time users complain about accessibility problems, interruptions in the functioning of the site or technical works that are ordered by the government (Kuchta-Nykiel 2017).

5. The role of social networks in building an armoured democracy

The above actions on the part of authoritarian state institutions prompt a rational reflection on the possibility of using the same solution by democratic states for defence. Many cases can be identified where politicians or citizens in a democratic state have had their access to websites restricted or blocked.

An example of this is the blocking of the account of Donald Trump for two years by the owners of popular social networks Facebook and Instagram because in their forums he questioned the results of the elections and called for violence, contributing to the attack on the seat of the US Congress and the deaths of innocent citizens in January 2021. Donald Trump was also blocked on X (Twitter), YouTube and Snapchat (Polsatnews.pl 2021).

The issue of the suspension of D. Trump's accounts divided society in the United States, sparking a heated debate. Some citizens were happy that the platforms calmed D. Trump, while others spoke of an attack on freedom of speech. This is a natural reaction for citizens living in a democratic system since the mechanism of blocking websites poses a risk to freedom of speech and access to information. However, actions of this kind by social networks show that online platforms have long belonged to the public sphere, which stands guard over public order and democratic values adopted in Western civilizations.

By not accepting groups or organisations that promote violence or attack people because of characteristics protected by law, Facebook,[5] Instagram and X (Twitter) blocked a number of such accounts between 2016–2022. These include the Facebook profile of the Polish nationalist movement (2016) or the account of the National-Radical Camp (ONR) in Ukraine (2019). In 2019, Facebook has also blocked accounts linked to far-right populist organisations, including the British National Party (BNP) and the English Defence League (EDL). In 2020, Facebook removed the page of Polish populist Janusz Korwin-Mikke, and in 2022 blocked access to his political party – The Confederacy (Konfederacja). In the same year, X (Twitter) blocked the account of Marjorie Taylor Greene, a Republican member of the House of Representatives, who in November 2021 was first elected to the United States Congress. This means that social networks are taking over the central platform of communication in the modern world, becoming at the same time agencies *of fake news* to combat illegal content (e.g., incitement to violence, hate speech), hitting users and political organisations whose activities are not only illegal but also threaten democratic values and polarise societies.

[5] Facebook blacklist divides entities into three different levels, corresponding to the gradation of the threat level. The third level consists of militarized social movements and conspiracy groups that promote violence, and private individuals and groups that promote hatred. The second level consists of entities that commit violence against representatives of public administration or the military, but generally do not direct it against the civilian population. The first level covers terrorist organisations promoting hatred or criminal activity, linked to the organisation or incitement to violence against civilians, persistent dehumanisation or incitement to violence against persons on the basis of their protected characteristics; it also covers the involvement in regular criminal activity.

6. Information defence mechanisms

When a would-be autocrat or outside agents try to undermine the independence of some actors, political institutions, or political system, it is important to know who has the right – and perhaps also the duty – to take steps against such actions.

From the above analysis, it follows that such a role can be taken by the social networks themselves, which are taking more and more decisive steps in this direction. Similarly, democratic states contribute to this trend – in order to protect their system and citizens. An example is the solutions taken by, among others, the United States, which blocked the websites of Iranian state media in 2021 (Dziennik.pl 2021). This trend was most evident after the Russian military aggression in Ukraine in February 2022. The dynamics of events in the field of International Security gave social networks and political actors an impetus to action.

Sanctions imposed by Western countries have increasingly affected ordinary citizens of Russia. However, the media could still spread propaganda about the war in Ukraine also outside Russia (Musiał-Karg, Łukasik-Turecka 2023: 13–14). This is why the EU and the United States are trying, to the best of their ability, to stop *fake news* and the phenomenon of disinformation. EU member states, the United Kingdom, the United States, Australia and Canada have decided to block Russian TV channels from broadcasting their propaganda. Now also Facebook, X (Twitter) and Google are going in this direction and blocking Russian media on their sites (Bankier.pl 2022). However, this is not a total block, but a geolocation block, which means that stations such as Russia Today cannot publish content on X (Twitter) in many European countries (dailyweb.pl 2022). At the beginning of the war, YouTube blocked access to Russian-funded channels. The same goes for other accounts, including Sputnik TV. All this is in response to the sanctions imposed by the EU against Russia.

The actions taken by state and non-state actors are aimed at reducing the risk of Kremlin propaganda and at increasing resistance to authoritarianism. As Lithuanian Minister of Foreign Affairs, Gabrielius Landsbergis noted: "Nowadays, the most obvious 'front line' of authoritarianism – the border between the free world and the enslaved zones – is located in Ukraine. Putin does not even hide that his war is not against Ukraine, but against democracy as such, which he calls the 'collective West'. Autocrats try to create the illusion that they are the future and seek to rebuild the international order according to their own imagination" (Ministerstwo Spraw Zagranicznych Republiki Litewskiej 2022).

Analysing the above trend, which mobilizes supporters of democracy and coordinates actions to increase resistance to authoritarianism, it is clear that it becomes even more relevant after Russia began the war in Ukraine and the intensification of the interaction of authoritarian forces of such regimes as China, Iran, Syria, Venezuela, Belarus and Hungary.

The classical approach assumes that armoured democracy can be seen as a useful category, both theoretical and practical, whose main goal is to preserve the regime by legally eliminating its opponents. They can (and do) affect (aggressively) fundamental civil rights and freedoms, including freedom of the press. From a historical point of view, we have never seen such a large number of Democratic states that stand in solidarity and unite to successfully use the latest tools of armoured democracy. This will be relevant in the context of future electoral processes, and especially during the election campaign period, when autocrats, populists or foreign forces will try to violate, undermine and even interfere in democratic elections. It also means that armoured democracy is experiencing its renaissance (this concept has lost popularity in the last few decades).

The idea behind the fight against disinformation is that any enemy of democracy who wants to use the media for their own purposes can be immediately removed from access. The first step towards this is the fact that social networks themselves and state services increasingly monitor the activity of users of the network, which undoubtedly represents an invaluable information value for its protection. The interest in and tracking of social networking content is also not concealed by US law enforcement agencies, which view such efforts as a form of identification and early warning of any threats to public and national security (Waters 2012).

It is tempting to design a version of the armoured information model, on the basis of which any member of the executive branch proposing to restrict media freedom, judicial independence or the freedoms of civil society organisations would automatically lose access to the media. In contrast, the information monitoring system may be of concern to online privacy advocates because, under the proposed model, it will be designed to increasingly monitor specific individuals – which will serve to detect content that could signal activities that threaten democracy and its order. However, it is necessary to pay attention to many details. First, this practice clearly resembles the methods used during the Cold War, through which the content of Foreign Press articles or radio and television broadcasts was subjected to similar analysis when the West defended its political system against the communist system (CBC 2012). Secondly, the potential manipulations of virtual networks that occur do not remain within the exclusive reach of government special services. Indeed, access to *spyware* (shortened equivalent to *spy software*), which enables the collection and processing of information about users' activities without their approval, can be found in the case of political and economic actors as well as private network users (Mider 2008: 353). Third, social media – despite the freedom to choose information channels – reinforces polarizing tendencies in the perception of reality, thereby limiting the informational dimension of the media. The tendency to limit the field of establishing relations and searching for information only to a group of people and views similar to our own will make it possible to divide citizens into those with authoritarian views and those with democratic views.

The negative and positive features of the design of this model were presented one after another, but they are interdependent. Although each proposal can be implemented on its own, it is suggested that many of them can act as a supplement rather than a substitute. Moreover, the *de facto* independence of social networks in the pragmatic dimension of obtaining data from microblogging platforms finds confirmation in real situations of a political nature. It seems that the optimal solution is cooperation with political actors, which may be a necessary condition for the implementation of the concept of armoured information as an element of armoured democracy. Hence the idea that the state and private sectors can jointly develop effective mechanisms and ways to combat disinformation, which may in the long term determine the effects of electoral competition, as well as their impact on the political consciousness of users who remain the object of manipulation and verbiage. Not surprisingly, it is becoming increasingly common for state services to intervene and become more active on social media. It is highly likely that this phenomenon will intensify, as from year to year we notice the increased activity of the Kremlin in the use of multidimensional hybrid activities (informational, military, political, economic) in order to influence the results of elections in different countries.

7. Three-dimensional model of armoured information

Institutional environment (micro-scale)

As regards the desirable features of the armoured information model, it is to be assumed that the activity of social organisations and citizens interested in cooperation will be important in order to ensure the fairness of the electoral process in the coming years. In addition, the creation and expansion of so-called state and international institutional cooperation is important in such a model. It will be important to centralise the leadership structure responsible for responding to the cyber crisis situation in a given country, for the overall cyber security strategy and its coordination. Following the example of Estonia, within the framework of government administration, separate cells responsible for managing cyber crises can be created.

Education and infrastructure environment (micro-scale)

A further element of such a model will be the adoption of a comprehensive and inclusive agenda, favouring non-governmental actors, which should play an important and active role in cyber crisis situations. To this end, governments should place particular emphasis on mobilising civil society by devoting a significant part of the state budget to educating citizens about risks and promoting an understanding of the essence of information.

International environment (macro-scale)

An important element of the proposed model is also the interaction of a given democratic state with the international community. To this end, political elites need to build international cooperation in the cybersecurity sphere and even encourage citizens of other countries to become volunteers, among others, enabling them to build a digital identity under the vision: “a country without borders.”

Parallel considerations relate to the development and promotion of international information security mechanisms, including in bilateral, regional and multilateral institutions between regional democratic states. This can be expressed by seeking to build relationships between government departments to strengthen links between each country’s central cybersecurity coordinating bodies and by regularly exchanging information on good practices in protecting national critical infrastructure. It will also be important for the EU to take a position on unacceptable interference in elections and disinformation and develop legislation to prevent hybrid threats.

Armoured information activities are part of a broader strategy that can achieve the following effects:

1. A new way of fighting authoritarian forces.
2. Stopping the expansion of the wave of populists and autocrats to other countries or regions in the geopolitical dimension.
3. Development of international cooperation between democratic states based on bilateral relations and at the level of collegial supranational institutions; the European region as a community of armoured democracy.
4. Integration and activity of social organizations and citizens to strengthen the sense of civic community; citizens will become better consumers/recipients of news, and awareness of democratic mechanisms will increase.
5. Strengthening the democratic society of the EU.
6. Strengthening the democratic character of elections and their procedures and the quality of democracy in the country.

8. Discussion

The following table shows the similarities and differences between armoured democracy, armoured constitutionalism, and armoured information. The most significant common element is the desire of all three concepts to preserve the *status quo* of the democratic system. If democracy is protected by the constitution and information (i.e. freedom of speech), it can be argued that armoured information is a more comprehensive and flexible concept. But if we compare the time of implementation of this action in all three concepts, as presented in the table, it becomes clear that they have a completely different goal.

Table. Main features of armoured democracy, armoured Constitution and armoured information

Concept	Armoured democracy	Armoured constitution	Armoured information
Primary objective:	preserving democracy	preserving democracy	preserving democracy
Actions in the long term:	fighting anti-democratic forces before they become too strong	preventing the government from violating the constitution	prevention of activity of anti--democratic forces in virtual space
Protecting democracy from actors:	enemies of democracy, government	governments that seek to violate the constitution or use it for their particular purposes; various actors, including the judiciary, civil society, press	enemies of democracy, foreign services, populists, state and private actors (trolls)
Methods of struggle:	prohibition of parties (and possibly other associations); restriction of freedom of speech; restriction of the right to association	difficulties in amending the constitution; strengthening the veto; introduction of a parliamentary system at the expense of the president	surveillance by security services and social organisations of profiles and accounts on social networks of undemocratic entities (deleting accounts and posts, banning); active and regular activities aimed at informing about entities (non--democratic forces), their activities and activities in the internet space; restriction of freedom of expression

Source: own study.

While armoured democracy aims to prevent anti-democratic forces from coming to power, armoured constitutionalism tries to design the constitutional order in such a way that it can withstand anti-democratic actions on the part of officials. The task of armoured information, on the other hand, is to prevent the activity of anti-democratic forces, thereby limiting the field of action and depriving them of the necessary means to realize their intentions.

It should be noted that in the literature of the subject, a lot of space has already been devoted to the discussion of possible abuses in an armoured democracy. Possible misuse of armoured information should also be considered. First, the authorities of social platforms and state services have the power to interfere with the content processed by millions of users. Secondly, such powers bring tangible benefits in terms of content security.

Thirdly, these actors have the ability to take control of a person, social groups and even states.

It is important to clearly articulate a set of assumptions that have been at the heart of any consideration so far, namely that the information to be protected serves to protect the interests not only of a powerful elite but also of the state and its social system, which should be adopted through fair and transparent procedures. It is also important that the protection of information is widely seen as right and necessary.

As indicated at the beginning of this article, there are countries that have already adopted all the features of the armoured information model proposed by the author (i.e. Estonia); others are at the stage of consideration or implementation (in particular EU countries). Systematic data on their use are already available. Since the annexation of Crimea by Russia in 2014 and the subsequent invasion of Ukraine in 2022, this process has definitely accelerated and democratic states are considering what legal, institutional or technical solutions should be put in place to safeguard the integrity of the electoral process and the quality of the democratic system. It is also important to specify (challenges) previously proposed design features for the armoured information model in the context of restrictions on freedom of speech:

1. **from a technical point of view**, it concerns the restriction of activity on social networks (e.g., through limits on followers and observations, posting, likes/follows, use of #hashtags; limits on video posts, comments and commenting, accounts, news settings; rules on live streaming; message limit);
2. **from a legal point of view**, internet companies and those involved in the social media field, in cooperation with political actors and social organisations, will be forced in countering disinformation to create a legal framework to combat hybrid threats;
3. **from a political point of view**, it will become important to find effective diplomatic means, especially among EU countries, in building a collective defence, taking into account a range of political, historical and cultural factors;
4. **from a social point of view**, public education and confidence-building in political and private institutions will be important.

Conclusions

The proposed model of the concept of armoured information is aimed at limiting damage and neutralizing the impact of anti-democratic forces. However, armoured information may differ conceptually from armoured democracy, which seeks to keep enemies of democracy out of government. At the same time, it may represent a new method of combating authoritarian internal or external forces.

This article has also attempted to present this concept as a process that can be methodically implemented and which, in order to protect the political system, will inevitably progress on a global scale. This analysis also attempts to determine the effectiveness of the proposed concept in identifying (suggesting) the essential features of such a model to make it resistant to the reliability of Information (media) in such a way that it is less susceptible to internal and external interference. Among other things, a three-dimensional model of armoured information was proposed, which would be based on three dimensions: the institutional environment, the educational-infrastructural environment and the international environment. This model assumes a comprehensive and integrated system of strategy for building armoured information in a given state.

In order to estimate the effects empirically as a unit of analysis, a period is taken in which individual leaders remain at the helm of the government without interruption. The effectiveness of many of the proposed features of such a model could not be demonstrated empirically. Of particular importance are the many factors of information resilience that have been presented and evaluated in this analysis, and all this brings us closer to a concept that is gradually becoming more important in practice.

The proposed simple empirical model may not be able to capture the complexity of constraints in the real world. Its effectiveness depends on the introduction of strategically important elements of the constitutional, technical, political and social order. Although this analysis has attempted to capture different levels of complexity by examining the effectiveness of the implementation of armoured democracy. It becomes important to further study this problem in different groups of countries. In fact, it may be necessary to analyse the actual institutions to ultimately find any effects. Therefore, future research should also address whether legal, institutional, political (international) and social practices are crucial to the implementation of the proposed model: if trust between government and citizens is sufficiently high, detailed and long, then constitutional provisions or technical aspects may be unnecessary.

References

Bäcker, R., J. Rak (2019), *Trajektoria trwania opancerzonych demokracji* [The Trajectory of Armoured Democracies], „Studia nad Autorytaryzmem i Totalitaryzmem" 41(3): 63–82.

Bankier.pl (2022), *Facebook, YouTube i Google blokują rosyjskie media państwowe. Inni szykują się do blokady* [Facebook, YouTube and Google Block Russian State Media. Others Are Preparing to Block], https://www.bankier.pl/wiadomosc/Amerykanscy-giganci-technologiczni-blokuja-rosyjskie-media-panstwowe-8289327.html (5.04.2023).

Butcher, P. (2019), *Disinformation and Democracy: The Home Front in the Information War*, „European Policy Centre," https://www.epc.eu/content/PDF/2019/190130_Disinformationdemocracy_PB.pdf (5.05.2023).

Bryjka, F. (2022), *Rosyjska dezinformacja na temat ataku na Ukrainę* [Russian Disinformation on the Attack on Ukraine], Polski Instytut Spraw Międzynarodowych. Komentarz [The Polish Institute of International Affairs. Commentary], https://pism.pl/publikacje/rosyjska-dezinformacja-na-temat-ataku-na-ukraine (5.06.2023).

CBC (2012), *FBI Seeks Social Media Data Mining Tool*, http://www.cbc.ca/news/technology/story/2012/02/13/technology-fbi-social-media-app.html?cmp=rss&partner=skygrid (5.06.2023).

Contiades, X., A. Fotiadou (2013), *Models of Constitutional Change*, [in:] X. Contiades (ed.), *Engineering Constitutional Change: A Comparative Perspective on Europe*, Canada and the USA, (London–New York: Routledge): 417–468.

dailyweb.pl (2022), *Twitter włącza w Europie geoblokady dla rosyjskich mediów* [Twitter Turns on Geoblocks for Russian Media in Europe], https://dailyweb.pl/twitter-wlacza-w-europie-geoblokady-dla-rosyjskich-mediow/ (5.06.2023).

Dziennik.pl (2021), *USA blokuje strony internetowe irańskich mediów państwowych* [US Blocks Iranian State Media Websites], https://technologia.dziennik.pl/internet/artykuly/8195847,usa-blokada-strony-internetowe-iran.html (7.06.2023).

Fraszka, B. (2020), *Państwa bałtyckie a rosyjskie zagrożenie* [The Baltic States and the Russian Threat], Warsaw Institute. Raporty specjalne, https://warsawinstitute.org/pl/panstwa-baltyckie-rosyjskie-zagrozenia-hybrydowe/ (7.06.2023).

Kuchta-Nykiel, M. (2017), *Ograniczanie wolności internetu i social media. Co władza może zrobić, by utrudnić komunikację?* [Restricting Internet and Social Media Freedom. What Can the Authorities Do to Hinder Communication?], https://socialpress.pl/2017/07/ograniczanie-wolnosci-internetu-i-social-media-co-wladza-moze-zrobic-by-utrudnic-komunikacje (16.06.2023).

Landau, D., R. Dixon (2015), Constraining Constitutional Change, „Wake Forest Law Review" 50(4): 859–890.

Legucka, A. (2022), *Russian Disinformation: Old Tactics and New Narratives*, [in:] A. Legucka, R. Kupiecki (eds.), *Disinformation, Narratives and Memory Politics in Russia and Belarus*, (Abingdon-on-Thames–New York: Routledge). DOI: 10.4324/9781003281597-3.

Liberini, F., M. Redoano, A. Russo, Á. Cuevas, R. Cuevas (2020), *Politics in the Facebook Era. Evidence from the 2016 US Presidential Elections*, CESifo Working Paper, (Munich: Center for Economic Studies and Ifo Institute).

Loewenstein, K. (1937a), *Militant Democracy and Fundamental Rights*, ,,I. American Political Science Review" 31(3): 417–432.

Loewenstein, K. (1937b), *Militant Democracy and Fundamental Rights*, ,,II. American Political Science Review" 31(4): 638–658.

Łukasik-Turecka, A., M. Malužinas (2023), *Digital Disinformation During the 2020 Parliamentary Elections in Lithuania*, [in:] M. Musiał-Karg, Ó.G. Luengo, *Digital Communication and Populism in Times of Covid-19. Cases, Strategies, Examples*, (Cham: Springer): 75-89. DOI: https://doi.org/10.1007/978-3-031-33716-1_6.

Ministerstwo Spraw Zagranicznych Republiki Litewskiej [Ministry of Foreign Affairs of the Republic of Lithuania] (2022), *W Wilnie oficjalnie utworzono kohortę, która zwiększy odporność na autorytaryzm* [A Cohort Has Been Officially Formed in Vilnius to Increase Resistance to Authoritarianism], https://urm.lt/default/pl/news/w-wilnie-oficjalnie-utworzono-kohorte-ktra-zwiekszy-odporno-na-autorytaryzm (9.06.2023).

Mider, W. (2008), *Partycypacja polityczna w internecie. Studium politologiczne* [Political Participation on the Internet. A Political Science Study], (Warszawa: Dom Wydawniczy Elipsa).

Musiał-Karg, M., A. Łukasik-Turecka (2023), *Disinformation in the Media Space during the War in Ukraine: How did Kremlin's Fake News Blame Ukraine, the USA and NATO for the Invasion*, [in:] M. Musiał-Karg, N. Lubik-Reczek (eds.), *The War in Ukraine. (Dis)Information-Perception-Attitudes*, (Berlin: Peter Lang): 13–38.

Polsatnews.pl (2021), *Facebook na dwa lata zablokował konto Donalda Trumpa* [Facebook Blocked Donald Trump's Account For Two Years], https://www.polsatnews.pl/wiadomosc/2021-06-05/facebook-na-dwa-lata-zablokowal-konto-donalda-trumpa/ (6.05.2023).

Schopflin, G. (1994), *Postcommunism: The Problems of Democratic Construction*, ,,Deadalus" 123(3).

Świerczek, M. (2019), *Maki-Miraż, czyli sowiecka sztuka dezinformacji* [Maki-Miraz, or the Soviet Art of Disinformation], ,,Przegląd Bezpieczeństwa Wewnętrznego" 21: 191–207.

(U)Report (2016) of the Report 116-XX Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 2: Russia's use of Social Media with Additional

Views, https://www.intelligence.senate.gov/sites/default/files/documents/ReportVolume2.pdf (15.06.2023).

Waters, G. (2012), *Social Media and Law Enforcement. Potential Risks*, „FBI Law Enforcement Bulletin" 11, http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2012/socialmedia-and-law-enforcement (15.06.2023).

Visualcapitalist (2022), Mapped: The State of Global Democracy in 2022, https://www.visualcapitalist.com/mapped-the-state-of-global-democracy-2022/ (15.06.2023).