sciendo

Hybrid Warfare through Interference in Electoral Processes Using Advanced Technology and Its Impact on Global Security. Case Study: The 2024 Romanian Presidential Election

Eugen GABOR*
National University of Political Studies and Public Administration (SNSPA), Bucharest, Romania
**Corresponding author, eugen.gabor24@gmail.com*

Marian OANCEA
The Bucharest University of Economic Studies (ASE), Bucharest, Romania
marian.oancea@fabiz.ase.ro

Vladimir PRIPP
University of Bucharest (UB), Bucharest, Romania
vladimir.pripp@s.unibuc.ro

Abstract. *In the 21st century, the climate of the geopolitical arena is significantly more volatile than for most of the second half of the 20th century. Asymmetrical threats generated mainly but not exclusively by non-state entities compelled regional and worldwide forces to reevaluate their main security strategies. Moreover, several state entities that are highly relevant to managing global issues engaged in much more unpredictable behavior than usual. The spectacular technological developments of the last two decades, which seem to evolve in an exponential manner, created new tools for those who aim to alter the geostrategic status quo through hybrid warfare actions. The main goal of our study is to present some preliminary conclusions on the impact that the use of new technologies by hostile foreign forces in electoral processes can have on the institutional architecture that at least in some parts of the globe managed to ensure a stable and secure environment for several decades. These conclusions are drawn through a case study that analyzes the recent annulment of the first round of the Romanian presidential election. Although many details of this event are not yet clarified, at least for public opinion, the available information clearly suggests that hybrid warfare through new technologies is able to create mistrust and sever links that are vital for ensuring stability both at a national and international level. The Romanian case proves that the main objective of interferences in elections is not always that of helping a certain candidate to win but creating chaos.*

Keywords: new technologies, hybrid warfare, global security, elections, Romania, foreign interference.

Introduction

Global security was shaken in the last years by events that resemble practices from the darkest periods of the 20th century. Russia's overt invasion of Ukraine, started on February 24th, 2022, or Hamas' terror attack launched on October 7, 2023, and the war that ensued prove that the use of military force is still a main instrument on the global geopolitical arena, regardless of the suffering and destruction that it causes. On the other hand, hybrid warfare actions are on the rise as well. Often operations meant to alter the manner in which the public views certain political, social, or economic phenomena can be just as efficient for reaching certain goals as military

DOI: 10.2478/picbe-2025-0138

campaigns. These operations are becoming more and more sophisticated and successful because technological innovation constantly provides them with new tools.

The crises of contemporary liberal democracies can be enhanced by the risks that accompany the constantly growing participation of citizens in the digital environment (Chilvers & Kearnes, 2019, p. 3). Unattended, these risks are poised to grow in the next years, given that the younger generations are relying more than ever on the new instruments that technological innovation provides to them (Boulianne & Teocharis, 2020).

Artificial Intelligence (AI) plays a central role in the latest developments of new technologies, with generative models like ChatGPT disrupting patterns of action in various aspects of social and economic life. Besides numerous advantages, the proliferation of AI models also brings diverse threaths regarding ethics, privacy, and security (Wach et al., 2023, p. 9). A large language model (LLM) like GPT-3, an upgraded version of ChatGPT, can develop certain ideological biases, therefore influencing the users (Gover, 2023). Moreover, as we will see below, this kind of model can be used for building messages for mass guerilla political campaigns.

In the cyber world, another major innovation is represented by the emergence of the Metaverse, which is described as *"...a compound word of transcendence meta and universe and refers to a three-dimensional virtual world where avatars engage in political, economic, social, and cultural activities. It is widely used in the sense of a virtual world based on daily life where both the real and the unreal coexist."* (Park & Kim, 2022, p. 4211) The Metaverse can be associated with augmented reality (AR) or virtual reality technologies (VR) but has a social meaning, being able to accommodate a large number of people (Park & Kim, 2022, p. 4210). Although it does not yet have the same impact on the political environment as large language models like ChatGPT, the Metaverse could become in the future both a political actor and a political battleground.

We mentioned above that AI tools are being used for drafting political messages that can be used for manipulating voters. At the same time, AI can be used for generating images or audio and video materials in order to trick the audience into believing a false political narrative. The main goal of such a product, named *deepfake*, is to convince the voter of its authenticity. More precisely, the concept of *deepfake "...is a combination of the words "deep learning" and "fake," and primarily relates to content generated by an artificial neural network, a branch of machine learning."* (Mirsky & Lee, 2020, p.7)

The main goal of our paper is to analyze the manner in which technology is used in hybrid warfare actions that can have a negative impact on global security. Firstly, we present briefly our methodological approach and we establish a theoretical background by focusing on two of the main concepts of our study: hybrid warfare and global security. Secondly, we realize a case study around the alleged foreign interference in the 2024 Romanian presidential election. Our conclusions are built on the main features of this peculiar succession of events.

Methodology

The main research method is the case study, because it *"focuses on a recent phenomenon, which has a complex structure, making it difficult to be extracted from context"* (Chelcea, 2007, p.600)., This case study is "an individual case study" (Ibidem, p.602), because we are concentrating on an individual event, the 2024 Romanian Presidential Election, which can be analyzed from a longitudinal perspective "*allowing us to see the case in different moments of its evolution"* (Ibidem) and which is also revelatory, because the use of cyberturfing in political campaigns has

not been thoroughly researched. Since their appearance, social networks have been used as means of promotion for both individuals, such as political candidates and organizations, such as corporations and political parties. Even though hybrid warfare is not a new phenomenon, it is a very complex one, which is continuously evolving, employing new technologies, such as cyberturfing. Thus, the nature of this research is rather descriptive, with the main purpose of gathering as much information as possible, in order to *"explain the less known"* (Mitulescu, 2011, p.35) influences of cyber-warfare onto elections. The main sources are official reports issued by foreign and domestic institutions and press investigations.

Hybrid Warfare

War, as any other human activity, has continuously evolved, due to technological advancement, and is no longer waged only with soldiers manning guns. The term "hybrid warfare" illustrates the evolution of conflicts, which are incorporating *"new combination of features that were not as strategically prevalent in previous wars"* (Mumford & Carlucci, 2022, p. 194).

All the modern technologies used to wage unconventional forms of warfare in the third millennium fall within Ofer Fridman's definition of hybrid conflict, which use *"newly available technologies to influence the hearts and minds of targeted audiences"*. (Fridman, Kabernik, & Pearce, 2019, p.1) and is characterized by the *"unique combinational or hybrid threats specifically targeting U.S. vulnerabilities"* (Hoffman , 2014, p.330). Even though the author is referring directly to the US, this form of warfare can affect any country, especially the Western ones, which are the preferred and most vulnerable targets of hybrid warfare, because they are *"open, pluralistic and liberal societies with freedom of the press and rule of law"* (Weissmann, Nilsson, Thunholm, & Palmertz, 2021, p.2).

In modern times, not only the ways in which wars are being waged has changed, but also the belligerents. Hybrid warfare can be waged by *"any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the battlespace to obtain their political objectives"* (Hoffman, 2010, p.443), which *"may involve both state and non-state actors"* (Almäng, 2019, p.4). Another important characteristic illustrated by Hoffman is that hybrid war tactics can be employed by multiple actors at the same time: "*we can expect to face competitors who will employ all forms of war and tactics, perhaps simultaneously"* (Hoffman, 2014, p.330). This trait is important because it highlights the fact that during hybrid warfare, a nation can be under attack from multiple enemies/belligerents that might not necessarily cooperate or be part of the same alliance, making it harder for the besieged nation to defend itself and to counterattack. However, even though they are distinctive enemies, their attacks are most successful when they focus on the same target at the same time, *"employ all forms of war and tactics, perhaps simultaneously"* (Ibidem).

Local criminal networks are one of the structures which can be used by foreign powers or non-state actors in order to obtain leverage during hybrid confrontations for *"either strategic and financial gains"* (Long, 2024, p.87). Firstly, state or non-state foreign actors rely on international criminal organizations in order to surveil, kidnap, or even harm persons of interest all over the world (Miller, Mekhennet, & Brown, 2024). Secondly, these organizations can be engaged in lucrative financial operations, such as *"drug and human trafficking, child pornography, identity theft, copyright piracy, cybercrime and [...] looting of historical artefacts*" (Goertz & Streitparth, 2019, p. 45) which, on one hand, improve the finances of non-state hybrid warfare belligerents, such as terrorist organizations, which are either providing or acquiring from criminal organizations drugs or weapons. As tools within the hybrid warfare, criminal organization help not only non-

state actors, but also other foreign nations, by contributing to social instability, generated by violence, pushing drugs and economic instability, which, in turn, lead to *"destabilising a political system and at questioning the legitimacy of a government"* (Ibidem, p. 120).

In modern times, information has become a major weapon in hybrid warfare, especially due to the fact that technology, which is an integrated part of most peoples' lives, grants us access to vast sources of news and data, thus increasing the *"danger posed by non-military means and methods of political struggle"* (Fridman, Kabernik, & Pearce, 2019). Through the use of information networks, which allow disinformation to *"to be disseminated much further and much faster than ever before"* (Ibidem), hybrid warfare can employ a large spectrum of instruments, starting from the seemingly harmless *"political satires, news parodies, [...] and misleading advertising"* (Jayakumar, Ang, & Anwar, 2021, p. 19), which, in turn, might lead to *"propaganda and psychological warfare"* (Fridman, Kabernik, & Pearce, 2019, p. 225). The way in which people access information has also changed. Nowadays, classical news sources are perceived as being unreliable. On average, less than half of the Europeans trust standard news sources, such as national radio and TV stations (48%), newspapers (38%), while less than a third trust private Radio and TV Stations (28%) (European Parliament, 2023). After ditching newspapers, radio and TV stations, people embraced social networks as their novel news source, a process which *"blurred the lines even further between news and opinion"* (Mcintyre, 2018, p.93), because they are not accessing objective information, but biased personal opinions expressed by influencers or self-declared experts in various fields.

People who use social networks as a news source are limiting their informational outreach, by unfriending those *"who disagree with their political opinions"* (Mcintyre, 2018, p.94), obtaining a biased, polarized opinion. In the hybrid warfare, social networks represent a fertile ground for disinformation not only due to the aforementioned tendency of polarization but also because it's because are allowing *"anyone to report, film, or manufacture "facts" or "news" and make it available to the general public."* (Atkinson, 2018, p.69) and don't always provide the proper tools in order to identify and eliminate the false information. Fake news on social media can occur on two different instances. Fake news can either be *"produced purposefully [...] by those seeking to make money from advertising"* (Maheshwari, 2016) or be the result of *"misinformed social media posts"* (Ibidem).

Besides fake news, another important facet of the digital side of hybrid warfare is cyber-warfare, characterized by *"the use of cyber-attacks with a warfare-like intent"* (Robinson, Jones, & Janicke, 2015), which are mostly directed against *"sophisticated technological civilizations of the West"* (Gartzke, 2013, p. 41), with stronger military capabilities, which are nearly impossible to defeat through traditional warfare. However, cyber-attacks can also be inflicted onto non-military targets, which are less capable of defending themselves. The most dangerous cyber threats are *"espionage, crime, cyber war, and cyber terrorism"* (Nye, 2010, p.16). The first threat refers to obtaining sensitive information or secrets by employing different digital techniques without raising alarms, *"making it difficult to deter or capture cyber spies"* (Gartzke, 2013, p. 70) or to prove what country or organization was the perpetrator. Digital crimes refer to acts such as "*the spread of viruses or other malware, hacking and distributed denial of service (DDoS) attacks."* (McGuire & Dowling, 2013, p.3) which can be targeting individuals, private companies, or state actors/organizations. Cyber-war is less broad than cyber-warfare, and strictly refers to *"conducting, military operations [...] disrupting if not destroying the information and communications systems"* (Arquilla & Ronfeldt, 1993). Historically speaking, cyber-war is proven to have two major uses. On one hand, its purpose is to *"disable the enemy's defenses"*,

facilitating the military operation's success. Secondly, it is meant to promote propaganda, in order *"to demoralize the enemy, distributing e-mails and other Internet media in place of [...] dropping pamphlets."* (Ibidem). Lastly, cyber terrorism is characterized by *"cyber-attacks where the intent is to intimidate or coerce a civilian population, the policy of a government [...] or affect the conduct of a government"* (Robinson, Jones, & Janicke, 2015, p. 76). The aftermath of the attack is also important for propaganda purposes, because it highlights the strength of the attacker and the weakness of the victim. Moreover, it can be interpreted as a rallying call, for non-state actors to gather support and new members, by providing *"fertile ground for the rise of radical ideas"* (Kapsakoli, 2023, p.61).

In the cyber-warfare, state institutions are not affected only by the direct attacks as the ones previously illustrated. Their authority might be undermined by citizen's negative opinions and actions, which, in turn, might be influenced by disinformation campaigns organized by foreign or domestic, state or non-state entities.

The practice of astroturfing refer to *"business-backed grassroots campaigns [...] (i.e., fake grassroots), especially when they involve participation that is heavily incentivized"* (Walker & Rea, 2014, p. 293), in order to *"gain mass acceptance for a commercial benefit or a political ideology*" (Leiser, 2016, p. 4). Those who support this kind of voter propaganda are directly influencing citizens' rightful involvement within the electoral system, not only influencing their vote, but also their intent of participating in the electoral process or other civic actions, such as protests, boycotts etc. This form of manipulation has three distinct actors. First, there are the victims, citizens whose attitudes are affected. Secondly, there are the *sellers*, *"paid agents to falsely represent popular sentiment surrounding a product or service"* (Ibidem). Lastly, there are the *investors*, internal or external actors who are financing the operation. Astroturfing is part of disinformation efforts not because of the transmitted message, which can illustrate the truth, but due to the fact that it generates *"the false impression of independent popular support"* (Keller, Schoch, Stier, & Yang, 2019, p.2).

Cyberturfing, a term that illustrates the online equivalent of astroturfing (Leiser, 2016, p.4), has great implications for the democratic functioning of a country. On one hand, it has a positive impact, by promoting and supporting groups fighting for democracy and social justice (Chan, 2022). On the other hand, it can be used to disseminate false information and messages of hatred towards minorities or denigrate political competitors. Due to the fact that social media became the major source of information for the general public, not only mainstream or extremist political actors, but also *"hyperpartisan media, far-right groups or actors with economic motives"* (Keller, Schoch, Stier, & Yang, 2019, p.2) are using cyberturfing in order to influence people's perception.

Global security after the Cold War

Global security refers, first and foremost, to possessing the military capabilities of protecting the lives and well-being of citizens and the vital political and economic interests of the political entities that encompass these citizens, at a global level. However, the military aspect is not the only one to be taken into account when this concept is analyzed. For instance, especially since the end of the 20th century, elements like the environment can be included in the discussion (Meder, 2008, p. 9). Moreover, global security can be gravely endangered by the lack of social justice, which can be enhanced by cultural perspectives that disregard fundamental human rights (Davis, 2008, p. 137). In such conditions, developing new military instruments might not ensure stability without proper social expenditures (Rogers, 2012, p. 12). Additional elements that have a

growing importance are food security, bio-security, or health security (White & Davies-Bright, 2021, pp. 19-20)

The latest waves (fourth and fifth) of the industrial revolution are also influencing the above-mentioned landscape. New technologies can be weaponized by those who aim to alter the geopolitical status quo (Gabor, Oancea & Pripp, 2023). The current trends indicate that in the following decades the importance of the fruits of technological innovation (artificial intelligence, big data, robotics, biosciences, 3D printing, nanoengineering, etc.) will continue to grow (Manning, 2020, pp. 1-2).

Digital tools are becoming vital not only for the military but also for activities of hybrid warfare like the ones described in the previous section. Instead of contributing to the building of a more stable and prosperous world order, they are fueling a geopolitical storm that undermines the pillars of the international institutional architecture that managed to neutralize major threats to global peace for several decades. This stark reality is enabled by a renewal of political and economic rivalries that once seemed to belong to the past. Francis Fukuyama (1992) considered shortly after the end of the Cold War (1947-1991) that a gradual universalization of liberal democracy and free market economy is unavoidable. Although it is argued that some of Fukuyama's conclusions might have been misinterpreted, it is clear that this type of optimism characterized the post-Cold War intellectual environment, at least until September 2001. More recently, even Fukuyama (2023) highlights that an age of instability replaced the unipolar order that emerged after 1991. On the other hand, Samuel P. Huntington (1996) quickly observed that the ideological bipolarity of the Cold War could be replaced by a multipolar landscape organized around cultural boundaries.

Therefore, for at least two decades, the level of unpredictability in the global political arena has been growing. The new multilateralisms are complicating the efforts of building mechanisms of global governance. A collective insecurity is becoming an unintended consequence of globalization (MacLean, Black & Shaw, 2006, pp. 3-10). Removing this insecurity is a difficult task for various reasons. For example, flaws in the conception or management of international institutions are limiting the possibilities of preventing military or hybrid conflicts. The United Nations (UN), according to Article 1 of the UN Charter, has the responsibility of removing the threats to global or regional peace. However, there are no practical instruments created to ensure that this target is achievable. The UN Security Council, which should handle this kind of cases, is often rendered useless by geopolitical rivalries (Mack & Furlong, 2004, p. 59). Five members of the Security Council (the United States of America, the United Kingdom, France, the Russian Federation, and China) retain veto power since the creation of the institution, which is described as incompatible with a democratic international order (Niemetz, 2015, p. 74).

Global security, given that Fukuyama's theory of the end of history was factually disproven, is further influenced by ideological forces and transformations. Therefore, both global and national security are linked to ideological security. For instance, the Chinese government prioritizes the protection of the ideological pillars of the regime in its strategic approach to international relations. Moreover, according to the Xi administration, the main ideological traits of China ought to be not only preserved but also exported (Segal & Fitz-Gerald, 2021, p. 4). This philosophy underlines the fact that we have not yet entered a post-ideological era, although, obviously, the new technologies and the integrated global value chains altered significantly the geostrategic landscape inherited from the 20th century (Blanchette, 2020). The promoters of liberal democracies and of an international order based on fundamental human rights should also

put forward a clear ideological agenda. Otherwise, protecting open societies worldwide and securing a peaceful climate could become an even more difficult task. Global security would benefit from the implementation of an updated version of the Helsinki Final Act (1975), which started to impose the upholding of human freedoms as a standard international practice (Sletzinger, 2014).

An essential element in any debate regarding global security is the fact that, just as Benjamin Franklin affirmed more than two centuries ago, security mustn't be obtained by sacrificing liberties. Neutralizing military or hybrid threats must be done in a manner that preserves vital rights, like *"...the right to life, the right to sustenance, the right to an income, the right to healthcare, the right to an identity..."* (Hamourtziadou, 2020, p. 121) At the same time, it must be taken into account that maintaining a peaceful and stable order requires not only collaboration between states but also the involvement of entitities that are acting below and beyond the level of the state (Schroeder, 2021, p. 54). Last, but not least, we must emphasize once again the role of technology both in upholding and undermining global security. The cyberspace represents a political, economic, and ideological battleground. Artificial Intelligence (AI) can produce in cyberspace the same advantages that tanks or rockets can produce in fields divided by trenches. The ICT (Information and Communications Technology) infrastructure gradually became an indispensable item in shaping and pursuing foreign policy objectives (Tikk-Ringas, 2015, p. 67) This means that, although classical war is not by any means becoming a historical artifact, hybrid threats to global security require the utmost attention of both political actors and civil society organizations.

Case study: the 2024 Romanian presidential election

Technology was already in the 20th century an important tool in the political arena. The emergence of radio and cinematography had, for instance, a notable role in the development and consolidation of fascist forces (Cannistraro, 1972). Later, television also became part of the political battleground, with debates between candidates often influencing the outcome of elections (Greenberg, 2009). In the last 25 years, the internet and the meteoric rise of social networks further enhanced the grip of technology on politics. The pace of innovation seems to be increasing exponentially. Already in several countries, AI was used in order to modify the manner in which the electorate perceives different candidates or movements (Gabor, Oancea & Pripp, 2024).

In many cases, internal political interests are fueling deceptive acts in which technology plays a key role. However, we also can identify several documented situations in which foreign entities get involved in the politics of another country through new technologies, with the obvious goal of altering the regional or global geopolitical order. The institutional architecture that contributes to maintaining a certain level of global security can be harmed by this type of endeavor.

A famous example is represented by Cambridge Analytica, a US based political communications firm that managed to acquire vast amounts of data regarding a large number of citizens, with a goal that in time was at least partially achieved: modifying their electoral behavior. Such an outcome was possible, among others, because certain social networks had significant shortcomings in conceiving and applying their privacy policies (Kaiser, 2019, p. 9). The lack of regulation of technology companies enables the so-called *surveillance capitalism*, which relies on profiling citizens for advertising purposes (Dawson, 2021, pp. 63-64). In the United Kingdom (UK), Cambridge Analytica contributed to targeted messaging meant to boost

the support for the camp that advocated for leaving the European Union (EU) (Kaiser, 2019, p. 169). These kinds of actions show that labeling Cambridge Analytica as a *psychological warfare firm* is appropriate. According to former employees of the organization, this warfare was conducted in collaboration with foreign entities (Wylie, 2018, p. 8).

According to the United States intelligence agencies, hybrid warfare acts coordinated by geopolitical rivals include cyber activity, overt actions conducted under governmental supervision, and the use of intermediaries, such as the so-called *trolls* that are responsible for disseminating certain narratives online (Galante & Ee, 2018, p. 2). Both the USA and allied states (Germany, the Netherlands, Estonia, Lithuania, etc.) were at some point targets of hybrid attacks. On the other hand, data leaked by controversial figures like Julian Assange or Edward Snowden indicates that the US also used the cyber domain for external intelligence activities. Given that no country can claim that it is immune to cyber threats, agreements like the one adopted by the US and China can act as a factor of deterrence (Shad, 2018, pp. 44-46).

Recently, suspicions regarding foreign hybrid attacks arose around the Croatian presidential election held on 29 December 2024 (the first round) and January 13 2025 (the second round). Croatian researchers identified a disinformation campaign on social media, fueled by fake accounts (bots), some of them having profile pictures generated with AI programs. For instance, one bot posted on Facebook more than 100 messages in a day, aiming to boost the popularity of a candidate that opposes supporting Ukraine's struggle against the Russian invasion launched on February 24th, 2022 (Centre for Information Resilience, 2025). In Germany, parliamentary elections took place on February 23rd, 2025. Bots that are allegedly tied to the Russian Federation were active in the German electoral campaign as well. According to the German Office of Foreign Affairs, sleeper accounts were used to spread AI-generated content meant to create support for political movements that have the potential of undermining the German liberal democratic system (Lunday, 2025). Once again we can notice that new technologies are used for creating and spreading fake news that can have a negative impact on national, regional, and global security.

The information presented above has the role of setting the context of our case study. The hybrid warfare techniques used during the 2024 Romanian presidential election are not unprecedented but have some particularities that distinguish them. Moreover, the outcome of this endeavor is extremely uncommon: the Constitutional Court of Romania (CCR) annulled the first round of the election, cancelling a run-off for which the voting in the diaspora had already started (Anghel, 2024). In the history of the EU, only in one other member state was a similar decision taken: in 2016, the Constitutional Court of Austria annulled the second round of the presidential elections. However, the reason behind this decision was not linked to any hybrid warfare activities. In this case, the defeat of a far-right candidate was nullified because of the improper counting of absentee ballots in several districts (Oltermann, 2016).

The peculiarity of the Romanian 2024 presidential election attracted worldwide attention, both politicians and researchers trying to comprehend the causes and the implications of such a situation. Public figures like J. D. Vance (vice-president of the USA) Elon Musk (billionaire member of the second Donald Trump administration and owner of the X social network), Thierry Breton (former European commissioner), Kaja Kallas (High Representative of the EU for Foreign Policy and Security Policy and former Prime Minister of Estonia), Alexander de Croo (former Belgian Prime Minister), and Viktor Orban (Prime Minister of Hungary) issued various statements regarding this topic (Mihai, 2025; Boga, 2025; Woodward, 2025; Marin, 2025; Coșlea, 2025; Arambescu, 2024). Clearly, there are foreign political actors that aim to replicate

this model and foreign political actors that are trying to shape possible answers to similar scenarios.

In 2024, Romania was governed by a coalition inspired by the German *GroKo* (Christian Democrats and Social Democrats) model. The Social Democratic Party (PSD) and the National Liberal Party (PNL) put aside their apparent ideological differences with the stated goal of ensuring stability and economic and social development. Seen as pillars of the political establishment, these parties presented themselves as protectors of the liberal democracy that can hold off the ascension of extremist forces (Popescu, 2024). Initially, the results of this endeavor seemed more than promising. In an unprecedented move both at the national and European level, PSD (member of the Party of European Socialists - PES) and PNL (member of the European People's Party - EPP) decided to run on a common list at the European elections held in June 2024. Their alliance obtained 48.55% of the votes and 19 of the 33 seats attributed to Romania (Cojan, 2024).

Although the result was more than encouraging, PSD and PNL decided to have separate candidates for the presidential election scheduled for 24 November and 8 December 2024. The incumbent Klaus Iohannis, former president of PNL, was barred from running by a constitutional limit of two terms. In a crowded field of 14 candidates, 4 were independent. One of them, Călin Georgescu (62 years), kept a relatively low-profile in the traditional mass-media and was not involved in large grassroots campaigns that earlier helped right-wing populist movements gain momentum. Nevertheless, he built an online campaign that proved to be really effective, spreading his messages in communities all across the country and the diaspora.

Călin Georgescu's ideological profile contributed to his labeling as a marginal candidate. Many opinion polls conducted in September and October were not measuring the support for him, placing him in the *Other candidate* category (Euronews, 2024; Bancăș, 2024). Although he was mentioned in the public space as a potential prime minister in several occasions, a populist right-wing party declaring its support for him for a brief time (Meseșan, 2020), his level of notoriety was not extremely high. A part of the mainstream media avoided him for several reasons. Firstly, he expressed his admiration for Romanian far-right movements like the interwar Iron Guard. Secondly, he stated that it would be in Romania's best interest to leave the North Atlantic Treaty Organization (NATO) (Bian, 2024). However, later he stated that his declarations were misinterpreted, that he is not against NATO, and that he rejects political extremism (Coman, 2024).

On October 5, the CCR rejected the presidential bid of Diana Șoșoacă (Pantazi & Popescu, 2024), a Member of the European Parliament (MEP) and leader of a radical right-wing party that had several political ideas that resembled those of Georgescu. Although, as far as we know, it is not proven yet in scientific studies that this decision boosted the support for Georgescu, it can be argued that such a decision, even if it was taken on the basis of the Constitution, reduced the trust in the political establishment and helped consolidate a climate that favored outsiders like Georgescu.

The first opinion polls that measured consistent support for Georgescu appeared just a few weeks before the date of the first round (G4Media, 2024; Roman, 2024). However, none of them anticipated that the candidate could qualify for the run-off, his highest number being just slightly above 10%. The results of the first round of the presidential election revealed a completely different image: Călin Georgescu occupied the first place, with 22.94% (2 120 404) of the votes, and therefore qualified for a run-off alongside the president of the center-right Save Romania Union (USR), Elena Lasconi (Gherghiță, 2024). Notably, he obtained the highest number of votes in the diaspora as well (43.16% - 346 103 votes).

Although such a scenario was considered highly unlikely by both sociologists and political analysts, this does not mean *per se* that the electoral process was manipulated or that the candidate and his supporters did something illegal or immoral. So why do we construct a study regarding hybrid warfare and global security around this case? On November 28, just a few days after the first round of the election, a meeting of the Supreme Council of National Defence (CSAT) was held. On December 4, President Klaus Iohannis decided to declassify documents presented in the CSAT meeting by various institutions. These documents do not prove beyond any doubt that Georgescu tried to create an uneven playing field in the election with foreign help. However, there is clear evidence that foreign entities acted in cyberspace in order to influence the outcome of the electoral process with the goal of destabilizing the Romanian political regime and therefore contributing to the modification of the geopolitical status quo.

According to the Romanian Intelligence Service (SRI), a state actor coordinated more than 85 cyber-attacks on the IT&C (Information Technology & Communication) infrastructure that constitutes the backbone of the elections (Secretariatul Consiliului Suprem de Apărare a Țării, 2024a). Information systems from more than 33 countries were used in these attacks, which did not achieve the goal of creating malfunctions in the Romanian IT systems responsible for the electoral process (Secretariatul Consiliului Suprem de Apărare a Țării, 2024b). The nature of the action makes it indeed highly unlikely that a private entity could have been behind this operation. At the same time, although some platforms that were used originated in the Russian Federation, it is difficult to clearly locate the core of the network that operated in this endeavor. Another issue mentioned by a document presented by SRI is that on the Chinese TikTok platform, Călin Georgescu had preferential treatment. While the other candidates had limitations in spreading their messages because they were correctly labeled as political campaigning, Georgescu had no such barriers, being able to reach voters even after the electoral campaign officially came to an end. Apparently, this advantage was not the effect of a deliberate strategy of the platform's coordinators. After the Romanian authorities notified TikTok regarding these issues, the unlawful content was blocked in Romania but remained accessible to users from other countries. However, the content was not deleted and became available once again in Romania after a while. After verifying this case, representatives of TikTok concluded that the dissemination of pro-Georgescu messages on the platform was the effect of a mass guerilla political campaign. Moreover, in November, such a campaign was initiated to boost the popularity of the Party of Young People (POT), which supported Georgescu in the presidential election (Secretariatul Consiliului Suprem de Apărare a Țării, 2024a). This action was meant to influence the outcome of the parliamentary election held on December 1, in which POT ultimately obtained more than 6% of the vote, managing to acquire 31 seats in the legislature (Onofrei, 2024).

The SRI also stated that sleeper accounts were the key for the mass guerilla political campaign. Most of them were activated in the last two weeks of the electoral campaign, making it difficult for the authorities to react and for the public to become aware of the nature of the operation. Overall, more than 25 000 accounts were used. 797 of them were created in 2016, the year in which TikTok was launched. The activity of some of these accounts was coordinated through Telegram groups created in September 2022 (Telegram is an instant-messaging platform founded by Russian entrepreneurs Nikolai and Pavel Durov). Moreover, some of them were linked to the Russian publication *Sputnik* (Secretariatul Consiliului Suprem de Apărare a Țării, 2024c). Although this does not prove beyond any doubt Russia's involvement in this activity, it amplifies the already existing suspicions.

According to the SRI, an important part of the operation developed on TikTok was represented by recruiting influencers that became essential for spreading pro-Georgescu messages that were not labeled as political publicity. For instance, the hashtag #echilibrusiverticalitate (equilibrium and verticality) flooded the feed of Romanian users and contributed to the rise of the candidate's notoriety and favorability. The campaign built around this hashtag was identical with a campaign coordinated earlier in Ukraine by the Russian Federation (Secretariatul Consiliului Suprem de Apărare a Țării, 2024d). Many of the influencers were paid through the *FameUp* platform. More than 100 influencers with more than 8 million active followers were involved in this process. As a result, the hashtags associated with the Georgescu campaign reached 9th place worldwide in the trending tops. On the other hand, fake accounts were created in order to promote the idea that institutions like the Romanian Police or even the SRI were backing Georgescu (Secretariatul Consiliului Suprem de Apărare a Țării, 2024c).

Regarding the funds that fueled this campaign, Georgescu's claim that he had no expenses whatsoever in the entire electoral period produced even more question marks around the nature of his strategy. A Romanian citizen, Bogdan Peșchir, spent more than 1 million euros on TikTok for promoting various videos. Most of this amount was used for spreading pro-Georgescu messages. At least for now, Peșchir cannot justify the provenance of the money. Currently (March 2025), Peșchir is under preventive arrest, being accused of corrupting voters through electronic means of communication (Cîmpean, 2025). He is associated with Gabriel Prodănescu, a Romanian-born South African citizen, who left Romania for Germany before 1989 and settled in South Africa in 1995. It is worth mentioning that some of the influencers were paid 1 000 euros for sharing a video that was part of the pro-Georgescu propaganda through FA Agency, a South African entity (Secretariatul Consiliului Suprem de Apărare a Țării, 2024c). Regarding Prodănescu, it must be underlined that he is involved in crypto-currency businesses, controlling companies from South Africa, Romania, and also the United Kingdom (UK) (Garaiman, 2024). In December, an investigation proved that FA Agency is controlled by the Polish subsidiary of Gambling Media Group (GMG), a company that manages marketing campaigns for online casinos. GMG is linked to a Ukrainian publicity agency named Zlodei. Both GMG and Zlodei are based in Kiev. The latter is controlled by businessmen who were accused by the authorities of money laundering (VIGINUM, 2025, pp. 6-8). It is not known if FA Agency and Zlodei played any other part in the campaign that favored Georgescu other than recruiting influencers. Moreover, for now there are no public proofs that a state coordinated them.

The Foreign Intelligence Service (SIE) stated, without presenting clear links between the Russian Federation and Călin Georgescu, that the Kremlin is responsible for spreading fake news through cross-posting on social media in countries perceived as unfriendly. Especially electoral processes are vulnerable in front of foreign interference. Some of the content that was disseminated was generated through AI programs. Moreover, the proper topics were identified through sociological research conducted in the targeted countries (Secretariatul Consiliului Suprem de Apărare a Țării, 2024e).

The outcome of declassifying this information was the decision taken by the CCR on December 6 to annul the first round of the presidential election, which meant restarting the entire process from ground zero. The judges unanimously concluded that the electoral process was altered by several irregularities, the legislation being intentionally breached through the actions exposed in the above-mentioned reports. For instance, campaign actions were financed in an unlawful manner. Therefore, the competition took place on an uneven playing field, one of the candidates clearly benefitting from the operation that was implemented mainly in cyberspace.

According to the Court, the electoral campaign took place in an environment that lacked transparency, so the election cannot be considered either free or fair. This meant that the democratic character of the Romanian regime, stated in the Constitution, would have been undermined if the results of the election had generated legal consequences (Curtea Constituțională a României, 2024).

The Decision emphasizes that digital technologies and AI tools were vital for the condemned actions. The document does not name the Russian Federation but indicates that the European legislation prohibits using funds from outside the EU for promoting candidates. Regarding TikTok, the judges suggest that the platforms' algorithms were abusively exploited by the architects of the operation (Curtea Constituțională a României, 2024). Therefore, once again it is highlighted that the platform itself is not responsible for what happened.

The conclusion of the Court is that by annulling the election, the institution maintains the fundamental elements of the constitutional order, guaranteeing that Romania remains a democracy and that the rule of law is upheld (Curtea Constituțională a României, 2024). Such a bold and unprecedented statement drew both praise and criticism at home and abroad.

In February 2025, the Service for Vigilance and Protection against Foreign Digital Interference (VIGINUM), a structure that functions under the authority of the French Government, published a report that analyzes how information and influencers were manipulated on TikTok in order to sway the outcome of the 2024 Romanian presidential election. The goal of the report is to warn the French public of the danger of foreign digital interferences in electoral processes and to help the French authorities to prevent or neutralize such endeavors. The document is based on open sources and on investigations conducted by representatives of the Service (VIGINUM, 2025).

VIGINUM observes that TikTok is more popular in Romania than in France and that the foreign interference in the Romanian electoral campaign was built not only through TikTok but also through social networks like Facebook or Instagram, which are part of the Meta conglomerate. On TikTok, in the last two weeks of the electoral campaign, the number of followers of Georgescu's account and the number of views of his videos tripled. Moreover, the #calingeorgescu hashtag had more than 73 million views in just a week. According to the report, this spectacular progress was possible because of a sophisticated astroturfing campaign (the meaning of this concept is detailed below). Once again, the idea that the platform's algorithms were manipulated resurfaces. However, it is stated that the masterminds of the campaign had very detailed knowledge on how TikTok functions.

According to representatives of TikTok, more than 27 000 fake accounts were used to influence the 2024 Romanian elections. Many of these accounts, coordinated through Telegram, posted commentaries on the videos published by the influencers recruited through the *FameUp* platform. Georgescu was not the only candidate that was favored. The populist right-wing Alliance for the Union of Romanians (AUR) was also advantaged by the manipulation of the algorithms. As mentioned above, AUR supported for a brief period Georgescu for the position of Prime Minister. Regarding the entity that ordered the astroturfing campaign, VIGINUM highlights that a clear identity is not yet known, although the Romanian authorities stated that a foreign state was clearly involved (VIGINUM, 2025, p. 5).

One of the conclusions of the report is that the hybrid operation that targeted the 2024 Romanian presidential election represents an upgraded version of similar endeavors that affected, in the same year, parliamentary elections held in Georgia and Moldova. Its main outcome, given

that the CCR annulled the first round of the election held on November 24, is that the trust of the Romanian public in the electoral process was severely damaged (VIGINUM, 2025, p. 12).

On February 26, 2025, prosecutors announced that a criminal case was opened against Călin Georgescu. The former candidate was accused, among others, of incitement to actions against the constitutional order, the communication of false information in official documents, and involvement in the establishment of an organization with a fascist, racist, or xenophobic character. Although he was not arrested, the court decided to put him under judicial control, which means that he is barred from leaving the country (Higgins, 2025). The investigation revealed that one of the main collaborators of Georgescu in planning and executing his political campaign was Horațiu Potra, a security consultant who was involved in several missions in African countries. Georgescu previously denied any links with Potra (Ion, 2024). It was revealed that Potra traveled to Moscow in September 2024 (Bonea, 2024) and received money from a Russian businesswoman in Dubai in January 2025 (Roman, 2025). All these elements amplify the suspicions that the Russian Federation is behind the operation that favored Georgescu and that the candidate was aware of it from the very beginning.

On March 9, 2025, the Central Electoral Committee (BEC) rejected Georgescu's candidacy in the presidential election rescheduled for May 2025, citing the CCR's decisions of rejecting Șoșoacă's candidacy and annulling the 2024 presidential election as key precedents (Biroul Electoral Central, 2025). Unsurprisingly, the CCR upheld the decision taken by the BEC (Curtea Constituțională a României, 2025).

Conclusions

The 2024 Romanian presidential election was clearly affected by an extensive and sophisticated campaign conducted by foreign entities. The pattern of the interference has been used in hybrid warfare before. It is highly unlikely that domestic forces could have managed such interference. The financial resources needed for such an endeavor are in the range of tens of millions of euros (Raducanu, 2025). For a private company or person, such an investment would have been extremely risky, the chances of at least recovering the amount that was spent being extremely low. Moreover, if these blatant illegalities would have been designated and conducted internally, the chances of holding accountable those who were responsible would have been significantly higher. Last but not least, the involvement of individuals or companies based in countries like South Africa, the UK, Poland, or Ukraine suggests that the operation was managed from outside Romania.

Given that our analysis deals with an ongoing situation, there are still some aspects that at least publicly are not yet clarified. Firstly, there are no elements that prove beyond any doubt the identity of the state that planned and executed this operation. There are several solid clues that point towards the Russian Federation, but at least for now, such a conclusion cannot be drawn from a scientific perspective. Secondly, it is not proven yet beyond any doubt that Călin Georgescu would have been in contact with the masterminds of the operation or aware of the illegal nature of it. It is the responsibility of the judiciary to provide clear answers in this regard.

Regardless of Georgescu's potential involvement in this hybrid warfare action, it is unlikely that the main goal of it was helping him to win the election. Such an objective might have been set only after the results of the first round. Firstly, the operation, as we mentioned before, was an upgraded version of endeavors that were earlier conducted outside the UE. Just as Hungarian prime-minister Viktor Orban noticed (Darvari, 2024), the perpetrators seemed to have been testing how new technologies can influence important parts of the electorate inside EU

countries. Both protectors and enemies of liberal democracies have valuable lessons to learn from this case. Secondly, in many situations, the goal of hybrid warfare is to generate chaos. From this point of view, this operation was highly successful. For the first time in the history of the EU, a presidential election was annulled while the electoral process was ongoing. For the first time in the history of Romania, the country's president resigned, after his mandate was extended through a decision of the CCR (Păcurar, 2025). Moreover, the trust of the citizens in the institutions responsible for guaranteeing national security and in the political establishment was further diminished.

This case also has a negative impact on global security. Especially after February 24, 2022, Romania's geopolitical importance increased significantly. After December 6, some of Romania's allies required explanations regarding the outcome. The causes and implications of such a decision created confusion and tenseness. Partners from both NATO and the EU engaged in a dialogue with the Romanian authorities on this topic. President Klaus Iohannis presented a detailed image of the events at the European Council meeting held on December 19, 2024 (Administrația Prezidențială, 2024). While some leaders expressed their support for the manner in which the inference was handled (Dumitrescu, 2025), others stated that they were concerned about the upholding of democratic values (Marica, 2025). Although no major rearrangements took place in Romanian foreign policy until now, the case we analyzed shows that hybrid attacks through new technologies can weaken key strategic partnerships. The political class, the institutions designed to uphold national security, and the academia have a shared responsibility in preventing or mitigating the effects of such an operation.

Bibliography

Administrația Prezidențială (2024). Participarea Președintelui României, Klaus Iohannis, la reuniunea Consiliului European. *Administrația Prezidențială,* December 19, 2024. Available at: https://www.presidency.ro/ro/media/comunicate-de-presa/participarea-presedintelui-romaniei-klaus-iohannis-la-reuniunea-consiliului-european1734641118. Accessed in February 2025.

Almäng, J. (2019). War, vagueness and hybrid war. *Defence Studies*, 19(2), 189–204. https://doi.org/10.1080/14702436.2019.1597631

Anghel, V. (2024). Why Romania Just Canceled Its Presidential Election. *Journal of Democracy*, 2024. Available at: https://www.journalofdemocracy.org/online-exclusive/why-romania-just-canceled-its-presidential-election/. Accessed in February 2025.

Arambescu, D. (2024). Viktor Orban consideră alegerile din România drept un "experiment util" pentru Ungaria: "A fost ca într-un laborator". *Libertatea*, November 29, 2024. Available at: https://www.libertatea.ro/stiri/viktor-orban-considera-alegerile-din-romania-drept-un-experiment-util-pentru-ungaria-a-fost-ca-intr-un-laborator-5102720. Accessed in February 2025.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is Coming! *Comparative Strategy*, 12(2). Retrieved from https://www.rand.org/pubs/reprints/RP223.html.

Atkinson, C. (2018). Hybrid Warfare and Societal Resilience: Implications for Democratic Governance. *Information & Security: An International Journal*, 39(1), 63–76. https://doi.org/10.11610/isij.3906

Bancăș, L. (2024). Sondaj INSCOP: Cine intră în turul II la alegerile prezidențiale și cum arată o finală Ciolacu – Simion. *Digi24,* October 24, 2024. Available at:

https://www.digi24.ro/alegeri-prezidentiale-2024/sondaj-inscop-cine-intra-in-turul-ii-la-alegerile-prezidentiale-si-cum-arata-o-finala-ciolacu-simion-2980743. Accessed in February 2025.

Bian, N. (2024) Detectorul de minciuni /Georgescu, declarație in iunie: NATO este cea mai slabă alianță militară de pe planetă / Pentru ce să stai într-un club care nu oferă siguranță?/ Georgescu, marți seara: Nu doresc ieșirea din NATO, nu doresc ieșirea din Uniunea Europeană. *G4Media,* November 26, 2024. Available at: https://www.g4media.ro/detectorul-de-minciuni-georgescu-declaratie-in-iunie-nato-este-cea-mai-slaba-alianta-militara-de-pe-planeta-pentru-ce-sa-stai-intr-un-club-care-nu-ofera-siguranta-georgescu-marti-seara-nu-dor.html. Accessed in February 2025.

Biroul Electoral Central (2025). Decizie privind respingerea înregistrării candidaturii independente a domnului Georgescu Călin la alegerile pentru Președintele României din anul 2025, Nr. 18D/09.03.2025. *Biroul Electoral Central*, March 9, 2025. Available at: https://prezidentiale2025.bec.ro/wp-content/uploads/2025/03/decizie_18D.pdf. Accessed in March 2025.

Blanchette, J. (2020) *Ideological Security as National Security*. Center for Strategic and International Studies.

Boga, B (2025). Elon Musk picks up a gross disinformation about the elections in Romania and accuses "tyrannical behavior". *SpotMedia,* January 11, 2025. Available at: https://spotmedia.ro/en/news/politics/elon-musk-picks-up-a-gross-dezinformation-about-the-elections-in-romania-and-accuses-tyrannical-behavior. Accessed in February 2025.

Bonea, M. (2025). Horațiu Potra a fost la Moscova în septembrie 2024. Iubita bodyguardului lui Georgescu s-a fotografiat cu mercenari ceceni. *Digi24,* February 26, 2025. Available at: https://www.digi24.ro/stiri/actualitate/justitie/horatiu-potra-a-fost-la-moscova-in-septembrie-2024-spun-anchetatorii-iubita-lui-s-a-fotografiat-cu-mercenari-ceceni-3135789. Accessed in March 2025.

Boulianne, S., Theocharis, Y. (2020) Young People, Digital Media, and Engagement: A Meta-Analysis of Research. *Social Science Computer Review,* 38(2), 111-127.

Cannistraro, P. V. (1972). The Radio in Fascist Italy. *Journal of European Studies*, 2(2), 127–154. doi:10.1177/004724417200200201.

Centre for Information Resilience (2025). Disinformation campaign uncovered by researchers ahead of Croatian presidential run-off. *Centre for Information Resilience,* January 8, 2025. Available at: https://www.info-res.org/cir/articles/disinformation-campaign-uncovered-by-researchers-ahead-of-croatian-presidential-run-off/. Accessed in February 2025.

Chan, J. (2022). Online astroturfing: A problem beyond disinformation. *Philosophy & Social Criticism*, *50*(3), 019145372211084. https://doi.org/10.1177/01914537221108467.

Chelcea, S. (2007). *Metodologia cercetării sociologice: metode cantitative și calitative* (3rd ed.). București: Editura Economică.

Chilvers, J., Kearnes, M. (2019) Remaking Participation in Science and Democracy. *Science, Technology, & Human Values,* XX(X), 1-34.

Cîmpean, A-M. (2025). Bogdan Peschir, financier of Calin Georgescu's campaign on TikTok, placed in 30-day preventive arrest. *ȘtiriPeSurse*, March 22, 2025. Available at: https://www.stiripesurse.ro/bogdan-peschir-financier-of-calin-georgescus-campaign-on-tiktok-placed-in-30-day-preventive-arrest_3622091.html. Accessed in March 2025.

Clarke, R. A., Knake, R. (2010). *Cyber War : the Next Threat to National Security and What to Do About It*. New York: Harpercollins E-Books.

Cojan, L. (2024). Rezultatele finale ale alegerilor europarlamentare. Cine sunt românii care vor intra în Parlamentul European. *Digi24,* June 18, 2024. Available at: https://www.digi24.ro/alegeri-europarlamentare-2024/bec-anunta-rezultatele-finale-ale-alegerilor-europarlamentare-2831399. Accessed in February 2025.

Coman, S. (2024). Georgescu se dezice de legionari și extremiști, deși s-a declarat admirator al lui Zelea Codreanu și al mareșalului Antonescu. Pe cel din urmă l-a și plagiat în discurs. *Euronews România*, December 2, 2025. Available at: https://www.euronews.ro/articole/calin-georgescu-se-dezice-de-legionari-dar-plagiaza-discursurile-maresalului-anto. Accessed in February 2025.

Coșlea, A. (2025). Premierul belgian Alexander De Croo: Rusia a intervenit în alegerile din România. *HotNews,* February 1, 2025. Available at: https://hotnews.ro/premierul-belgian-alexander-de-croo-rusia-a-intervenit-in-alegerile-din-romania-1892036. Accessed in February 2025.

Curtea Constituțională a României (2024). HOTĂRÂREA nr.32 din 6 decembrie 2024 privind anularea procesului electoral cu privire la alegerea Președintelui României din anul 2024. *Curtea Constituțională a României*, December 6, 2024. Available at: https://www.ccr.ro/wp-content/uploads/2024/12/Hotarare_32_2024.pdf. Accessed in February 2025.

Curtea Constituțională a României (2025). HOTĂRÂREA nr.7 din 11 martie 2025 privind contestațiile formulate împotriva Deciziei Biroului Electoral Central nr.18D din 9 martie 2025 privind respingerea înregistrării candidaturii independente a domnului Călin Georgescu la alegerile pentru Președintele României din anul 2025, precum și a semnului electoral. *Curtea Constituțională a României,* March 11, 2025. Available at: https://www.ccr.ro/wp-content/uploads/2025/03/Hotarare_7_2025.pdf. Accessed in March 2025.

Darvari, A. (2024). Viktor Orban, reacție ciudată după ce Călin Georgescu a câștigat pe TikTok: "Mulțumim românilor!". *Newsweek România,* November 29, 2024. Available at: https://newsweek.ro/international/viktor-orban-reactie-ciudata-dupa-ce-calin-georgescu-a-castigat-pe-tiktok-multumim-romanilor. Accessed in February 2025.

Davis, J. M. (2008). International Perspectives on Social Justice: Essentials for the Effort Toward Global Security. In Osborne, R.E., Kriese, P. (eds.). *Global Community. Global Security*, pp. 137-152. Amsterdam & New York: Rodopi B. V.

Dawson, J. (2021) Microtargeting as Information Warfare. *The Cyber Defense Review*, 6 (1) (Winter 2021), 63-80.

Dumitrescu, R. (2025). Russia manipulated elections in Romania, French president Emmanuel Macron says. *Romania-Insider,* February 21, 2025. Available at: https://www.romania-insider.com/russia-manipulated-elections-romania-macron-2025. Accessed in February 2025.

Euronews (2024). Sondaj INSCOP pentru alegerile prezidențiale 2024: Mircea Geoană și Marcel Ciolacu, umăr la umăr în primul tur. *Euronews România*, September 19, 2025. Available at: https://www.euronews.ro/articole/sondaj-inscop-alegeri-prezidentiale-2024-septembrie- mircea-geoana-si-marcel-ciolacu. Accessed in February, 2025.

European Parliament. (2023). TV still main source for news but social media is gaining ground | News | *European Parliament*. Retrieved from www.europarl.europa.eu website:

https://www.europarl.europa.eu/news/en/press-room/20231115IPR11303/tv-still-main-source-for-news-but-social-media-is-gaining-ground.

Ferrag, M. A., Kantzavelou, I., Maglaras, L., Janicke, H. (2023). *Hybrid Threats, Cyberterrorism and Cyberwarfare*. Boca Raton, London & New York: CRC Press.

Fridman, O., Kabernik, V., Pearce, J. C. (2019). *Hybrid conflicts and information warfare : new labels, old politics*. Boulder, Colorado: Lynne Rienner Publishers, Inc.

Fukuyama, F. (1992) *The End of History and the Last Man*. New York: Free Press.

Fukuyama, F., Fasting, M. (ed.) (2023) *După sfârşitul istoriei: un dialog despre ultimii 30 de ani*. București: Corint Istorie.

Gabor, E., Oancea, M., Pripp, V. (2023). Digital Democracy and the Growing Threat of Illiberalism.Opportunities and Limitations as Reflected by the Estonian Case. *Perspective Politice*, XVI (1-2), 66-84.

Gabor, E., Oancea, M., Pripp, V. (2024). The Impact of Deep Fakes in the Age of Populism and Post-Democracy. *Revista de Ştiinţe Politice. Revue des Sciences Politiques*, 83, 32 – 46.

Galante, L., Ee, S. (2019). *Defining Russian Election Interference:: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents*. Washington, DC: Atlantic Council.

Garaiman, R. (2024). Factorul "Prodănescu": afaceri peste hotare. Captura, December 2024. Available at: https://captura.ro/factorul-prodanescu-afaceri-peste-hotare/. Accessed in February 2025.

Gherghiță, A. (2024). Rezultate finale BEC alegeri prezidențiale, turul 1. Călin Georgescu ocupă primul loc, Elena Lasconi rămâne pe doi. *Libertatea*, November 26, 2024. Available at: https://www.libertatea.ro/stiri/rezultate-finale-alegeri-prezidentiale-turul-i-bec-romania-diaspora-5097221. Accessed in February 2025.

Gover, L. (2023). Political Bias in Large Language Models. *The Commons: Puget Sound Journal of Politics*, 4(1).

Greenberg, D. (2009). Torchlight Parades for the Television Age: The Presidential Debates as Political Ritual. *Daedalus*, 138(2), 6–19. http://www.jstor.org/stable/40543931.

G4Media (2024). Sondaj INSCOP: Ciolacu și Simion intră în turul doi / Următorii clasați: Lasconi, Geoană, Ciucă / Sondaj Atlasintel: Ciolacu pe primul loc, Lasconi și Simion își dispută umăr la umăr intrarea în turul doi / Călin Georgescu a crescut în ambele sondaje. *G4Media,* November 14, 2024. Available at: https://www.g4media.ro/sondaj-inscop-ciolacu-si-simion-intra-in-turul-doi-urmatorii-clasati-lasconi-geoana-ciuca-sondaj-atlasintel-ciolacu-pe-primul-loc-lasconi-si-simion-isi-disputa-umar-la-umar-intrarea-in-turul.html. Accessed in February 2025.

Hamourtziadou, L. (2020). Security challenges of the 21st century: new challenges and perspectives. *Journal of Global Faultlines*, 6 (2) (December 2019-February 2020), 121-123.

Higgins, A. (2025). Romania Opens Criminal Case Against Ultranationalist Politician. *The New York Times*, February 27, 2025. Available at: https://www.nytimes.com/2025/02/27/world/europe/romania-calin-georgescu.html. Accessed in March 2025.

Hoffman, F. G. (2010). "Hybrid Threats": Neither Omnipotent Nor Unbeatable. *Orbis*, *54*(3), 441–455. https://doi.org/10.1016/j.orbis.2010.04.009

Hoffman, F. G. (2014). Hybrid warfare and challenges. In Mahnken, T.G., Maiolo, J. A. (eds), *Strategic Studies*, pp. 329-336. New York: Routledge.

Huntington, S. P. (1996). *The Clash of Civilizations and the Remaking of World Order*. New York: Simon and Schuster.

Ion, I. (2024). Călin Georgescu susține că nu-l știe pe Horațiu Potra: „Știu și eu cum a auzit toată lumea". *Libertatea*, December 10, 2024. Available at: https://www.libertatea.ro/stiri/calin-georgescu-sustine-ca-nu-l-stie-pe-horatiu-potra-stiu-si-eu-cum-a-auzit-toata-lumea-5115108. Accessed in March 2025.

Jayakumar, S., Ang, B., Anwar, N. D. (2021). *Disinformation and Fake News*. Singapore: Springer Singapore : Imprint: Palgrave Macmillan.

Kaiser, B. (2019). *Targeted. The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Faceboook Broke Democracy and How It Can Happen Again*. New York: Harper Collins.

Kapsakoli, E. (2023). Cyberterrorism: A New Wave of Terrorism or Not? In *Hybrid Threats, Cyberterrorism and Cyberwarfare*. Boca Raton., London & New York: CRC Press.

Keller, F. B., Schoch, D., Stier, S., Yang, J. (2019). Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign. *Political Communication*, *37*(2), 1–25. https://doi.org/10.1080/10584609.2019.1661888

Leiser, M. (2016). AstroTurfing, "CyberTurfing" and other online persuasion campaigns. *European Journal of Law and Technology*, *7*(1), 1–27.

Long, M. (2024). Shadows of power beneath the threshold: where covert action, organized crime and irregular warfare converge. *Intelligence and National Security*, 1–27. https://doi.org/10.1080/02684527.2024.2417454

Lunday, C. (2025). Putin's bot army tries to swing German election. *Politico*, February 6, 2025. Available at: https://www.politico.eu/article/germany-election-flood-social-media-x-russia-bots-kremlin-operation-false-news/. Accessed in February 2025.

Mack, A., Furlong, K. (2004) When Aspiration Exceeds Capability: The UN and Conflict Prevention. In Price, R. M., Zacher, M. W. (eds.) *The United Nations and Global Security*, pp. 59-74. New York & Basingstoke: Palgrave Macmillan.

MacLean, S.J., Black, D.R., Shaw, T.M. (eds.) (2006) *A Decade in Human Security: Global Governance and New Multilateralisms*. Aldershot & Burlington: Ashgate.

Maheshwari, S. (2016). How Fake News Goes Viral: A Case Study. *The New York Times*. Retrieved from https://www.nytimes.com/2016/11/20/business/media/how-fake-news-spreads.html

Manning, R. A. (2020). *Emerging Technologies: New Challenges to Global Stability*. Atlantic Council: Scowcroft Center for Strategy and Security.

Marica, I. (2025) US vice president says Romania canceled presidential election over "flimsy intelligence suspicions" and "continental pressure". *Romania-Insider,* February 17, 2025. Available at: https://www.romania-insider.com/jd-vance-romania-elections-annulment-feb-2025. Accessed in February 2025.

Marin, V. (2025). Șefa diplomației UE, despre manipularea alegerilor prin platforme: Cazul României nu este izolat, trebuie să ne mișcăm repede. *HotNews,* February 12, 2025. Available at: https://hotnews.ro/sefa-diplomatiei-ue-despre-manipularea-alegerilor-prin-platforme-cazul-romaniei-nu-este-izolat-trebuie-sa-ne-miscam-repede-1900584. Accessed in February 2025.

McGuire, M., Dowling, S. (2013). *Cyber crime: A review of the evidence Research Report 75* (pp. 1–35). Retrieved from https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5e089b9bac3cdba577724cf0cd23f648a4f952d9

McIntyre, L. (2018). *Post-Truth*. Cambridge, MA: Mit Press.

Meder, L. (2008). Global Security: Needed: A New Definition for a New Century. In Osborne, R.E., Kriese, P. (eds.). *Global Community. Global Security*, pp. 9-16. Amsterdam & New York: Rodopi B. V.

Meseșan, D. (2020) "Premierul nostru". Cine a ajutat, din umbră, la promovarea lui Călin Georgescu, propunerea AUR pentru postul de prim-ministru. *Libertatea*, December 22, 2020. Available at: https://www.libertatea.ro/stiri/premierul-nostru-cine-a-ajutat-din-umbra-la-promovarea-lui-calin-georgescu-propunerea-aur-pentru-postul-de-prim-ministru-3343752. Accessed in February 2025.

Mihai, C. (2025) Vance's Munich speech sparks mixed reactions in Bucharest. *Euractiv,* February 17, 2025. Available at: https://www.euractiv.com/section/politics/news/vances-munich-speech-sparks-mixed-reactions-in-bucharest/. Accessed in February 2025.

Miller, G., Mekhennet, S., Brown, C. (2024). Iran turns to Hells Angels and other criminal gangs to target critics. *Washington Post.* Retrieved February 7, 2025, from Washington Post website: https://www.washingtonpost.com/world/2024/09/12/iran-criminal-gangs-target-dissidents/

Mirsky, Y., Lee, W. (2020) The Creation and Detection of Deepfakes: A Survey. *ACMComput. Surv*, 54(1).

Mitulescu, S. (2011). *Metode de cercetare in stiintele sociale*. Bucharest: Pro Universitaria.

Mumford, A., Carlucci, P. (2022). Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*, *8*(2), 1–15. https://doi.org/10.1017/eis.2022.19

Niemetz, M. D. (2015) *Reforming UN-Decision Making Procedures: Promoting a deliberative system for global peace and security.* London & New York: Routledge.

Nye, J. (2010). Cyber Power. In *WWW.BelferCenter.org* (pp. 1–30). Retrieved from https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/cyber-power.pdf.

Oltermann, P. (2016). Austrian presidential election result overturned and must be held again. *The Guardian,* July 1, 2016. Available at: https://www.theguardian.com/world/2016/jul/01/austrian-presidential-election-result-overturned-and-must-be-held-again-hofer-van-der-bellen. Accessed in February 2025.

Onofrei, N. (2024) Rezultatul final al alegerilor parlamentare 2024: Clasamentul oficial al partidelor la Senat și Camera Deputaților. *HotNews,* December 7, 2024. Available at: https://hotnews.ro/rezultatul-final-al-alegerilor-parlamentare-clasamentul-oficial-al-partidelor-la-senat-si-camera-deputatilor-1856560. Accessed in February 2025.

Park, S-M., Kim, Y-G. (2022) A Metaverse: Taxonomy, Components, Applications, and Open Challenges. *IEEE Access*, 10, 4209-4251.

Pantazi, C., Popescu, A. (2024) BREAKING Judecătorii Curţii Constituţionale au anulat candidatura Dianei Șoșoacă la președinția României / Șoșoacă nu mai are nicio cale de atac. *G4Media,* October 5, 2024. Available at: https://www.g4media.ro/surse-judecatorii-curtii-constitutionale-au-anulat-decizia-bec-de-inregistrare-a-candidaturii-dianei-sosoaca-la-presedintia-romaniei.html. Accessed in February 2025.

Păcurar, B. (2025). Klaus Iohannis: "Pentru a scuti România de această criză, demisionez din funcția de președinte al României". *Digi24,* February 10, 2025. Available at: https://www.digi24.ro/stiri/actualitate/politica/klaus-iohannis-si-a-dat-demisia-3115315?. Accessed in February 2025.

Popescu, A. (2024) Nicolae Ciucă: Bătălia acestui an este între democraţie şi autoritarism. *Digi24,* April 16, 2024. Available at: https://www.digi24.ro/stiri/actualitate/politica/nicolae-ciuca-batalia-acestui-an-este-intre-democratie-si-autoritarism-2761885. Accessed in February 2025.

Raducanu, A. (2025). Emil Hurezeanu, replică pentru JD Vance: Campania lui Georgescu a fost plătită cu milioane de euro. *Oficiul de ştiri,* February 22, 2025. Available at: https://oficiuldestiri.ro/emil-hurezeanu-replica-pentru-jd-vance-campania-lui-georgescu-a-fost-platita-cu-milioane-de-euro. Accessed in February 2025.

Robinson, M., Jones, K., Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, *49*(49), 70–94. https://doi.org/10.1016/j.cose.2014.11.007

Rogers, P. (2010) *Losing Control. Global Security in the Twenty-first Century*, third edition. London & New York: Pluto Press.

Roman, M. (2024) Sondaj la comanda USR: Marcel Ciolacu conduce cu 24,5%, urmat de George Simion și Elena Lasconi cu 19%. Călin Georgescu, surpriza de pe locul patru, peste Mircea Geoană și Nicolae Ciucă. *G4Media*, November 22, 2024. Available at: https://www.g4media.ro/sondaj-la-comanda-usr-marcel-ciolacu-conduce-cu-245-urmat-de-george-simion-si-elena-lasconi-cu-19-calin-georgescu-surpriza-de-pe-locul-patru-peste-mircea-geoana-si-nicolae-ciuca.html. Accessed in February 2025.

Roman, M. (2025) SURSE Cine e femeia blondă surprinsă alături de Horațiu Potra și teancuri de bani în Dubai: Anait Martirosyan, o rusoaică care se prezintă drept agent imobiliar. *G4Media*, March 4, 2025. Available at: https://www.g4media.ro/surse-cine-e-femeia-blonda-surprinsa-alaturi-de-horatiu-potra-si-teancuri-de-bani-in-dubai-anait-martirosyan-o-rusoaica-care-se-prezinta-drept-agent-imobiliar.html. Accessed in March 2025.

Schroeder, U. (2021) The Transformation of Security Concepts: Beyond the State. In Geib, R., Melzer, N. (eds.). *The Oxford Handbook of the International Law of Global Security*, pp. 54-68. Oxford: Oxford University Press.

Secretariatul Consiliului Suprem de Apărare a Țării (2024a). Notă, anexă la nr. DSN1/1743, 04.12.2024. *Administrația Prezidențială.* Available at: https://www.presidency.ro/files/userfiles/Documente%20CSAT/Document%20CSAT%20SRI%20II.pdf. Accessed in February 2025.

Secretariatul Consiliului Suprem de Apărare a Țării (2024b). Raport, nr. DSN1/1701, 02.12.2024. *Administrația Prezidențială.* Available at: https://www.presidency.ro/files/userfiles/Documente%20CSAT/Document%20CSAT%20STS.pdf. Accessed in February 2025.

Secretariatul Consiliului Suprem de Apărare a Țării (2024c). Notă, anexă la nr. DSN1/1742, 04.12.2024. *Administrația Prezidențială.* Available at: https://www.presidency.ro/files/userfiles/Documente%20CSAT/Document%20CSAT%20SRI%20I.pdf. Accessed in February 2025.

Secretariatul Consiliului Suprem de Apărare a Țării (2024d). Notă de informare, nr. DSN1/1741, 04.12. 2024. *Administrația Prezidențială.* Available at: https://www.presidency.ro/files/userfiles/Documente%20CSAT/Document%20CSAT%20MAI.pdf. Accessed in February 2025.

Secretariatul Consiliului Suprem de Apărare a Țării (2024e). Notă, nr. DSN1/1740, 04.12.2024. *Administrația Prezidențială*. Available at: https://www.presidency.ro/files/userfiles/Documente%20CSAT/Document%20CSAT%20SIE.pdf. Accessed in February 2025.

Segal, H., Fitz-Gerald, A. (2021) *Relevant Global Security Trends.* Centre for International Governance Innovation.

Shad, M. R. (2018) Cyber Threat in Interstate Relations: Case of US-Russia Cyber Tensions. *Policy Perspectives,* 15 (2), 41-55.

Sletzinger, M. (2014) *The Lasting Impact of the Helsinki Process.* Washington, DC: The German Marshall Fund of the United States.

Tikk-Ringas, E. (eds.) (2015). *Evolution of the Cyber Domain: The Implications for National and Global Security.* London: The International Institute for Strategic Studies.

VIGINUM (2025). Manipularea algoritmilor și instrumentalizarea influencerilor Concluzii desprinse din alegerile prezidențiale din România & riscuri pentru Franța. *Service de vigilance et protection contre les ingérences numériques étrangères*. Available at: https://www.sgdsn.gouv.fr/files/2025-02/20250204_VIGINUM_Rapport%20public_ Elections_Roumanie_risques_France_ROU.pdf. Accessed in February 2025.

Wach, K., Duong, C.D., Ejdys, J., Kazlauskaitė, R., Korzynski, P., Mazurek, G., Paliszkiewicz, J., & Ziemba, E. (2023). The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT. *Entrepreneurial Business and Economics Review*, 11(2), 7-30. https://doi.org/10.15678/EBER.2023.110201

Walker, E. T., Rea, C. M. (2014). The Political Mobilization of Firms and Industries. *Annual Review of Sociology*, 40(1), 281–304. https://doi.org/10.1146/annurev-soc-071913-043215

Weissmann, M., Nilsson, N., Thunholm, P., Palmertz, B. (2021). *Hybrid Warfare*. London: Bloomsbury Publishing

White, N. D., Davies-Bright, A. (2021) The Concept of Security in International Law. In Geib, R., Melzer, N. (eds.). *The Oxford Handbook of the International Law of Global Security,* pp. 19-36. Oxford: Oxford University Press.

Woodward, A. (2025). Could German election result be annulled by European Commission? *Euro Weekly News,* January 12, 2025. Available at: https://euroweeklynews.com/ 2025/01/12/could-german-election-result-be-annulled-by-european-commission/. Accessed in February 2025.

Wylie, C. (2019) *Mindf*uck – Cambridge Analytica and the Plot to Break America.* New York: Random House.