European Journal of Law and Public Administration
ISSN: 2360-6754 | e-ISSN: 2559-7671
Covered in: Erih Plus; HeinOnline; CEEOL; RePEc; CrossRef; Google Scholar; KVK; WorldCat; ICI Journals Master List - Index Copernicus; EBSCO.

2024, Volume 11, Issue 2, pages: 226-236 | https://doi.org/10.18662/eljpa/11.2/244

Cyber Risks to National Security: Manipulation of the Electoral Process Through the Use of Bots and Algorithms on Social Platforms

Cristian CUCOREANU [1]

[1] Lecturer PhD, "Stefan cel Mare" University of Suceava, Romania, cucoreanu_cristian@yahoo.com

Abstract: *Developments in digital technologies and the growth of social media networks have brought to the forefront new risks and vulnerabilities to national security, including the manipulation of elections through cyber-assisted means. This article examines at a theoretical level how bots and advanced algorithms are being used to disseminate disinformation, amplify controversial content and influence public perceptions during election campaigns. The study briefly analyzes the mechanisms through which these digital tools exploit the vulnerabilities of social media platforms, with a direct impact on the transparency of the democratic process. The legal implications of these practices are discussed, as well as countermeasures adopted at national and international level. Finally, the article proposes solutions to strengthen the cyber defense capacity of states and protect the electoral process from cyber threats.*

Keywords: *cyber risks; national security; manipulation; electoral process; use of bots; algorithms; social platforms.*

How to cite: Cucoreanu, C. (2024). Cyber risks to national security: manipulation of the electoral process through the use of bots and algorithms on social platforms. *European Journal of Law and Public Administration, 11*(2), 226-236. https://doi.org/10.18662/eljpa/11.2/244

©2024 Published by In Manifest Network in partnership with LUMEN Publishing. This is an open access article under the CC BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

National security context in the digital age. The role of IT&C infrastructures in electoral processes.

National security, in the new digital age, has become an active concept, integrating traditional and new dimensions, of which cyber has a leading place. The rapidly evolving new technological transformations have redefined not only how states exercise their sovereignty but also the risks they face. In this context, the main strategic priority is the protection of IT&C infrastructures, given their interdependence with the smooth functioning of democratic processes, including electoral elections.

The promotion of electoral processes is strongly linked to the use of information and communication technologies, from the management of voter databases to the dissemination of election data through digital platforms. This technological dependence, while offering multiple benefits in terms of efficiency and quick access to information, also creates a number of risks and vulnerabilities. Cyber-attacks, disinformation and algorithmic manipulation on social platforms have the potential to undermine the integrity of elections, affecting public perception and trust in the democratic system.

The security of these infrastructures is no longer just a matter of basic technological protection, but requires an integrated and complex approach, encompassing legal-strategic and operational aspects. Also, the role of online platforms in the electoral process raises new issues, as they become spaces of influence that can be exploited by hostile unknown actors, be they state or non-state. In such a reality, the identification, prevention and management of cyber threats to the electoral process become imperative for the protection of democratic values and national security.

The importance of combating cyber threats to democratic elections.

Combating cyber threats to democratic elections is an obligation of any modern state seeking to protect its sovereignty, political stability and citizens' trust in the electoral process. In an era of ever closer connections, democratic elections are also influenced by external, not just internal, factors that exploit the digital environment to manipulate people's opinions, spread misinformation and influence election results. These actions also jeopardize the democratic foundations on which a normal society is based, not just undermine the electoral process.

The integrity of the electoral process is vulnerable to the use of sophisticated technologies, such as artificial intelligence (AI) and content-spreading algorithms on social media platforms, which can propagate hostile

messages and artificially steer electoral preferences. These techniques can generate social instability in the absence of effective countermeasures, eroding citizens' trust in state institutions and creating the conditions for a fragile political climate.

At the same time, protecting the electoral process from such threats is not just a matter of taking countermeasures in the face of cyber attacks. The implementation of preventive strategies is mandatory, including permanent monitoring of the digital space, strict regulation of social media platforms and educating the public about the risks and vulnerabilities associated with cyber misinformation and manipulation. In this regard, combating cyber threats should not be treated as a separate challenge, but as an integral part of a comprehensive and targeted effort to strengthen democratic stability.

IT&C infrastructures and their vulnerabilities in the electoral process

Definition of critical IT&C infrastructures in elections. Main vulnerabilities in the cyber environment.

IT&C infrastructures, in the new context of digitalization, are the central pillar of electoral processes. They ensure the smooth functioning of a wide range of activities, from the management of voter databases and the transmission of official information to the monitoring of the electoral process and the centralization of voting results. These infrastructures, although dependent on complex technologies, are vulnerable to a multitude of cyber risks that can compromise the integrity and transparency of elections, generating serious consequences for national security and democratic stability (Supreme Council of National Defense. November 28, 2024). Knowledge and understanding of the role of these networks, along with analyzing their inherent vulnerabilities, are essential for developing effective protection strategies.

The IT&C systems used during electoral processes include IT systems for voter registration, communication networks, digital platforms for information dissemination and, in some cases, electronic voting systems. These components are interrelated and form a complex ecosystem that facilitates the conduct of the electoral process in an accessible and efficient manner (Permanent Electoral Authority, 2024). For example, voter databases store information of a personal nature, which is essential to ensure fair voter turnout. At the same time, communication networks enable the operational coordination of the authorities involved in organizing elections

and the transmission of results in real time. The role of these systems is all the more important as they not only support the electoral process, but also strengthen citizens' confidence in its conduct.

However, these infrastructures face numerous vulnerabilities that can make them targets for cyber attacks. Exposure to hacking attacks is one of the main problems, which can target either unauthorized access to databases or manipulation of electoral results (Council of the European Union, n.d.). The absence of appropriate security measures, such as data encryption or strong authentication systems, also increases the risk of compromise. Another significant vulnerability is related to the use of outdated technologies, which cannot withstand advanced attacks and are often exploited by state or non-state cyber actors.

The reliance on social media platforms for information dissemination is another extremely sensitive issue. These networks, while useful in promoting transparency, are vulnerable to disinformation and manipulation campaigns that can influence voters' opinions (Latschan, 2023). By way of example, content distribution algorithms can be exploited to amplify negative or biased messages, while fake accounts and bots can create a distorted image of political reality (Mediacritica, 2023).

Given the above, these types of infrastructures play an important role in the electoral process, but their vulnerabilities can be exploited to destabilize elections and undermine and diminish society's trust in the democratic system. It is a strategic priority for state institutions to identify and manage these vulnerabilities in order to ensure the proper conduct of elections and to protect the fundamental values of democracy.

The impact of social platforms on the transparency of the electoral process.

Social networks have become a ubiquitous element in everyday life, significantly influencing the way people communicate, interact and form opinions. In the context of electoral processes, they play a dual role (facilitating the rapid transmission of electoral information and encouraging people to participate on the one hand, but on the other hand, they also facilitate the spread of misinformation and manipulation of public opinion. This complex impact of social media platforms poses great challenges for the security of the electoral process, in particular in terms of influencing voters' decisions, perceptions of candidates and trust in election results.

One of the most important effects of these networks on elections is the increase in the amount of information, whether correct or false. The algorithms of these platforms prioritize the content that generates the most

reactions and interactions, which often favors posts that are sensational, even if they are erroneous. This phenomenon allows misinformation to spread rapidly, creating a misperception of political reality and thus influencing citizens' choices. Moreover, cyber actors can modify these algorithms to send fake messages, using fake accounts or bots, manipulating online conversations, dividing and alienating public opinion.

Another significant problem is the personalization of content, which is achieved through data collected about users. This practice allows the delivery of highly targeted messages tailored to the psychological and behavioral profile of each user. During election campaigns, this capability is often used to steer voters in a certain direction with messages that influence their voting decisions, often without them being aware of the manipulative process they are exposed to. This type of approach raises many questions about the transparency of the electoral process and the protection of users' personal data.

Platforms can also generate an information echo-chamber effect, where users are only exposed to views similar to their own beliefs, limiting access to diverse perspectives and creating dissenting public opinion. In such a restricted information environment, voters may become more vulnerable to misinformation propaganda, and constructive discussion and democratic debate are replaced by ideological conflicts.

In addition, the lack of a clear regulatory framework on the content published on social networks and the lack of accountability of companies in the field of social media helps to maintain these risks. This type of platform becomes a breeding ground for those who want to undermine the integrity of the electoral process, either through cyber attacks or psychological manipulation, in the absence of strict control and transparency measures.

As a general conclusion, we can say that social media platforms have a strong impact on the fairness of elections, creating both opportunities and major risks. While these systems can facilitate democratic participation and increase transparency, their exploitation through manipulation and disinformation undermines the core values of democracy. Combating these negative effects requires a combination of strong regulation, such as the development of technologies to detect negative behaviors and to educate the public about the risks associated with the use of digital platforms in electoral contexts.

Case study - The 2024 presidential elections and suspicions of manipulation on TikTok

The 2024 presidential election was a complex test for the transparency of the democratic process, marked by suspicions of manipulation of public opinion through the social media platform TikTok. This situation highlighted major vulnerabilities of the digital space in the electoral context, especially through the use of advanced techniques such as the use of bots and the manipulation of the platform's algorithms to promote a particular candidate (Meeting of the Supreme Council of National Defense, November 28, 2024). In this study we analyze in detail the dynamics of these suspicions and the potential impact of these practices on public opinion and the electoral process.

One of the main allegations concerned the use of bots to spam the comment sections of election-related videos. Bots, automated programs designed to post repeated messages, were suspiciously used to flood the comments with the name of a particular candidate. This practice had two significant effects, one related to creating a perception of massive support and the other to directing the public conversation toward that candidate. By obsessively repeating his name in various contexts, the bots have generated a digital omnipresence effect, which can subconsciously influence users' perceptions, leading them to believe that the candidate is an inevitable choice.

Another important aspect of this is how TikTok's algorithms may have been manipulated to favor the distribution of content about that candidate. The platform's recommendation algorithms, which are built to increase interactions and time spent on the app, are vulnerable to intentional misuse. Suspicions suggest that they may have been set or targeted to constantly promote videos of the same candidate, driving users to a specific information feed. This practice could lead to a phenomenon known as information tunneling, where users are constantly exposed to the same narrative, which can change perceptions of reality and limit access to alternative viewpoints.

The consequences of the use of bots and the manipulation of algorithms on public opinion are major. On the one hand, these tactics can undermine public confidence in the electoral process, fueling suspicions about the fairness and transparency of elections. On the other hand, they can directly influence voting decisions by creating a perception of a candidate's artificial legitimacy or inevitability. In addition, such practices raise serious questions about the fairness and transparency of elections, as

advantages gained through digital manipulation can destabilize political competition.

Against the background of this unprecedented situation there is a need for stricter regulation of digital platforms, as well as the importance of developing effective mechanisms to detect and prevent online manipulation. At the same time, educating users to recognize forms and techniques of misinformation and manipulation becomes a key priority, as an informed population is less susceptible to negative influences in the digital space. In the absence of clear and firm measures, the risk that such practices will intensify in future elections remains high, jeopardizing democratic principles and political stability.

Strategies and measures to combat cyber risks in electoral processes

Policies and regulations to protect elections from cyber influences.

A strategic priority for democratic states in an increasingly technology-dependent global environment is to protect electoral elections from the risks of cyber-attacks. These risks, which are generated by both state and non-state actors, threaten to undermine the integrity of democratic processes by undermining public confidence in elections and, by extension, in state institutions. In order to prevent and combat negative cyber influences, it is beneficial to implement clear policies and adopt advanced technologies that ensure both technological security and transparency of the electoral process (Cybersecurity Strategy of Romania 2022-2027, 2022).

A fundamental role in defending elections against cyber interference is played by strict regulations and enforced policies. In this regard, it is necessary to develop a legislative framework to establish precise and strict security standards for IT&C infrastructures used during elections, as well as to regulate the activity of social media platforms during the electoral period. An example of such a measure is to impose transparency on online political advertisements by requiring labeling and disclosure of funding sources. The legislation should also include clear sanctions for using bots or algorithmic manipulation to influence public opinion. In parallel, international cooperation is becoming essential, given the cross-border nature of cyber-attacks on non-state actors. Democratic states need to work together to develop treaties and agreements to deter external interference and enable coordinated responses to such incidents.

Beyond policies, the use of advanced technologies to detect and prevent online manipulation is vital. Artificial intelligence-based systems can be used to identify suspicious activities (e.g. the creation and massive use of

fake accounts or the automated posting of repetitive messages). These tools can analyze online behavior patterns, such as posting frequency and distributed content, to detect bots. In addition, machine learning algorithms can be developed to differentiate between human and artificially generated activity, giving election authorities and social media companies a powerful tool to prevent manipulation.

Making transparent how social media platforms' recommendation systems work is an effective approach to algorithmic manipulation. This would enable both users and authorities to better understand how content is promoted and to identify potential abuses. Technology companies should also be obliged to put in place mechanisms to prevent the artificial amplification of content by malicious actors by introducing barriers to limit the impact of automated activity.

Cooperation between governments, private companies and international organizations

In the face of increasingly sophisticated cyber threats, cooperation between governments, the private sector and international organizations is becoming an essential pillar of cybersecurity, especially in the context of protecting electoral elections. In an international digital environment, acts of cyber interference are not limited to national borders, and effective solutions to prevent and combat these threats require strong partnerships between state and non-state actors. Governments, as the competent authorities in protecting national security, must play a central role in formulating and implementing national cyber defense strategies, but this role cannot be complete without close cooperation with the private sector and international organizations (Romania Presidential Administration, 2020).

Governments are primarily responsible for creating the appropriate legislative framework and providing the necessary resources to protect IT infrastructures. They must also coordinate internal and external efforts to detect and neutralize threats, both in terms of financial resources and technical expertise. To this end, governments can encourage private companies, especially those in the IT&C sector, to actively participate in hardening IT infrastructures. These companies have not only the technology to identify vulnerabilities in systems, but also the advanced knowledge to deploy fast and effective solutions in the face of cyber attacks. In this partnership, private sector companies can become a key element in ensuring security by providing technological expertise and operational support in the implementation of innovative protective solutions (National Country Defense Strategy 2020-2024).

International bodies play a key role in promoting standards and coordinating actions at global level. Given the cross-border nature of cyber-attacks, cooperation between states and international organizations such as the United Nations, the European Union or Interpol is vital to create a unified response framework. These entities facilitate the exchange of information and best practices, help to establish international rapid response protocols and support the formation of cooperation networks between states. A relevant example is the international conventions that regulate behavior in cyberspace and impose clear responsibilities on signatory states to prevent and combat cyber attacks. Through these instruments, international organizations contribute to building collective resilience to cyber risks.

Cooperation between governments and international organizations, as well as partnerships between private and public companies, goes beyond information sharing to include joint cyber-attack simulation exercises, the implementation of rapid response protocols and the development of joint strategies to educate the public and decision-makers. It is important that this type of cooperation is underpinned by clear and transparent policies that set out the responsibilities of each state involved and facilitate a unified response to threats (Ministry of Foreign Affairs, n.d).

In conclusion, it is only through a common approach that national security can be ensured, thus protecting the fundamental values of democracy.

Conclusion

In the context of the rapid evolution of technology, cyber risks have become a significant threat to national security. These risks not only affect the IT infrastructures of states, but also endanger the normal functioning of democracies, having the power to undermine citizens' trust in state institutions and electoral processes. Cyber attacks can be launched by a wide range of actors, including states, extremist groups, criminal organizations and even individuals with malicious intent. For this reason, cyber security must be integrated into the national defense strategy, and the competent authorities must anticipate and quickly respond to any type of cyber threat that can affect the stability and integrity of the state.

An important aspect in protecting national security is the adaptation of IT&C systems, which must become stronger in the face of cyber attacks. In this sense, the authorities must ensure not only the technological protection of IT systems, but also a thorough understanding of their vulnerabilities, which could be exploited by different types of actors.

Investments in IT&C infrastructure and the development of appropriate cyber security protocols are fundamental to protecting electoral processes and other vital sectors of the economy and public administration. Adapting infrastructures does not only mean the implementation of advanced technological solutions, but also the continuous training of personnel and the development of proactive strategies for the detection and prevention of cyber threats.

In order for the democratic system of a state to be protected against cyber risks and vulnerabilities, it is mandatory to adopt active measures to ensure the fairness of electoral elections. These measures cannot only be effective at the time of an attack, but must also include strategies to prevent online manipulation before it occurs. In this sense, clear regulations, cooperation between governments and the private sector, as well as education regarding the use of digital space by citizens are essential components for strengthening security and conducting electoral elections in a correct and transparent manner. Educating the public is a key factor, as awareness of the risks and adoption of responsible behavior online can significantly reduce the impact of manipulations and external influences on elections.

In conclusion, protecting democracy from cyber risks and threats involves not only the development of protective technologies, but also a coordinated effort at the national and international level, which includes strict regulations, cooperation and continuous education for citizens. National security and transparency of elections, in an increasingly digitized world, can only be ensured through a global and integrated approach, which includes prevention, protection and rapid reaction.

References

Council of the European Union (n.d). *Top cyber threats in the EU*. https://www.consilium.europa.eu/ro/infographics/cyber-threats-eu/. Accessed on November 2024.

Cybersecurity Strategy of Romania 2022-2027, *Regulation of the field of cyber security at the national level*, 2022. https://www.mae.ro/node/28367

Latschan, T. (December 4, 2023). What do we do with addiction to social networks?, *Focus- DW*. https://www.dw.com/ro/ce-facem-cu-dependen%C8%9Ba-de-re%C8%9Belele-social/a-67622577

Mediacritica (December 14, 2023.). *PEINTELES. What are bots?*. https://mediacritica.md/peinteles-ce-sunt-botii/?gad_source=1&gclid=Cj0KCQiAr7C6BhDRARIsAOUKifg5lcvHZLf-2k92BRldzo99T7PJLJtevJESou27DpEV9Q6iUHd3pxEaAlMNEALw_wcB

Meeting of the Supreme Council of National Defense, November 28, 2024. https://www.presidency.ro/ro/media/comunicate-de-presa/sedinta-consiliului-suprem-de-aparare-a-tarii1732806042

Romania Presidential Administration (2020). *National Defence Strategy 2020-2024. „Together for a safe and prosperous Romania in a world marked by new challenges".* https://www.presidency.ro/files/userfiles/National_Defence_Strategy_2020_2024.pdf

The Ministry of Foreign Affairs (n.d). *The issue of cyber security within international organizations and Romania's involvement as a member of them.* https://www.mae.ro/node/28369. Accessed on December 2024.

The Permanent Electoral Authority (2024). https://www.roaep.ro/instruire/operatori-de-calculator-sectii-votare/