Hacking democracy:

the threat of digital electoral interference for the European Union

Dr. E. Kapsokoli[1]

(Post-Doctoral Researcher at the Department of International and European Studies of the University of Piraeus and holds a PhD degree from the same department. She was a PhD Fellow at the European Doctoral School on the Common Security and Defence Policy (CSDP). She is also a researcher at the Laboratory of Intelligence and Cuber-security of the University of Piraeus and a research fellow at the Institute for National and International Security (INIS) of Serbia. Her main research interests include international security, terrorism, Islamic terrorism, cuber-security, cuber-terrorism, and digital democracy)

Elections are one of the cornerstones of democracy. This is true because democracy as a system of governance is very fragile and needs to be safeguarded, to ensure societal stability. Thus, democratic procedures such as elections should be transparent and inclusive with respect of human and political rights, political diversity, freedom of expression, and freedom of press. The fact that the users of cyberspace are more than 5.3 billion, and thus constitute 66% of the global population, highlights the importance of the information communication technologies (ICTs) in our daily life. The introduction of digital technology into the political sphere has had a significant effect on electoral processes affecting both voting behavior and the underlying factors that influence it. Cyberspace is the new arena for both supporters and opponents of democracy. The security challenges that arise between voters, candidates and political parties are abundant. Cyberspace functions as a channel of disinformation, thus misleading its users about the electoral processes.

---

[1] **Eleni Kapsokoli** is post-doctoral researcher at the Department of International and European Studies of the University of Piraeus and holds a Ph.D. degree from the same department. She was a Ph.D. Fellow at the European Doctoral School on the Common Security and Defence Policy (CSDP). She is also a researcher at the Laboratory of Intelligence and Cyber-security of the University of Piraeus and a research fellow at the Institute for National and International Security (INIS) of Serbia. Her main research interests include international security, terrorism, Islamic terrorism, cybersecurity, cyberterrorism, and digital democracy.

In more details, the electoral processes have been digitalized, and states use digital technology to conduct the elections. Electronic voting and ballots, as well as voting devices, constitute the digitalization of elections. Other examples of the above can be found in live-streaming websites and applications, certified lists of voters, and programs that count votes. The digitalization of democratic processes enables citizens to be a vital part of political processes. The digital electoral processes can offer important benefits such as time saving and reducing further bureaucracy and complexities in the electoral system. Other advantages are the facilitating of political campaigns and transparency to democratic procedures. An important result of the above is the higher percentage of voters turnout, which is a crucial indicator for the governance of their country.

But at the same time, the digitalization of elections raises significant security threats. The main security threat is that of the 'digital electoral interference'. There is a conceptual ambiguity on what exactly it means. The lack of a commonly accepted definition complicates the security of democratic processes. There are two main definitional approaches for this threat, there is a direct and indirect manner to conduct digital electoral interference. The direct manner is conducted via malicious cyber means, such as cyberattacks (hacking) on electoral bases and voting results. The indirect manner involves disinformation campaigns and the spreading of fake news, which undermine public trust and thereby democracy.

Due to the digitization of electoral processes, there are myriad vulnerabilities that malicious state and non-state actors can exploit to undermine societal resilience. First, the 'hack and leak' tactic is a usual tool and part of disinformation, which is also called 'doxing'. Moreover, the perpetrators make malicious use of social media and online platforms with paid commentators and advertisements, the creation of troll-accounts and the defamation of accounts which influence the political processes. In addition, there is a phenomenon of 'dirty' financing (money laundering, illegal financial support to politics, cryptocurrency political donations, etc.) in politics which increases political corruption. Furthermore, the perpetrators conduct malicious cyber activities to influence the functioning of electronic voting machines and the online transmission of data, and to distribute false online information about voting

procedures. Finally, perpetrators launch sophisticated online disinformation campaigns and reproduce fake news regarding the political processes and candidates.

During the last decade, several incidents of digital electoral interference have affected the reliability of democracy, undermined public faith in electoral processes and as a result destabilized societal balance. The widespread accusations of Russian election interference (e.g., French and US presidential elections), demonstrated how the distribution of stolen information in the digital sphere in combination with targeted influence campaigns - may affect the integrity and functioning of democracies. Considering upcoming elections in Europe, both the EU and its member-states realized that electoral interference - although not a new one - is a complex issue to tackle. The safeguarding of democracy by the EU was clearly pointed out by the president of the European Commission Jean Claude Juncker, who stated in September 2018 that "We must protect our free and fair elections".

These incidents have forced the EU to adopt or revise existing policies and strategies, to address and prevent these new security threats, and limit their impact. In particular, the EU adopted a multi-faceted response, by combining legal and technological measures, as well as ones that involve the functioning of the cooperation between public and private sector (social media platforms and digital technology companies). The EU's response focuses on cybersecurity issues that relate to electoral interference and has taken notable steps to counter this threat. Firstly, the EU has launched the 2017 and 2020 cybersecurity strategies which clearly mentioned the safeguarding of transparent governance and electoral processes, to maintain the integrity, availability, and confidentiality of elections. In 2015, the EU established the East StratCom Task Force and its flagship EUvsDiSinfo, which are responsible to monitor and respond to ongoing disinformation campaigns and increase public awareness. The Union emphasized multiple times the need of a joint action against disinformation and electoral interference. This need was supported by the adoption of the EU Code of Practice on Disinformation (2018 and 2022), which is a self-regulatory regime with the participation of crucial social media, advertising, and digital technology companies to ensure a transparent, safe, and trustworthy online environment. In 2020, the EU launched the European Democracy Action Plan (EDAP) which has as a key goal the promotion of the free and fair elections, the strengthening of media freedom,

and the countering of disinformation. Based on the above, it is safe to argue that the protection of electoral processes is not only an issue of security, but also an issue that calls into question the way the EU should safeguard its digital space regarding elections.

Confronting this threat is a major challenge, since the EU has twenty-seven member-states, which conduct elections in different ways and counter the emergence of their threats. Moreover, not all states are able to protect themselves from the potential cyberattacks to the digital electoral processes. Strengthening cooperation with the private sector is a step to the right direction, but not a panacea. Building resilience in societal and digital terms is a necessity before the EDAP proceeds with the preparation of guidelines for e-voting for all member-states. Currently, only three (France, Estonia, and Belgium) out of 27 European members-states and six out of 44 European countries use e-voting. This proves the insecurity or the lack of capacity building in this field. France is using e-voting regarding the national elections and electoral management body e.g., election of trade union leaders, non-binding referendums; Belgium is using e-voting for the national and sub-national elections; and Estonia, the tech-oriented country is using e-voting for national elections (no less than 36% and sometimes nearly 64% of voters cast their ballots online). These three member-states are trying to promote a safe, flexible, and transparent digital ecosystem to facilitate digital electoral processes in an automated and less-costly manner. E-voting could be used only for elections with low security risks and from very tech-oriented states, but it is not ready to be used for national elections. Voters should be guaranteed that their votes matter, regardless of the malicious attempts of some perpetrators.

To conclude, democracies need to harness digital technology. Over the past decade, democracies have witnessed numerous attempts by both state and non-state actors to destabilize the roots of democratic societies. On the other hand, democracies managed during the Covid-19 pandemic, to hold digital elections with success. Digital electoral interference is a low-cost and accessible option for malicious actors to spread fear, to cause destabilization and to create feelings of insecurity and violation. The fact that many member-states do not acknowledge this issue and do not publicly attribute malign activities to the offending adversaries or are under pressure to limit support to

EU-level activities to counter disinformation - hinder the safe conduct of elections. However, the EU is trying to counter these threats by promoting public-private partnership. But also, the Union and its institutions are trying to monitor and respond to disinformation campaigns and malicious cyber activities. The above goal is strongly supported by promoting fact-checking initiatives and self-regulating the digital technology companies and the social media. All the above, are desirable goals for all states, but it is worth mentioning that democratic processes such as elections are fundamental to the quality of state's governance and are the reflection of our society.

Sources

Baines, P. and Jones, N. (2018). Influence and interference in foreign elections. *RUSI Journal 163, no1*.

Brattberg, E. (18 August 2020). European Lessons for Tackling Election Interference. *CNAS.* https://www.cnas.org/publications/commentary/european-lessons-for-tackling-election-interference

Economou, E.M.L., Kyriazis, N.C. and Platias, A. (2022). *Democracy in times of crises*. Springer.

Ellena, K. and Shein, E. (7 April 2022). The Dark Side of Democracy. *International Foundation for Electoral Systems.* https://www.ifes.org/publications/dark-side-democracy

Elliott, C. (19 February 2019). Here Are the Real Fake News Sites. *Forbes*. https://www.forbes.com/sites/christopherelliott/2019/02/21/these-are-the-real-fake-news-sites/?sh=7f05b3d63c3e

ENISA. (2019). *Election cybersecurity: challenges and opportunities*. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities

European Commission. (3 December 2020). *Communication from the Commission to the European Parliament, the Council, the European Economic Social Committee and the Committee of the regions on the European Democracy action plan*. https://ec.europa.eu/info/sites/default/files/edap_communication.pdf

IDEA (Institute for democratic and electoral assistance). (Last access 5 April 2023) Is e-voting currently used in any elections? https://www.idea.int/data-tools/question-view/742

Shackelford, S. (2017). Making democracy harder to hack. University of Michigan Journal of Law Reform 50, no.3, pp.636-638 https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1178&context=mjlr

Tucker, J.A, Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D. and Nyhan, B. (19 March 2018). Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature. *Hewlett Foundation*. https://hewlett.org/library/social-media-political-polarization-political-disinformation-review-scientific-literature/

Wheatley, S. (2019). Foreign Interference in elections under the non-intervention principle: we need to talk about "coercion". *Duke Journal of Comparative and International Law 31, no. 161*.