Article

Wilfried Martens Centre for European Studies

European View
2024, Vol. 23(2) 226–234

DOI: 10.1177/17816858241288397
journals.sagepub.com/home/euv
Sage

The 2024 EU elections and cybersecurity: A retrospective and lessons learned

Eva Saeva and Iva Tasheva
CYEN, Brussels, Belgium

Abstract
This article analyses the cybersecurity threats to elections and draws out the lessons learned from the EU (Parliament) elections of June 2024, putting forward recommendations for further improvement. The objective of the analysis is thus manifold. First, it summarises the cyber threats pertinent to elections—those capable of influencing or distorting the election process and outcome. Second, it discusses the measures adopted in preparation for the 2024 EU elections and provides an analysis of how the election campaigns and actual elections across the 27 member states developed. Third, it offers recommendations for improving the cyber resilience of future elections. The analysis will cover both strictly cyber-specific threats and broader hybrid threats.

Keywords
Cybersecurity, Cyber resilience, EU institutions, Cyber threats, Elections, Artificial intelligence

Introduction

In June 2024 EU nationals across all 27 member states voted to appoint 720 Members of the European Parliament (MEPs) to represent them for the period 2024–9. This was a critical vote, setting the tone of Europe's democratic voice in a decade of growing insecurity, both in the conventional sense and in terms of cybersecurity. While the trustworthiness and integrity of elections are crucial, their confidentiality, probity and authenticity are continually being challenged. Information security measures need to be put in place

Corresponding author:
Iva Tasheva, CYEN, Avenue Paul Hymans 121, 1200 Brussels, Belgium.
Email: iva.tasheva@cyen.eu

to preserve genuine, uninterrupted, authentic and free public debate. Such measures are also needed to preserve the availability of public communication channels, to vet the authenticity of online identities and to guarantee the privacy of communications.

The trustworthiness of election results is crucial, especially if votes are cast online. Election systems therefore need to be resilient. Investing in cybersecurity—from awareness campaigns for political leaders and polling station staff to strengthening the security of systems, networks, devices and identities—must be a top priority for political parties.

The cyber threats relevant to the election process

Cybersecurity, defined as the security of information and communications technology (ICT) systems and networks, has been getting progressively more attention in recent years due to massive and continual cyber incidents. Cybersecurity was an integral part of the debate surrounding the security of the 2019 EU elections and has become even more relevant since, with the increased digitalisation of voting systems, including votes being cast online, not to mention the evolving threat landscape.

Cyber threats, if not addressed, could significantly impact registration systems. Hackers could tamper with voter data, block authorities' servers/websites at critical moments, hack campaign websites and social media accounts, spread disinformation and—while no such case has yet been reported—theoretically tamper with the software for online voting in order to affect electoral results. Malicious accounts often spread manipulative and untruthful content through social media networks. The potential consequences are grave, underscoring the urgency of our collective efforts to provide assurance of elections' cybersecurity.

In the report *Predictions for Cybersecurity Threats in 2024* (CYEN 2024b), we identified the top five threats that would dominate the year of the EU elections. Three of the five were strictly related to the elections: disinformation campaigns, abuse of artificial intelligence (AI) and data breaches. These predictions have sadly become a reality, as EU Cybersecurity Agency (ENISA) Executive Director Juhan Lepassaar has evidenced (Gatopoulos 2024). Lepassaar notes the worrying increase in the number of hacktivist attacks aimed at disrupting European infrastructure, which doubled from the fourth quarter of 2023 to the first quarter of 2024 (Gatopoulos 2024). This represented a solid capacity-building exercise for the hacktivists, just in time for the EU elections. On disinformation, in a recent case demonstrating how easy it is to spread fake news, British comedian Joe Lycett highlighted how fact-checking did not seem to be prioritised at many British news outlets, including *BBC News*, *Sky News* and the *Independent*, when he announced that several items of 'news' reported by these outlets were actually fake and had been made up by him (Badshah 2024). His campaign was not related to the elections, but is a major red flag that demonstrates how easy it is to plant untruthful information, how quickly it can go viral and, as a consequence, how it can be considered believable just because it comes from a 'reliable' source.

More data comes from ENISA, which identified disinformation as the second most prominent threat and AI abuse as the tenth most prominent threat in its *Cybersecurity Threats for 2030* report (Mattioli et al. 2023). The 2024 EU AI Act classifies '. . . AI systems intended to be used to influence the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda . . . as high-risk AI systems' (European Parliament and Council 2024, para. 62). Such systems must assess and reduce risks, maintain use logs, be transparent and accurate, and ensure human oversight. When it comes into effect on 2 August 2026, the AI Act will effectively ban AI systems that manipulate people's decisions or exploit their vulnerabilities, or that evaluate or classify people based on their social behaviour or personal traits, all potential actions that are very relevant in the context of elections. Indeed, in terms of cybersecurity, the AI Act specifically focuses on the importance of securing high-risk AI systems and banning the unacceptable use of such systems, including those that impact people's decisions (CYEN 2024a). AI-enabled threats, such as deep fakes, could be used to impersonate political figures with manipulative intent, with their impact multiplied by bot accounts used to facilitate the spread of fake content.

Identity theft from political leaders is also a cause for concern, as the use of weak passwords for social media accounts can lead to easy access and impersonation. This enables malicious actors to spread 'fake' messages from political leaders' real accounts, reaching a large audience and gaining significant attention.

Distributed denial of service (DDoS) attacks, which take down websites or services and are often politically motivated, are on the rise in the EU. Cloudflare (Tomé 2024) reports that 53.42 million threats per day to government websites in the EU are being mitigated in 2024, with 68% of those being DDoS threats. There were no significant attacks on European election-related organisations just before the elections, but the two-day DDoS attack on Dutch politics-related websites on 5 and 6 June should be noted, as well as attacks on the websites of EU member state governments—Bulgaria on 6 June, France on 11 and 23 May and 9 June, Sweden on 29 April and 18 May and Denmark on 7 May.

A critical concern is that cyber-attacks such as those involving ransomware, malware, phishing or DDoS do not have to be sophisticated to cause damage and interfere with the election process or results. The lack of cyber awareness and hygiene among political party personnel, campaign organisers, suppliers and European institutional personnel has become a significant threat.

Was the EU prepared for cybersecure elections?

European institutions' cybersecurity prior to the 2024 EU elections was not adequate to the level of threat; this was the conclusion of the 2022 European Court of Auditors' *Special Report on the Cybersecurity of the EU Institutions, Bodies and Agencies*. The report noted that the level of cybersecurity maturity varied between bodies—they did not always adopt good practices, nor did they have sufficient support (European Court of

Auditors 2022). More recently, it was reported that an internal European Parliament review showed that its cybersecurity 'has not yet met industry standards' and is 'not fully in line with the threat level' posed by state-sponsored hackers and other threat groups, despite state-sponsored attacks on the Parliament having become more frequent and more sophisticated (Roussi 2023).

Indeed, in November 2022 the European Parliament's external website was hit by an allegedly Russian DDoS attack (Van Sant and Goujard 2022). And in February 2024 the phones of MEPs and their staff in the Subcommittee on Security and Defence were infiltrated by intrusive surveillance software (European Parliament 2024). The European Parliament also suffered a massive breach of the sensitive personal data of its staff, including that of MEPs' assistants, which exposed private information including home addresses, bank details and criminal records (Tar 2024). This is of particular concern as the information could be used for further attacks, such as blackmail or identity theft, after the 2024 elections.

Meanwhile, attacks were reported in a number of member states in the run up to the elections. The websites of the Dutch Party for Freedom (Partij voor de Vrijheid) and the Christian Democratic Appeal (Christen-Democratisch Appèl) were briefly unavailable on polling day (Schickler 2024), while the Belgian media channels *DH*, *La Libre Belgique* and *LN24 News* were also targeted by cyber-attacks (Carantonis 2024). Individual political figures and candidates suffered cyber-attacks too, most notably European Commission President Ursula von der Leyen, who saw her campaign website attacked by bots (Ahmatović 2024).

Securing the 2024 European elections: the EU measures

While much has been done to mandate a high common level of cybersecurity for the EU institutions (European Parliament and Council 2023) and, with the implementation of the NIS2 Directive (European Parliament and Council 2022), for the important and essential entities operating in the critical infrastructure sectors, very little was done in the run up to the 2024 EU elections to ensure their security.

ENISA did update its Elections Compendium in 2024, underscoring the crucial need for collaboration and information sharing between all interested parties (ENISA 2024). These actions include identifying the risks and the ways to manage threats and crises, providing training, and implementing the necessary technical and organisational measures to secure the elections (ENISA 2024). In a high-level meeting in Italy in May 2024, Věra Jourová, then European Commissioner for Values and Transparency, reiterated that the exchange of information between European countries was extremely important to combat fake news and propaganda. She also noted the role of AI and the need to create synergies between emerging AI systems and traditional media (ACN 2024).

On the social media side, the European Commission published guidelines on how to 'mitigate systemic risks online that may impact the integrity of elections' under the

Digital Services Act (European Commission 2024). These included implementing election-specific risk-mitigation measures tailored to each individual electoral period and local context; adopting specific mitigation measures linked to generative AI; and executing other measures, including preparing an incident response mechanism for electoral periods (European Commission 2024). In line with these guidelines, TikTok announced the measures it had taken, which included launching a dedicated in-app Election Centre for every EU country; removing over 2,600 pieces of content for violating the platform's civic and election-integrity policies and over 43,000 pieces of content for violating the platform's misinformation policies; and taking down over 96% of violative misinformation content before it was reported, and over 80% before it had received a single view in this period (TikTok 2024).

The above steps, however, came late in the election process and focused on the EU's security and cyber resilience. The cyber resilience of and support for the political parties in the individual member states varied, but all needed to adopt security measures to better protect their networks, systems and—ultimately—the trustworthiness of the EU election process.

Securing the 2024 European elections: the member states' measures

At the member state level, some good examples of proactive campaigns need to be mentioned. Polish Prime Minister Tusk announced that a special non-partisan commission had been tasked with investigating Russian and Belarusian influence in Poland (*Euronews* 2024). Belgium also appointed experts to track online disinformation (*Euronews* 2024). Director General of the Italian National Cybersecurity Agency Bruno Frattasi announced that the agency was working closely with the Ministry of the Interior, which presides over the voting system. He mentioned the importance of the preventative measures that the agency was taking to protect the systems and networks that could be attacked by malicious actors aiming to disrupt the voting process (*AGI* 2024). Germany's Federal Office for Information Security, whilst acknowledging cyber espionage, disinformation and, more concretely, hack-and-leak and DDoS attacks as threats to the elections, also stated that there was no clear evidence of any attempts to use cyber-attacks to influence the election process (Germany, Federal Office for Information Security 2024). Aligned with the German view was former UK National Cyber Security Centre chief Ciaran Martin's plea to keep calm and not let the 'hysteria' take over, pointing out that we confuse 'activity and intent with impact, and what might be technically possible with what is realistically achievable' (Martin 2024). He also highlighted that often in cases of system or network failures, it is not down to foreign interference but simply to a 'failure of state infrastructure' (Martin 2024), an important point to note if we are considering the forest and not the individual trees.

Nonetheless, the most notable efforts to secure elections have been observed outside the EU. In the US, the Cybersecurity and Infrastructure Security Agency has produced an Election Security Toolkit. It has also established a formal Multi-State Information

Sharing and Analysis Center and an Elections Infrastructure Information Sharing and Analysis Center, which provide no-cost services to secure the US election infrastructure (US, CISA 2024). These will be of critical importance in the upcoming November presidential elections.

Cybersecurity in the 2024 EU elections: an analysis

At the time of publication, a few months after the elections, there has been no comprehensive report on the cybersecurity of the 2024 EU elections. Aside from the incidents noted above, there have been no reports of major disruptions, data breaches, or bot or ransomware attacks in relation to the election process. Despite the intensiveness of the disinformation attacks, we have not, at the time of writing, seen any claims that they had a major impact on Europeans' views or the election results. This could mean that campaigns did manage to prioritise security measures over budgetary concerns, which are very often used as an excuse for not adopting the necessary measures.

However, a post-event analysis is needed to pinpoint the soft spots during the EU election process—to highlight where campaign staff could have done better and summarise the lessons learned, so that the same, or similar, mistakes are avoided next time. We need to acknowledge that despite measures being put in place, cybersecurity vulnerabilities will continue to be exploited during the rest of the elections expected in 2024 and beyond. Political parties should not lower their guard once the election process is over.

Furthermore, implementing fully and in a timely manner the Regulation on a high common level of cybersecurity for the EU institutions (European Parliament and Council 2023) and the NIS2 Directive (European Parliament and Council 2022) for national governments' ICT service providers is critical to ensure an adequate level of cyber protection for the EU in the future.

Finally, it is important to differentiate between attempts to interfere with the elections and the actual impact the different types of attacks have actually had and will have. Taking proactive measures is always important, but providing a genuine and clear picture of the threat landscape, without overestimating it, is even more important. Acknowledging that foreign states have tried and will try in the future to interfere with our elections is an important message for national governments to deliver, but only alongside a solution for every threat. More data-backed analysis and decisions are needed.

Conclusion

The security of the election process and the trustworthiness of election results are the foundations of democracy, and ensuring them requires a collaborative effort and harmonised ambition—be it in the context of the EU elections, member states' national elections or non-EU states' elections. While the cybersecurity threat landscape is evolving

and many of the cyber threats the EU is facing could have an impact on elections, this post-event analysis of the 2024 EU elections has shown that despite the low level of attention paid to cybersecurity in the preparations for the polls, there were no major incidents reported during the elections. Nonetheless, efforts need to continue in the EU and beyond to avoid cyber-attacks having a significant impact on election processes around the world. We would encourage government organisations to publish their own analyses and lessons learned in view of the large number of resources that are available, as evidence-based communication on the cybersecurity measures taken and their impact on elections would contribute to greater public trust in the decision-making process.

References

ACN. (2024). Elezioni Eu e sicurezza informatica: incontro a Roma tra Jourovà, Barachini e Frattasi [EU elections and cybersecurity: Meeting in Rome between Jourovà, Barachini and Frattasi]. 8 March. https://www.acn.gov.it/portale/w/elezioni-eu-e-sicurezza-informatica-incontro-a-roma-tra-jourova-barachini-e-frattasi. Accessed 23 July 2024.

AGI. (2024). Frattasi: 'Lavoriamo per prevenire cyberattacchi durante elezioni di giugno' [Frattasi: 'We are working to prevent cyber-attacks during the June elections']. 16 May. https://www.agi.it/cronaca/news/2024-05-16/frattasi-al-lavoro-per-prevenire-cyberattacchi-durante-elezioni-26408203/. Accessed 23 July 2024.

Ahmatović, Š. (2024). Von der Leyen's campaign website hit by cyberattack. *Politico*, 8 May. https://www.politico.eu/article/ursula-von-der-leyen-campaign-website-attack-cybersecurity-eu-election/. Accessed 23 July 2024.

Badshah, N. (2024). Joe Lycett discloses four fake stories he planted in UK media. *The Guardian*, 13 April. https://www.theguardian.com/culture/2024/apr/12/joe-lycett-discloses-four-fake-stories-he-planted-in-uk-media. Accessed 23 July 2024.

Carantonis, A. (2024). La DH, La Libre Belgique et la chaîne d'information LN24 ont été victimes d'une cyberattaque. [DH, La Libre Belgique and the information chain LN24 were victims of a cyberattack]. *DH Les sports*, 5 June. https://www.dhnet.be/medias/2024/06/05/la-dh-la-libre-belgique-et-la-chaine-dinformation-ln24-ont-ete-victimes-dune-cyberattaque-VDKPV7TA35CSTKPQGIOZIWMSOU/. Accessed 23 June 2024.

CYEN. (2024a). EU AI Act – What was agreed and how companies can prepare for its implementation. *YouTube*, 18 June. https://www.youtube.com/watch?v=h5ZjBy32Y2k. Accessed 23 July 2024.

CYEN. (2024b). Predictions for cybersecurity threats in 2024. 11 January. https://cyen.eu/index.php/en/2024/01/11/cyens-predictions-for-eu-cybersecurity-in-2024/. Accessed 25 June 2024.

ENISA. (2024). Safeguarding EU elections amidst cybersecurity challenges. 6 March. https://www.enisa.europa.eu/news/safeguarding-eu-elections-amidst-cybersecurity-challenges. Accessed 23 July 2024.

Euronews. (2024). EU countries beef up anti-disinformation efforts ahead of European elections. 6 June. https://www.euronews.com/my-europe/2024/06/05/eu-countries-beef-up-anti-disinformation-efforts-ahead-of-european-elections. Accessed 23 July 2024.

European Commission. (2024). Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections. *Press release*, 26 March. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1707. Accessed 23 July 2024.

European Court of Auditors. (2022). *Cybersecurity of EU institutions, bodies and agencies*. Luxembourg. https://www.eca.europa.eu/Lists/ECADocuments/SR22_05/SR_cybersecurity-EU-institutions_EN.pdf. Accessed 23 June 2024.

European Parliament. (2024). Recent revelations of spying on Members of the European Parliament and the lack of follow up on the PEGA committee recommendations (debate). 27 February. https://www.europarl.europa.eu/doceo/document/CRE-9-2024-02-27-ITM-021_EN.html. Accessed 23 June 2024.

European Parliament and Council. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. OJ L333 (27 December), 80. https://eur-lex.europa.eu/eli/dir/2022/2555. Accessed 23 July 2024.

European Parliament and Council. (2023). Regulation 2023/2841 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. OJ L2841 (18 December), 1. https://eur-lex.europa.eu/eli/reg/2023/2841. Accessed 23 July 2024.

European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. OJ L1689 (12 July), 1. https://eur-lex.europa.eu/eli/reg/2024/1689/oj. Accessed 23 July 2024.

Gatopoulos, D. (2024). Europe's cybersecurity chief says disruptive attacks have doubled in 2024, sees Russia behind many. *AP*, 29 May. https://apnews.com/article/europe-election-cybersecurity-russia-ukraine-5b0cca725d17a028dd458df77a60440c. Accessed 23 July 2024.

Germany, Federal Office for Information Security. (2024). Wahlen in Deutschland 2024 [Elections in Germany]. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Krisen-Grosslagen/Wahlen/wahlen_node.html. Accessed 23 July 2024.

Goujard, C. (2022). European Parliament website hit by cyberattack after Russian terrorism vote. *Politico*, 23 November. https://www.politico.eu/article/cyber-attack-european-parliament-website-after-russian-terrorism/. Accessed 23 July 2024.

Martin, C. (2024). Deepfakes are here and can be dangerous, but ignore the alarmists – they won't harm our elections. *The Guardian*, 11 June. https://www.theguardian.com/commentisfree/article/2024/jun/11/deepfakes-ignore-alarmists-elections. Accessed 23 July 2024.

Mattioli, R., Malatras, A., Hunter, E. N., Biasibetti Penso, M. G., Bertram, D., & Neubert, I. (2023). *Threats 2030: Identifying emerging cyber security threats and challenges for 2030*. ENISA. March. https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030. Accessed 23 July 2024.

Roussi, A. (2023). The European Parliament has an election security problem. *Politico*, 10 December. https://www.politico.eu/article/european-parliament-election-cybersecurity-problem/. Accessed 23 July 2024.

Schickler, J. (2024). EU election campaign marred by disruption and violence. *Euronews*, 12 June. https://www.euronews.com/my-europe/2024/06/07/dutch-cyberattacks-latest-in-eu-election-campaign-marred-by-disruption-violence. Accessed 23 July 2024.

Tar, J. (2024). European Parliament's recruitment application compromised in data breach. *Euractiv*, 7 May. https://www.euractiv.com/section/cybersecurity/news/european-parliaments-recruitment-application-compromised-in-data-breach/. Accessed 23 July 2024.

TikTok. (2024). How we kept our community safe during the 2024 European Parliament elections. 9 June. https://newsroom.tiktok.com/en-eu/how-we-kept-our-community-safe-during-the-2024-european-parliament-elections. Accessed 23 July 2024.

Tomé, J. (2024). Exploring the 2024 EU election: Internet traffic trends and cybersecurity insights. *The Cloudflare Blog*, 10 June. https://blog.cloudflare.com/exploring-the-2024-eu-election-internet-traffic-trends-and-cybersecurity-insights. Accessed 23 July 2024.

US, CISA (Cybersecurity and Infrastructure Security Agency). (2024). Cybersecurity toolkit and resources to protect elections. https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections. Accessed 23 July 2024.

Author biographies

Eva Saeva *is a cybersecurity consultant at CYEN, specialising in compliance with EU law. She has more than eight years of experience working on the policy and legal aspects of cybersecurity, in various positions in the European Parliament and Commission. She completed a Ph.D. in EU Cybersecurity Law at Newcastle University, where she was also a teaching assistant in EU Law.*

Iva Tasheva *is the co-founder and cybersecurity lead at CYEN, a Brussels-based cybersecurity risk and compliance consultancy. She is a published author and regular conference speaker, an appointed member of the ENISA Ad-Hoc Working Groups on Enterprise Security and Cloud Services, and a board member of Women 4 Cyber Belgium.*