

Defending the Ballot: Legal and Policy Responses to Cyber Interference in European Elections

Associate professor **Adriana Iuliana STANCU**¹

Associate professor **Tal PAVEL**²

Abstract

This study examines Russian cyber activities targeting European political elections, focusing on how Russia uses hacking, disinformation, and influence operations to undermine democratic institutions and sway public opinion. It highlights geographic hotspots in Central and Eastern Europe and the Balkans within the broader EU context. The research addresses key questions about the specific cyber tactics Russia employs and the legal and policy measures Europe has adopted to protect electoral integrity. The study maps Russian cyber threat actors and their strategies, assessing their operational objectives. It also evaluates existing national and EU-level legal frameworks and response mechanisms against foreign electoral interference. Methodologically, the study draws from a diverse range of reliable sources, including academic research, cybersecurity reports, journalism, and official publications, to provide a balanced and comprehensive analysis. Findings reveal that Russian cyber operations continuously and systematically target European elections using sophisticated methods. Current EU responses are fragmented, lack unified standards and enforcement, and create gaps in electoral security. The study argues for a holistic, multi-level European approach, emphasising the need for unified frameworks, permanent coordination, revised sanctions, and proportionate security measures. Ultimately, the research calls for an integrated European defence grounded in the rule of law, highlighting legally binding solidarity and institutional coherence among member states to strengthen democratic resilience.

Keywords: elections, cyber security, policy, Russia, attacks, European Union.

JEL Classification: K16

DOI: 10.62768/PLPA/2026/15/1/11

Please cite this article as:

Stancu, Adriana Iuliana & Tal Pavel „Defending the Ballot: Legal and Policy Responses to Cyber Interference in European Elections”, *Perspectives of Law and Public Administration* 15, no. 1 (March 2026): 158-176.

Article History

Received: 10 December 2025

Revised: 12 January 2026

Accepted: 20 February 2026

1. Introduction

In recent years, we have witnessed ongoing attempts to interfere with, breach, and manipulate election processes globally, influencing the democratic process in favor

¹ Adriana Iuliana Stancu - Faculty of Law and Administrative Sciences, “Dunarea de Jos” University of Galati, Romania, adriana.stancu@ugal.ro, ORCID: 0000-0001-6259-5116.

² Tal Pavel - Faculty of Law and Administrative Sciences, “Dunarea de Jos” University of Galati, Romania, tal@cybureau.org, ORCID: 0000-0002-4046-0867.

of the strategic benefits of the aggressor. These threats are carried out using cyber and information warfare, including both covert cyberattacks and overt efforts to influence public opinion and undermine the stability, integrity and legitimacy of democratic institutions and processes, also known as “Foreign Information Manipulation and Interference (FIMI)”³. In recent years, we have witnessed ongoing attempts to interfere with, breach, and manipulate election processes globally, influencing the democratic process in favour of the strategic benefits of the aggressor. These threats are carried out using cyber and information warfare, including both covert cyberattacks and overt efforts to influence public opinion and undermine the stability, integrity and legitimacy of democratic institutions and processes, also known as “Foreign Information Manipulation and Interference (FIMI)”⁴.

A U.S. Intelligence report from January 2017 assessed that Russia conducted an extensive campaign to undermine the chances of the Democratic candidate, Hillary Clinton, and to promote the Republican candidate, Donald Trump, in the 2016 presidential elections. This acted as a wake-up call for European countries preparing for elections in 2017, focusing attention on Russia as a potential perpetrator during elections⁵. Russia is considered one of the principal threat actors and the most active one, performing highly adaptable cyber and influence campaigns that tailor its strategies to geopolitical and local political shifts. In Europe, the Russian campaigns target mainly Ukraine, in addition to its western allies, including the US, NATO, G7 and EU countries, focusing on France, Germany, and Poland, in addition to Moldova. To undermine the democratic institutions and processes and weaken European stands, especially toward the Russian Full-scale invasion of Ukraine, in February 2022, Russia performed dozens of cyber and Foreign Information Manipulation & Interference (FIMI) attacks during European election campaigns, using hacking methods and influence manipulations⁶.

The scope of the paper encompasses geographic areas in Central-Eastern Europe and the Balkans, identified as hotspots, as well as an EU-wide perspective, focusing on incidents from the Bronze Soldier Crisis of 2007 to the present. To address

³ European Union External Action Service (EEAS). (2025, March 14). *Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)*. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en; Strategic Communication and Foresight (SG.STRAT). (2025). *3rd EEAS Report on Foreign Information Manipulation and Interference Threats*, <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3rd-ThreatReport-March-2025-05-Digital-HD.pdf>, accessed on 10 January 2026.

⁴ Idem

⁵ Marie Baezner, Patrice Robin, *Hotspot Analysis: Cyber and Information Warfare in elections in Europe*, December 2017, Center for Security Studies (CSS), ETH Zürich, <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-08.pdf>, accessed on 10 January 2026; David Siman-Tov, Gabi Siboni, and Gabrielle Arelle, „Cyber Threats to Democratic Processes”. *Cyber, Intelligence, and Security*, Volume 1, No. 3, December 2017: 51-63, https://www.inss.org.il/wp-content/uploads/2018/01/CyberENG1.3_6-53-65.pdf, accessed on 10 January 2026.

⁶ European Union External Action Service (EEAS). (2025, March 14). *Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)*; Strategic Communication and Foresight (SG.STRAT). (2025). *3rd EEAS Report on Foreign Information Manipulation and Interference Threats*.

the scope of the paper, the research aims to analyse two questions: (RQ1) What cyber measures has Russia taken to impact political elections in Europe? (RQ2) What legal countermeasures have been adopted by affected states, the European Union, and the affected countries to safeguard electoral integrity? The paper's core findings centre on how Russian cyber activities, ranging from disinformation campaigns to cyberattacks, have targeted elections with the intent to undermine democratic institutions, influence political outcomes, and erode trust in European governance. Therefore, its significance lies in mapping both the problem of Russian cyber influence through legal loopholes and the necessary steps for the EU to enhance its defences, while maintaining the rule of law and democratic freedoms⁷.

2. Methodology

This study prioritised the careful selection of diverse and highly reliable sources to ensure the robustness and credibility of the research findings. The criteria guiding the source selection process were grounded in key principles aimed at achieving comprehensive coverage and scholarly rigour. Relevance was paramount, as every source was chosen to directly address the research topic and questions, thereby maintaining focus on the study's core objectives. This ensured that the information and arguments presented were closely aligned with the study's thematic scope. Reliability was another critical factor, with preference given to sources recognised for their accuracy, transparency, and methodological soundness. This includes peer-reviewed academic publications, well-established cyber research companies known for rigorous analysis, and official documents issued by authoritative institutions. Such a criterion minimised the risk of bias or misinformation affecting the research outcomes. Diversity in capturing a multifaceted understanding of the subject matter.

The study integrated a broad spectrum of source types, encompassing primary data, secondary scholarly interpretations, and current journalistic reporting. This blend included academic articles for theoretical and empirical depth, analytical reports from cybersecurity firms providing industry insights, investigative journalism offering contemporary context, and official publications from government and intergovernmental organisations to anchor the research in recognised facts and policy frameworks. By adhering to these principles - relevance, reliability, and diversity - the methodology ensured a balanced, thorough, and credible evidence base underpinning the study's conclusions.

⁷ Daniëlle Flonk, Markus Jachtenfuchs, and Anke Obendiek, "Controlling Internet Content in the EU: Towards Digital Sovereignty," *Journal of European Public Policy*, vol. 31, no. 8 (2024): 2316–2342, <https://doi.org/10.1080/13501763.2024.2309179>. Also see Bente Kalsnes and Niels Nagelhus Schia, "Protecting Democracy: Comparing Codes of Conduct for Generative AI Use during Elections," *Information, Communication & Society*, March 2026: 1–17, <https://doi.org/10.1080/1369118X.2026.2647362>.

3. Russian Cyber Influence in European Elections: A Conceptual Framework

The National Institute of Standards and Technology (NIST) defines Cyberspace as “A global domain within the information environment consisting of the interdependent network of information systems infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”⁸ Most of the sources, researchers and definitions refer to cyberspace as consisting of three layers:

- Physical Layer - the tangible components of the IT infrastructure and physical domains;
- Logical Layer - software, protocols, and configurations that govern the operation of the digital infrastructure;
- Cyber-Persona Layer - human element in cyberspace, including user identities, roles, behaviours, and interactions with digital systems. (U.S AIR FORCE, 2023).

The National Institute of Standards and Technology (NIST) defines Computer Network Operations (CNO) as “the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace”⁹. CNO includes three known types of attacks:

- Computer network exploitation (CNE) – refers to intelligence gathering, espionage and reconnaissance operations.
- Computer Network Attack (CNA) – refers to attacks for destruction.
- Computer Network Influence (CNI) – refers to attacks for influence.

Bonfanti defines Cyber Influence Operations (CIOs) as “illegitimate (sometimes illegal) activities that are run in cyber-space, leverage the distributed vulnerabilities of cyber-space, and rely on cyber-related tools and techniques to affect an audience’s choices, ideas, opinions, emotions or motivations, and interfere with its decision-making processes”¹⁰. Dreikhausen and Salvi consider Cyber Influence Operations as a “subset of influence operations that combine the use of force on cyber infrastructure with a broader strategy of interference in the human domain, that is, the dimension of conflict and warfare that centres on competing actors’ efforts to influence human perception in their pursuit of strategic objectives”¹¹. Brangetto and Veenendaal predicted in 2016 that cyber influence operations “will become more prevalent because they offer the opportunity to undermine an opponent’s credibility

⁸ National Institute of Standards and Technology (NIST). (n.d.-b). *Cyberspace*. Retrieved August 17, 2025, from <https://csrc.nist.gov/glossary/term/cyberspace>.

⁹ National Institute of Standards and Technology (NIST). (n.d.-a). *Computer Network Operations (CNO)*. Retrieved August 17, 2025, from https://csrc.nist.gov/glossary/term/computer_network_operations.

¹⁰ Matteo E. Bonfanti, „An Intelligence-Based Approach to Countering Social Media Influence Operations”. *Romanian Intelligence Studies Review*, 19–20, 2018: 47–68. https://www.animv.ro/wp-content/uploads/2019/06/RRSI-no.-19_20.pdf, accessed on 10 January 2026.

¹¹ Viola Fee Dreikhausen, Andrea Salvi, *From cyber to hearts and minds*, European Union Institute for Security Studies. (2023, November 8), <https://www.iss.europa.eu/publications/briefs/cyber-hearts-and-minds>, accessed on 10 January 2026.

with little risk of escalation¹²“.

Russian campaigns against European countries may be considered cyber influence operations, aimed at undermining the stability of democratic systems and processes to serve Russian strategic purposes. Those operations are done against all three layers of cyberspace and by all three types of Computer Network Operations (CNO). Meaning, using hacking methods, to steal information and gather intelligence (CNE), implant malware for the destruction of Information and operating systems (CNA), and influence manipulations (CNI). Therefore, cyber influence operations are conducted on various digital platforms and methods, such as hacking to gather intelligence or disrupt operational systems, leaking information, disseminating disinformation, manipulating social media, and engaging in cyber espionage¹³. Various sources attribute dozens of cyber threat groups to Russia, operating for years, around the globe, while the most well-known are APT 28 and APT 29¹⁴, performing sabotage and espionage for strategic and political purposes and integrating cyber operations into a strategy capable of achieving political objectives, mainly to destabilise the democratic process, to undermine U.S global influence and European support of Ukraine¹⁵. Sometimes the Russian political interference in European countries is visible, and sometimes it is covert.

A chilling demonstration of cyber operations against the European political system was the claim that a plane carrying European Commission President Ursula von der Leyen was hit by GPS interference. This interference disabled the use of electronic navigational aids while she was approaching the airport at Plovdiv during her planned visit to Bulgaria. Arianna Podestà, deputy spokesperson of the European Commission, stated that “We can confirm there was GPS jamming but the plane landed safe,” adding that the Commission received information from Bulgarian authorities indicating that “they suspect this blatant interference was carried out by Russia”¹⁶. The findings suggest an overarching, comprehensive, and ongoing Russian effort to manipulate

¹² Pascal Brangetto, & Matthijs A. Veenendaal. „Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations”. In N. Pissanidis, H. Rõigas, M. Veenendaal (Eds.), *2016 8th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, 2016, 113–126, <https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf>, accessed on 10 January 2026.

¹³ Viola Fee Dreikhausen, Andrea Salvi, *op. cit.* (2023, November 8); Peter B.M.J. Pijpers, P.A.L. Ducheine, „Influence Operations in Cyberspace – How They Really Work” (September 24, 2020). *Amsterdam Law School Research Paper No. 2020-61*, Amsterdam Center for International Law No. 2020-31, Available at <http://dx.doi.org/10.2139/ssrn.3698642>.

¹⁴ Electronic Transactions Development Agency. (n.d.). *A Threat Actor Encyclopedia*. Retrieved August 23, 2025, from <https://apt.etda.or.th/cgi-bin/listgroups.cgi>; Sai. (2024, May 30). *The Nefarious Five: Top Russian State-Sponsored Cyber Threat Groups*. NetSecurity.Com. <https://www.netsecurity.com/the-nefarious-five-top-russian-state-sponsored-cyber-threat-groups/>, accessed on 10 January 2026.

¹⁵ Pascal Brangetto, & Matthijs A. Veenendaal, *op. cit.*, pp. 113–126; Cynet. (2025, July 23). *What Are Advanced Persistent Threats (APT) & 5 Defensive Measures*. <https://www.cynet.com/advanced-persistent-threat-apt-attacks/>, accessed on 10 January 2026; Paloalto Networks. (n.d.). *What Is an Advanced Persistent Threat?*, <https://www.paloaltonetworks.com/cyberpedia/what-is-advanced-persistent-threat-apt>, accessed on 10 January 2026.

¹⁶ Paloalto Networks. (n.d.). *What Is an Advanced Persistent Threat?*, <https://www.paloaltonetworks.com/cyberpedia/what-is-advanced-persistent-threat-apt>, accessed on 10 January 2026.

European democratic institutions and processes through various means, including cyber influence operations, aimed at targeting parliaments, parties, ministries and the election campaigns. These operations are primarily carried out by the most active and destructive cyber threat actors affiliated with the Russian establishment, namely APT 28 and APT 29.

Such cyber influence operations include, among others, Hacking, DDoS and Email compromise, in addition to Fake news, Internet trolls and bots¹⁷:

- Infrastructure Exploitation – Gathering or distorting data or functionality of IT systems or networks through actions like reconnaissance or data collection.
- Vote Manipulation – Altering vote counts, vote input, transmission, or the process of tallying votes to change the actual outcome, beyond just spreading false results or casting doubt.
- Strategic Publication – Illicitly obtained data (usually through exploitation) that is publicly released to embarrass or negatively impact the target.
- False-Front Engagement – Creating a fake public identity used to communicate, provoke, organize, or interact with others under false pretences.
- Sentiment Amplification – Boosting the spread and visibility of viewpoints. This can be overt (where the actor is identifiable) or covert (where the actor is obscured via fake identities or minimized attribution).
- Fabricated Content – Distribution of false or distorted information, including misleading statements about votes, election results, or other key facts.

4. National and Supranational Responses

To address the cyber information operation attributed to Russia, the European Union and European countries are taking various measures.

Diplomacy. Over the years, several countries have expelled and even severed diplomatic ties due to cyberattacks. In December 2019, the U.S. expelled 35 Russian diplomats over cyber-attack allegations of interference in the presidential elections¹⁸, and again in April 2021 for the same reason¹⁹. As part of this case, Poland expelled three more Russian diplomats²⁰. Albania even cut its diplomatic relations with Iran due to its cyberattacks on various governmental institutions²¹.

¹⁷ Laura Galante, Shaun Ec (2018, September 11). *Defining Russian election interference: An analysis of select 2014 to 2018 cyber enabled incidents*. Atlantic Council. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/defining-russian-election-interference-an-analysis-of-select-2014-to-2018-cyber-enabled-incidents-2/>, accessed on 10 January 2026.

¹⁸ BBC News. (2016b, December 29). *US expels Russian diplomats over cyber attack allegations*. <https://www.bbc.com/news/world-us-canada-38463025>, accessed on 10 January 2026.

¹⁹ Deutsche Welle. (2021, April 15). *US expels Russian diplomats, issues sanctions*. <https://www.dw.com/en/us-expels-russian-diplomats-and-issues-sanctions-over-solarwinds-hacking-attack/a-57215141>, accessed on 10 January 2026.

²⁰ Polska Agencja Prasowa. (2021, April 15). *Poland expels three Russian diplomats over cyber attacks*. <https://www.pap.pl/en/news/news%2C852871%2Cpoland-expels-three-russian-diplomats-over-cyber-attacks.html>, accessed on 10 January 2026.

²¹ Daryna Antoniuk, (2023, December 27). *Albanian parliament, telecom company hit by cyberattacks*.

European regional initiatives. The European Union established several institutions to confront cyber and hybrid threats:

- **The East StratCom Task Force** – was created by the EU in 2015 to counter pro-Russian disinformation and improve strategic communications in the EU's Eastern Neighbourhood, which includes Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine. Its main objectives are to effectively communicate EU policies, strengthen media freedom and independent media in the region, and improve the EU's capacity to forecast and respond to disinformation activities by external actors²².

- **The European Union Agency for Cybersecurity** – an agency dedicated to “achieving a high common level of cybersecurity across Europe”²³.

- **Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)** – an autonomous, network-based international organisation of 36 Participating States, established in 2017 by the first nine Participating States, NATO and the EU, to counter hybrid threats²⁴.

- **CERT-EU** – Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies, which “collects, manages, analyses and shares information with EU institutions, bodies and agencies on threats, vulnerabilities and incidents related to unclassified ICT infrastructure”²⁵.

- **Hybrid Rapid Response Teams** – dedicated teams to be deployed upon request to prepare against and counter hybrid threats and campaigns, and provide tailored and targeted short-term assistance to member states, as part of the EU hybrid toolbox²⁶.

- **Western Balkans Cyber Capacity Centre** – a regional-scale training centre in Podgorica established by France, Slovenia, and Montenegro for “support to the Western Balkans countries through increased cooperation and training in the field of cybersecurity and cybercrime”²⁷.

Sanctions. The EU has imposed sanctions on Russian individuals, entities, and

Recorded Future News. <https://therecord.media/albanian-parliament-telecom-company-hit-by-cyberattacks>, accessed on 10 January 2026; Daryna Antoniuk, (2024, February 2). *Iran-linked hackers claim attack on Albania's Institute of Statistics*. Recorded Future News. <https://therecord.media/iran-linked-hackers-claim-attack-on-albania-census-org>, accessed on 10 January 2026; Lazzar Semini, (2022, September 7). *Albania cuts diplomatic ties with Iran over July cyberattack*. AP News. <https://apnews.com/article/nato-technology-iran-middle-east-6be153b291f42bd549d5ecce5941c32a>, accessed on 10 January 2026.

²² The European Union Agency for Cybersecurity (ENISA). (n.d.). *ENISA*, <https://www.enisa.europa.eu/>.

²³ Idem.

²⁴ Hybrid CoE. (n.d.). *The European Centre of Excellence for Countering Hybrid Threats*. Retrieved September 7, 2025, from <https://www.hybridcoe.fi/>.

²⁵ European Union. (n.d.). *CERT-EU – Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies*. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/cybersecurity-service-union-institutions-bodies-offices-and-agencies-cert-eu_en, accessed on 10 January 2026.

²⁶ European Union. (2024, May 21). *Hybrid threats: Council paves the way for deploying Hybrid Rapid Response Teams*. <https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/hybrid-threats-council-paves-the-way-for-deploying-hybrid-rapid-response-teams/>, accessed on 10 January 2026.

²⁷ Western Balkans Cyber Capacity Centre. (n.d.). *Western Balkans Cyber Capacity Centre*. Retrieved October 8, 2025, from <https://wb3c.org/>.

military intelligence units involved in cyberattacks, disinformation campaigns, and destabilisation activities. In 2022, the EU set up 2022 a “Freeze and Seize Task Force” to “explore links between assets belonging to persons listed under EU sanctions and criminal activities” and to “strengthen coordination at operational level to ensure effective enforcement of EU sanctions across all Member States”²⁸.

In July 2023, restrictive measures were imposed by the European Union against seven Russian individuals and five entities responsible for conducting a “digital information manipulation campaign called 'RRN' (Recent Reliable News), aimed at distorting information and disseminating propaganda in support of Russia’s war of aggression against Ukraine”²⁹.

In October 2024, the European Council unveiled a new sanctions framework that focuses on Russian individuals and entities who “undermine the EU’s values, security, and the integrity of its member states” by a broad range of activities “including cyber-attacks, information manipulation and interference campaigns, cases of arson, vandalism and sabotage, including against our critical infrastructure as well as instrumentalisation of migration and other disruptive actions”³⁰. In December 2024, the European Union imposed sanctions on Russian cyber actors for conducting attacks and disinformation campaigns abroad³¹, and another sanctions package targeting 21 individuals and six entities for “Russia’s destabilising actions abroad”³². In May 2025, the European Council decided to prolong the restrictive measures against “cyber-attacks threatening the EU and its member states” for a further year, until 18 May 2026, while the legal framework (sanctions regime) for these measures is extended for three years until 18 May 2028³³.

²⁸ European Union. (n.d.). *CERT-EU – Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies*. Retrieved September 9, 2025, from https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/cybersecurity-service-union-institutions-bodies-offices-and-agencies-cert-eu_en.

²⁹ The Council of the EU. (2023, July 28). *Information manipulation in Russia’s war of aggression against Ukraine: EU lists seven individuals and five entities*. <https://www.consilium.europa.eu/en/press/press-releases/2023/07/28/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-seven-individuals-and-five-entities/>, accessed on 10 January 2026.

³⁰ The Council of the EU. (2024b, October 8). *Hybrid threats/Russia: Statement by the High Representative on behalf of the EU on Russia’s continued hybrid activity against the EU and its Member States*. <https://www.consilium.europa.eu/en/press/press-releases/2024/10/08/hybrid-threatsrussia-statement-by-the-high-representative-on-behalf-of-the-eu-on-russia-s-continued-hybrid-activity-against-the-eu-and-its-member-states/>, accessed on 10 January 2026.

³¹ James Coker, (2024, December 17). *EU Sanctions Russian Cyber Actors for “Destabilizing Actions.”* Infosecurity Magazine. <https://www.infosecurity-magazine.com/news/eu-sanctions-russian-cyber-actors/>, accessed on 10 January 2026.

³² The Council of the EU. (2025b, May 20). *Russian hybrid threats: EU lists further 21 individuals and 6 entities and introduces sectoral measures in response to destabilizing activities against the EU, its member states and international partners*. <https://www.consilium.europa.eu/en/press/press-releases/2025/05/20/russian-hybrid-threats-eu-lists-further-21-individuals-and-6-entities-and-introduces-sectoral-measures-in-response-to-destabilising-activities-against-the-eu-its-member-states-and-international-partners/>, accessed on 10 January 2026.

³³ The Council of the EU. (2025a, May 12). *Cyber-attacks: Council extends sanctions and legal framework*. <https://www.consilium.europa.eu/en/press/press-releases/2025/05/12/cyber-attacks-council-extends-sanc>

Cybersecurity Frameworks. European states are enhancing their cybersecurity frameworks and resilience against cyberattacks based on the assessment that “Russia will very probably mount cyber operations against Europe in the coming years, irrespective of developments in the Russia-Ukraine war”³⁴. The European Parliament adopted in October 2019 the “Foreign electoral interference and disinformation in national and European democratic processes”³⁵.

The growing problem of foreign electoral interference, as part of hybrid warfare, requires a coordinated EU-level response that combines security, legal, and technological measures. The key points include:

1. The significant role of disinformation, notably originating from Russian campaigns, but also from other foreign actors.

2. Recognition that protecting elections depends on a multifaceted approach involving governments, internet and social media companies, and civil society, without compromising freedom of expression.

3. The importance of media pluralism, protection of privacy and personal data, and civic education to build resilience against disinformation.

4. Concerns about circumvention of campaign finance transparency rules by foreign forces to influence elections.

5. Calls for increased EU and national funding for countering disinformation, supporting responsible journalism, promoting public service media, and strengthening democratic media in EU neighboring and candidate countries.

6. Urgency to classify electoral equipment as critical infrastructure to apply cybersecurity protections.

7. Advocacy for a legal framework to tackle hybrid threats at the EU and international levels.

8. Emphasis on cross-sector cooperation and the role of whistle-blowers as democratic safeguards.

9. Support for EU institutions and Member States to take decisive, collective action to protect the integrity of democratic processes and upcoming elections in Europe.

The resolution also highlights the EU's dependence on foreign technology as a vulnerability and urges the development of European alternatives. It highlights NATO's role in resisting disinformation. It calls on the European Commission and Member States to engage with stakeholders and international partners to comprehensively strengthen their defences against foreign interference.

In June 2020, the European Parliament adopted the “Setting up a special committee on foreign interference in all democratic processes in the European Union, including disinformation, and defining its responsibilities, numerical strength and term

tions-and-legal-framework/, accessed on 10 January 2026.

³⁴ Dragonfly Intelligence. (2025, April 3). *Europe | Outlook for Russian cyber operations*. <https://dragonflyintelligence.com/news/europe-outlook-for-russian-cyber-operations/>, accessed on 10 January 2026.

³⁵ European Parliament. (2019, October 10). *Foreign electoral interference and disinformation in national and European democratic processes*. https://www.europarl.europa.eu/doceo/document/TA-9-2019-0031_EN.html, accessed on 10 January 2026.

of office”³⁶. Key points of the decision include:

1. Recognition that foreign interference in democratic processes is a recurring, systematic issue that threatens the functioning of democracy and the values of the EU.
2. The committee's work will complement, not duplicate, the existing parliamentary committees responsible for related legislative areas.
3. Confidential evidence and testimonies may be heard in camera, with public transparency maintained for meeting attendance and minutes.
4. The committee will consist of 33 members and have a term of 12 months starting from its first meeting.
5. It may issue a mid-term report. It will present a final report with factual findings and recommendations for measures to counter foreign interference, while respecting the competences of other standing committees.

In February 2024, the European Parliament issued a resolution on the “allegations of Russian interference in the democratic processes of the European Union”, expressing grave concern about Russia's ongoing efforts to undermine European democracy through interference, disinformation, and funding of political actors. It condemns Russian hybrid warfare tactics, including falsification of history, cyberattacks, support for extremist and far-right forces, and infiltration of EU institutions. The Parliament calls for stronger internal reforms to protect against foreign influence, improve transparency, enhance integrity and accountability rules, and build a more secure culture within EU institutions. It supports investigations into alleged Russian interference, cooperation with national authorities, and stricter measures, including sanctions against Russia and its supporters. The resolution emphasizes the importance of safeguarding the integrity of upcoming elections and urges coordinated EU and national efforts to counter disinformation and foreign interference³⁷.

Public Awareness. The European External Action Service (EEAS) built up capabilities to identify, analyse and respond to FIMI since 2015, “when EU Member States first called on the EEAS to address Russian disinformation campaigns in the context of Russia’s aggression against Ukraine,” aiming to “deliver more targeted, impactful and coordinated responses to FIMI to protect the EU’s Common Foreign and Security Policy, democratic processes and citizens, as well as our partners worldwide”. The project activities to confront Russia’s FIMI attacks are described as “the flagship project of the EEAS”³⁸. The U.K. has implemented the Foreign Influence Registration Scheme (FIRS), which “requires individuals (in some cases including journalists) and

³⁶ European Parliament. (2020, June 18). *Setting up a special committee on foreign interference in all democratic processes in the European Union, including disinformation, and defining its responsibilities, numerical strength and term of office*. https://www.europarl.europa.eu/doceo/document/TA-9-2020-0161_EN.html, accessed on 10 January 2026.

³⁷ European Parliament. (2024, February 8). *Russiagate: allegations of Russian interference in the democratic processes of the European Union*. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0079_EN.html, accessed on 10 January 2026.

³⁸ European Union External Action Service (EEAS). (2025, March 14). *Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)*. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en, accessed on 10 January 2026.

organisations (in some cases including universities, NGOs, charities and the media) acting on behalf of foreign powers to register their activities, as a transparency and accountability measure”.

Official Statements and media coverage. Various European media outlets, research institutions, and governmental agencies report on the alleged Russian cyber influence operations, the investigations and analysis, and blame Russia publicly for those operations³⁹. For example, the official condemnations of NATO and the European Union and its Member States, together with international partners, of “the malicious cyber campaign conducted by the Russia-controlled Advanced Persistent Threat Actor 28 (APT28)⁴⁰”. Some official statements warned of expected Russian cyber operations and election manipulation, as seen in cases such as Moldova⁴¹ and Germany⁴².

³⁹ BBC News. (2016a, May 13). *Russia “was behind German parliament hack.”* <https://www.bbc.com/news/technology-36284447>, accessed on 10 January 2026; Nina dos Santos & Tim Lister, (2018, July 4). *Arron Banks: UK investigates alleged Russian links to Brexit backer.* CNN. <https://edition.cnn.com/2018/07/04/uk/uk-brexiteer-russia-links-arron-banks-intl/index.html>, accessed on 10 January 2026; Andy Greenberg, (2017, May 9). *The NSA Confirms It: Russia Hacked French Election ‘Infrastructure.’* WIRED. <https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/>, accessed on 10 January 2026; Institute for Strategic Dialogue. (2025a, July 10). *Country Report: Assessment of Foreign Information Manipulation and Interference (FIMI) in the 2025 German Federal Election.* <https://www.isdglobal.org/isd-publications/country-report-assessment-of-foreign-information-manipulation-and-interference-fimi-in-the-2025-german-federal-election/>, accessed on 10 January 2026; Institute for Strategic Dialogue. (2025b, August 11). *Election Report: Assessment of Foreign Manipulation and Interference in the 2025 Polish Presidential Election.* <https://www.isdglobal.org/isd-publications/election-report-assessment-of-foreign-manipulation-and-interference-in-the-2025-polish-presidential-election/>, accessed on 10 January 2026; Politietts Sikkerhetstjeneste. (2020, December 8). *Datainnbruddet mot Stortinget er ferdig etterforsket.* <https://www.pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/>, accessed on 10 January 2026; Reuters. (2017, September 4). *Merkel ally cites thousands of cyber-attacks from Russian IP addresses.* <https://www.reuters.com/article/usgermany-election-cyber/merkel-ally-cites-thousands-of-cyber-attacks-from-russian-ip-addresses-idUSKCN1BF1FA/>, accessed on 10 January 2026; Jon Rogers, (2017, May 6). *French election - publishing Macron emails could be a crime.* Express. <https://www.express.co.uk/news/world/801242/French-election-Macron-emails-crime-electoral-commission-Le-Pen>, accessed on 10 January 2026.

⁴⁰ Council of the European Union (2024a, May 3). *Cyber: Statement by the High Representative on behalf of the EU on continued malicious behavior in cyberspace by the Russian Federation.* https://www.consilium.europa.eu/en/press/press-releases/2024/05/03/cyber-statement-by-the-high-representative-on-behalf-of-the-eu-on-continued-malicious-behaviour-in-cyberspace-by-the-russian-federation/?utm_source=brev&utm_campaign=AUTOMATED%20-%20Alert%20-%20Newsletter&utm_medium=email&utm_id=320, accessed on 10 January 2026; NATO. (2024, May 3). *Statement by the North Atlantic Council concerning malicious cyber activities against Germany and Czechia.* https://www.nato.int/cps/en/natohq/official_texts_225229.htm, accessed on 10 January 2026.

⁴¹ Lola Boom, (2025, July 30). *Moldova’s president warns of ‘unprecedented’ Russian election meddling.* <https://www.politico.eu/article/moldova-warns-russian-election-interference-mai-sandu-cyberattack-disinformation/>, accessed on 10 January 2026.

⁴² Lorne Cook, (2021, September 24). *EU warns Russia over cyberattacks ahead of German elections.* AP News. <https://apnews.com/article/technology-russia-elections-media-foreign-policy-a9abb7e00e4430c402b07ae14cdd9c8c>, accessed on 10 January 2026.

5. European Regulatory Framework; Lack of a Common Unified Regulation

The EU's legal framework to counteract cybercrime has been reinforced in recent years by the introduction of directive NIS2 (EU) 2022/2555 of 14 December 2022, that has come into effect as from 15 January 2023, replacing directive NIS (EU) 2016/1148 of 6 July 2016. Despite these efforts, there is no common European regulation on the electoral process regarding the protection of electoral integrity in the virtual environment. Although it is a fundamental right and an essential condition of the rule of law, the right to vote and to be elected is protected by each Member State with its own non-uniform legal instruments, leading to an uneven and fragmented European framework. In addition to the legal problems arising from the lack of a common regulatory framework, there is also the danger of sending an undesirable message.

People perceive the Union as a territory with common rules. However, in the field of electoral security, there are no common or even proportional mandatory rules. Some states allocate a considerable budget to the digital protection of the electoral process, while others ignore the vulnerabilities of the online environment. It seems clear that, under these conditions, attackers find it relatively easy to exploit vulnerabilities. Recent research confirms that non-uniform regulation increases the risk of cross-border interference while weakening public confidence in the European electoral process as a whole. On the other hand, the current regulatory framework only tangentially regulates the electoral process, as it was not designed to directly address the challenges posed by digital vote manipulation.⁴³ Comparative statistics show that vulnerabilities have decreased significantly in countries that have strengthened their national legislation in this area. Still, at the European level, the common risk remains high without uniform legislation. This is why adopting a unified European regulatory framework for protecting the electoral process has become a priority for ensuring public confidence in European values and, implicitly, in the rule of law.

5.1. Regulatory Ambiguities in the Regulation and Attribution of Legal Liability

Establishing causality and attributing legal liability is the most challenging step in the case of cyber-attacks on electoral processes. In common parlance, people want to know who is to blame. From a legal point of view, the answer to this question is not easy to formulate, even when technical data points to a state actor or a known criminal group; substantiating legal action to establish liability and punish the perpetrators is a laborious and challenging process⁴⁴. This uncertainty has direct consequences for establishing legal liability. Who should be punished in the event of an attack that fatally affects the infrastructure of an election? The electoral authority, the IT service provider,

⁴³ Dennis W. J. Broeders, "Cyber Intelligence and International Security: Breaking the Legal and Diplomatic Silence?," *Intelligence and National Security*, vol. 39, no. 7 (2024): 1213–1229, <https://doi.org/10.1080/02684527.2024.2398077>.

⁴⁴ Peter B.M.J. Pijpers, P.A.L. Ducheine, *op. cit.* (2020).

the online platforms that did not stop the spread of disinformation messages, or the state from whose territory the attack originated? The lack of clear criteria means that blame is passed around like a ball from one institution to another. At the same time, the victims — citizens and their trust in the electoral process — are left without adequate protection⁴⁵.

Moreover, in the absence of a specific legal framework, states respond differently and disproportionately; some apply prompt diplomatic sanctions, while others hesitate to decide, citing a lack of evidence. The consequence of this legal reality is an uneven and fragile European response that jeopardizes the idea of unity. As the literature points out, the issue of establishing responsibility is not only technical but also legal and political, because what is considered “sufficient evidence” differs from one state to another. In accordance with the regulations as well as the experts in the field, identifying an act of cyber warfare with an official State actor is an elevated level of evidentiary standards. The fact that the technical identification can be done does not by itself equate to legal attribution; this is because the two are not mutually exclusive. Specifically, Tsagourias and Farrell⁴⁶ pointed out that in international law there is a level of proof known as the 'Standard of Sufficient Evidence', which requires the parties to provide convergent, credible, and verifiable evidence supporting their conclusions about the states' involvement, specifically that it managed, supported or accepted the operation in question.

In the absence of uniform rules on establishing legal liability, the defense of European democracy lacks a solid foundation. This reality benefits the perpetrators of attacks, allowing them always to be one step ahead of the law.

Inefficiency of the International Sanctions System. The adoption at the European level, starting in 2019, of a uniform cyber sanctions regime was considered an act of courage. The message conveyed to the public was that interference in democratic processes would not go unpunished. However, practice has shown once again that there is a big difference between intention and result. Enforcement procedures are cumbersome, and the actors concerned find ways to circumvent the restrictions imposed. At the same time, many of these sanctions have been challenged in the Court of Justice of the European Union, citing a lack of sufficient evidence. Some listings were cancelled by the CJEU on evidentiary grounds, which has substantially diminished their ultimate purpose, namely, general prevention⁴⁷. Political ones compound legal problems. Some officials use the sanctions imposed as genuine political victories, even though, beyond such rhetoric, cybercriminal groups continue to operate freely behind intermediary structures. If there is no system to monitor the enforcement of these sanctions, the legal framework is only symbolic⁴⁸. The inefficiency of the current

⁴⁵ Matteo E. Bonfanti, *op. cit.*, pp. 47–68.

⁴⁶ Nicholas Tsagourias, Michael Farrell, „Cyber Attribution: Technical and Legal Approaches and Challenges”, *European Journal of International Law*, Volume 31, Issue 3, August 2020: 941–967, <https://doi.org/10.1093/ejil/chaa057>.

⁴⁷ James Coker, *op. cit.* (2024).

⁴⁸ The Council of the EU. (2024b, October 8). *Hybrid threats/Russia: Statement by the High Representative on behalf of the EU on Russia's continued hybrid activity against the EU and its Member States*. <https://>

sanctioning system not only means that those who instigate and organize attacks go unpunished, but also that they can and do continue to exploit legislative loopholes and procedural gaps. Literature confirms this vulnerability, highlighting that, to be effective, a sanction must be swift, uniform, and severe in its application. In its current form, the European response to this type of crime remains fragmented and predictable, which considerably diminishes its general prevention capacity.

Security vs. freedom. Protecting electoral processes against cyber-attacks and disinformation campaigns is a technical and moral challenge because the protective measures target democratic social values guaranteed by constitutions. Interventions by authorities to limit the spread of fake news or block access to platforms that facilitate information manipulation directly or indirectly restrict freedom of expression. That is why we wonder whether it is possible to defend democracy without indirectly curtail the fundamental rights that define it.

The European Union has adopted the Code of Practice on Disinformation, revised in 2022. However, there is a risk that, without clear criteria, what is considered “disinformation” today could be viewed in the future as merely uncomfortable political discourse. Another considerable risk is the abuse of law, as civil society constantly warns of the possibility that security measures could become veritable instruments of censorship⁴⁹.

Recent studies confirm the existence of social tensions caused by the inability to ensure cybersecurity in electoral processes without indirectly affecting democratic values. On the one hand, there is a need to combat campaigns orchestrated by foreign actors, who have proven that they can influence opinions and electoral results⁵⁰. On the other hand, restrictive regulations may undermine the very fundamental values that are meant to be protected by fundamental state laws. Without a doubt, freedom of expression and political pluralism are the foundations of the rule of law, values that cannot be undermined even in the name of security. In the absence of proportionality between electoral security and respect for fundamental rights, there is a possibility that the measures taken will create more problems than solutions.⁵¹ The real challenge for the European Union remains finding strict rules that discourage and even stop hybrid attacks without restricting freedom of expression or diversity of opinion.

www.consilium.europa.eu/en/press/press-releases/2024/10/08/hybrid-threatsrussia-statement-by-the-high-representative-on-behalf-of-the-eu-on-russia-s-continued-hybrid-activity-against-the-eu-and-its-member-states/, accessed on 10 January 2026.

⁴⁹ European Parliament. (2019, October 10). *Foreign electoral interference and disinformation in national and European democratic processes*. https://www.europarl.europa.eu/doceo/document/TA-9-2019-0031_EN.html, accessed on 10 January 2026.

⁵⁰ Viola Fee Dreikhausen, Andrea Salvi, *op. cit.* (2023, November 8).

⁵¹ Yuxuan Lei, “The Role of Political Actors’ Preference Variation in the Decision-Making Process of the European Union,” *Social Sciences* vol. 14, no. 4 (2025): Article 193, <https://doi.org/10.3390/socsci14040193>.

5.2. Cross-border Cooperation between Domestic Legislation and European Efficiency

The cross-border nature of cyber-attacks is specific to this type of crime. These attacks have no state borders and are planned, disseminated, and executed in a virtual space that is open and accessible to all users regardless of nationality. The institutional response must also be joint and coordinated. However, international cooperation on the protection of electoral processes is weak and fragmented, despite the existence of structures such as Europol, Eurojust, and the European Union Agency for Cybersecurity (ENISA). These institutions provide technical assistance without being able to intervene directly in the electoral process.

On the other hand, the existence of specific internal procedures governing the conditions under which sensitive data can be significantly transmitted slows down the exchange of information. In the absence of coordinating authority at the European level, states' reactions are often late and uneven, a fact exploited by attackers, leading to chain reactions⁵². In the absence of a single legal framework applicable at EU level, the principle of solidarity cannot be applied in the case of elections. This idea is supported by recent reports showing that existing joint initiatives operate voluntarily and not out of legal obligation⁵³. The lack of practical cross-border cooperation is both an institutional problem and a breach in European security. Every attack on the digital infrastructure of a member state affects the entire European system, undermining citizens' trust in a united and supportive Europe. Experts in the field say that real coordination between electoral authorities and cybersecurity authorities can ensure consistent protection of European democracy⁵⁴. Pending these significant changes, the continent remains helpless and fragmented in its response to a cyberwar in which the attackers are often one step ahead.

5.3. Legislative Changes that are Needed

Analysis of the issues presented in the previous subsections highlights a complex reality. Although the European Union has robust legal instruments at its disposal, these are not comprehensive or uniform, making it impossible to apply them in practice. To combat external interference in electoral processes, a common approach based on cooperation and transparency is needed.

In our opinion, a single European regulatory framework dedicated to the protection of electoral processes is needed, including minimum mandatory standards for digital infrastructure security, clear criteria for legal liability, and coordinated

⁵² Hybrid CoE. (n.d.). *The European Centre of Excellence for Countering Hybrid Threats*. Retrieved September 7, 2025, from <https://www.hybridcoe.fi/>.

⁵³ European Union. (2024, May 21). *Hybrid threats: Council paves the way for deploying Hybrid Rapid Response Teams*. <https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/hybrid-threats-council-paves-the-way-for-deploying-hybrid-rapid-response-teams/>, accessed on 10 January 2026.

⁵⁴ Dragonfly Intelligence. (2025, April 3). *Europe | Outlook for Russian cyber operations*. <https://dragonflyintelligence.com/news/europe-outlook-for-russian-cyber-operations/>, accessed on 10 January 2026.

response procedures in the event of cyber-attacks. Such regulation would provide both consistency and legitimacy to Member States' interventions, eliminating the discrepancies that currently exist between them (European Parliament, 2024). We also consider it appropriate to consider a permanent coordination mechanism between electoral authorities and IT security authorities at the European level. In our opinion, it is equally essential to rethink the sanctioning regime to simplify procedures and use common criteria for evaluating evidence. In many situations, only a prompt and unified sanction can have the desired effect of preventing and deterring hostile actors. Finally, security measures must be designed in such a way that they do not undermine fundamental democratic values: freedom of expression, media pluralism, and the right to information. We cannot increase security through measures that diminish freedom of expression. Only by striking a balance between equality and security will we strengthen civic trust in European institutions and the rule of law. That is why protecting European democracy does not only mean introducing cybersecurity procedures for elections but also increasing solidarity between Member States by adopting a unified regulatory framework and sending a message of responsibility and mutual respect to citizens. We believe that through such a strategy, the European Union can ensure active and lasting protection of shared democratic values.

6. Conclusion

This study has demonstrated that Russian cyber influence operations targeting European elections represent a sustained and evolving threat to democratic institutions across the continent. The evidence reveals a systematic pattern of interference spanning nearly two decades, from the Bronze Soldier Crisis of 2007 through the present day. It utilizes sophisticated tactics, including infrastructure exploitation, vote manipulation, strategic publication of stolen data, false-front engagement, sentiment amplification, and fabricated content. Prominent cyber threat actors, particularly APT 28 and APT 29, have consistently targeted electoral systems, political parties, government institutions, and candidates across diverse European states, with notable operations in Ukraine, France, Germany, Poland, Romania, and Moldova demonstrating Russia's commitment to exploiting vulnerabilities whenever a strategic opportunity arises. Despite the European Union's commendable efforts to establish institutional safeguards — including the East StratCom Task Force, ENISA, the Hybrid Centre of Excellence, and successive rounds of sanctions — the current legal and policy framework remains fragmented and inadequate. While diplomatic responses, regional initiatives, and public awareness campaigns represent necessary steps, they have proven insufficient to deter Russian operations or provide comprehensive protection.

The sanctioning regime, though symbolically important, suffers from cumbersome enforcement procedures, legal challenges that overturn restrictions, and continued capacity for perpetrators to operate behind intermediary structures. More fundamentally, European states lack a unified regulatory framework governing electoral security, creating an uneven landscape where some nations invest substantially in digital protections while others leave critical vulnerabilities unaddressed. This inconsistency

not only invites targeted exploitation but also undermines public confidence in the integrity of European democratic processes. The contemporary challenge extends beyond technical and legal dimensions to encompass fundamental tensions between security and democratic values. Protective measures must navigate the delicate balance between preventing foreign interference and preserving freedom of expression, media pluralism, and political diversity — the very foundations the measures aim to protect. Without proportionate safeguards, security interventions risk becoming instruments of censorship rather than democratic defence.

Addressing these multifaceted vulnerabilities demands a holistic, multi-level approach that transcends current fragmented responses. First, the European Union must establish a unified regulatory framework for electoral security that establishes minimum mandatory standards for digital infrastructure protection, clear criteria for legal liability attribution, and coordinated response protocols. Second, permanent coordination mechanisms between electoral and cybersecurity authorities at the EU level are essential to enable swift, unified action. Third, the sanctioning regime requires a fundamental redesign, including simplified procedures, common evidence evaluation criteria, and effective monitoring systems to ensure compliance and general deterrence. Fourth, institutional responses must be anchored in principles of proportionality and democratic legitimacy, provided that security measures do not restrict fundamental freedoms.

Beyond institutional reform, defending European democracy requires genuine solidarity among member states. Current joint initiatives operate on voluntary rather than legal obligation, a reality that weakens collective resilience. The cross-border nature of cyber threats demands legally binding cooperation rather than discretionary measures. Ultimately, protecting electoral integrity is not merely a technical problem requiring cybersecurity solutions. It is fundamentally a question of whether the European Union can maintain the institutional coherence, legal consistency, and shared commitment necessary to preserve democratic legitimacy in an era of persistent hybrid warfare. The measure of Europe's success will not be found in individual defensive mechanisms, but in whether it can construct an integrated defence anchored in the rule of law, democratic values, and the genuine solidarity that the Union's founding principles demand.

Bibliography

1. Antoniuk, Daryna (2023, December 27). *Albanian parliament, telecom company hit by cyberattacks*. Recorded Future News. <https://therecord.media/albanian-parliament-telecom-company-hit-by-cyberattacks>, accessed on 10 January 2026.
2. Antoniuk, Daryna (2024, February 2). *Iran-linked hackers claim attack on Albania's Institute of Statistics*. Recorded Future News. <https://therecord.media/iran-linked-hackers-claim-attack-on-albania-census-org>, accessed on 10 January 2026.
3. Baezner, Marie & Patrice Robin, *Hotspot Analysis: Cyber and Information Warfare in elections in Europe*, December 2017, Center for Security Studies (CSS), ETH Zürich, <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-security-studies/pdfs/Cyber-Rep%20orts-2017-08.pdf>, accessed on 10 January 2026.

4. Bonfanti, Matteo E., „An Intelligence-Based Approach to Countering Social Media Influence Operations”. *Romanian Intelligence Studies Review*, 19–20, 2018: 47–68. https://www.animv.ro/wp-content/uploads/2019/06/RRSI-no.-19_20.pdf, accessed on 10 January 2026.
5. Boom, Lola (2025, July 30). *Moldova’s president warns of ‘unprecedented’ Russian election meddling*. <https://www.politico.eu/article/moldova-warns-russian-election-interference-mai-sandu-cyberattack-disinformation/>, accessed on 10 January 2026.
6. Brangetto, Pascal & Matthijs A. Veenendaal. „Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations”. In Pissanidis, N., H. Rõigas, M. Veenendaal (eds.), *2016 8th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, 2016, 113–126, <https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf>, accessed on 10 January 2026.
7. Broeders, Dennis W. J., “Cyber Intelligence and International Security: Breaking the Legal and Diplomatic Silence?,” *Intelligence and National Security*, vol. 39, no. 7 (2024): 1213–1229, <https://doi.org/10.1080/02684527.2024.2398077>.
8. Coker, James (2024, December 17). *EU Sanctions Russian Cyber Actors for “Destabilizing Actions.”* Infosecurity Magazine. <https://www.infosecurity-magazine.com/news/eu-sanctions-russian-cyber-actors/>, accessed on 10 January 2026.
9. Cook, Lorne (2021, September 24). *EU warns Russia over cyberattacks ahead of German elections*. AP News. <https://apnews.com/article/technology-russia-elections-media-foreign-policy-a9abb7e00e4430c402b07ae14cdd9c8c>, accessed on 10 January 2026.
10. Dreikhausen, Viola Fee & Andrea Salvi, *From cyber to hearts and minds*, European Union Institute for Security Studies. (2023, November 8), <https://www.iss.europa.eu/publications/briefs/cyber-hearts-and-minds>, accessed on 10 January 2026.
11. Flonk, Daniëlle, Markus Jachtenfuchs, and Anke Obendiek, “Controlling Internet Content in the EU: Towards Digital Sovereignty,” *Journal of European Public Policy*, vol. 31, no. 8 (2024): 2316–2342, <https://doi.org/10.1080/13501763.2024.2309179>.
12. Galante, Laura & Shaun Ee (2018, September 11). *Defining Russian election interference: An analysis of select 2014 to 2018 cyber enabled incidents*. Atlantic Council. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/defining-russian-election-interference-an-analysis-of-select-2014-to-2018-cyber-enabled-incidents-2/>, accessed on 10 January 2026.
13. Greenberg, Andy, (2017, May 9). *The NSA Confirms It: Russia Hacked French Election ‘Infrastructure.’* WIRED. <https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/>, accessed on 10 January 2026.
14. Kalsnes, Bente and Niels Nagelhus Schia, “Protecting Democracy: Comparing Codes of Conduct for Generative AI Use during Elections,” *Information, Communication & Society*, March 2026: 1–17, <https://doi.org/10.1080/1369118X.2026.2647362>.
15. Lei, Yuxuan, “The Role of Political Actors’ Preference Variation in the Decision-Making Process of the European Union,” *Social Sciences* vol. 14, no. 4 (2025): Article 193, <https://doi.org/10.3390/socsci14040193>.
16. Pijpers, Peter B.M.J. & P.A.L. Ducheine, „Influence Operations in Cyberspace – How They Really Work” (September 24, 2020). *Amsterdam Law School Research Paper* No. 2020-61, Amsterdam Center for International Law No. 2020-31, Available at <http://dx.doi.org/10.2139/ssrn.3698642>.
17. Santos, Nina dos & Tim Lister, (2018, July 4). *Arron Banks: UK investigates alleged*

- Russian links to Brexit backer*. CNN. <https://edition.cnn.com/2018/07/04/uk/uk-brexit-russia-links-arron-banks-intl/index.html>, accessed on 10 January 2026.
18. Semini, Lazzar (2022, September 7). *Albania cuts diplomatic ties with Iran over July cyberattack*. AP News. <https://apnews.com/article/nato-technology-iran-middle-east-6be153b291f42bd549d5ecce5941c32a>, accessed on 10 January 2026.
 19. Siman-Tov, David, Gabi Siboni, and Gabrielle Arelle, „Cyber Threats to Democratic Processes”. *Cyber, Intelligence, and Security*, Volume 1, No. 3, December 2017: 51-63, https://www.inss.org.il/wp-content/uploads/2018/01/CyberENG1.3_6-53-65.pdf, accessed on 10 January 2026.
 20. Tsagourias, Nicholas & Michael Farrell, „Cyber Attribution: Technical and Legal Approaches and Challenges”, *European Journal of International Law*, Volume 31, Issue 3, August 2020: 941–967, <https://doi.org/10.1093/ejil/chaa057>.