Report

Building Resilience Against Election Influence Operations: Preparing for the European Elections in 2024 and Beyond

Daria Azariev North, David Levine, Krystyna Sikora, and Nikoleta Diossy

G | M | F Alliance for Securing Democracy

International Foundation for Electoral Systems IFES

Table of Contents

Executive Summary

In 2024, nearly half of the world's population is heading to the polls. One of the biggest of these contests is the 2024 European Parliament elections from June 6–9, in which 366 million voters in the union's 27 member states will elect 720 members of the European Parliament (EP). This year's elections are taking place amid increasingly shifting geopolitical and technological landscapes. Now is the time for European countries and their partners to review and adapt the tools in their arsenals to combat malign election influence operations.

Understanding that countries can mount a strong defense of their democratic processes by continually learning from each other, this report offers snapshots of best practices for building resilience against election influence operations adopted by five different European countries—France, Sweden, Estonia, Bosnia and Herzegovina, and Ukraine—since the last EP election in 2019. The best practices include:

- Bolstering the government's ability to identify and counter foreign influence operations
- Adopting whole-of-society frameworks to build resilience across institutions and sectors of society most vulnerable to disinformation
- Investing in fact-based journalism and digital literacy programs for communities most at risk of being targeted, such as minority language populations
- Developing proactive crisis communication plans for election authorities to anticipate and respond to false narratives
- Leveraging robust, cross-sectoral coordination, particularly on emerging technology, to counter malign influence.

As autocratic actors continue to refine their influence efforts, it will be essential for European countries and others to adopt a similarly holistic approach. This includes working collectively across all sectors of society and learning from the experiences of others facing similar challenges. The five best practices described in this report are just a few ways European countries, and other countries facing similar threats, can bolster their preparedness and ensure resilience in the face of information-related threats ahead of future elections. How well European countries and others are able to do so will be critical to the foundation of democracy and electoral processes across the region for years to come.

Introduction

In 2024, more voters are heading to the polls than ever before. Nearly half of the world's population lives in countries that are holding national elections this year. The outcomes will have global ramifications for years to come. One of the biggest of these contests is the 2024 European Parliament elections from June 6–9, in which 366 million voters in the union's 27 member states will elect 720 members of the European Parliament (EP).

Many countries remain vulnerable to election influence operations—covert or overt efforts by foreign and domestic actors to circulate false, misleading, or harmful information or narratives to impact an election. Those actions aim to sow discontent and erode trust in democratic systems. Countries have varying capacity and preparedness to face these challenges, and there is no unified framework for meeting shifting threats to electoral integrity. As malign actors are increasingly coordinating and learning from one another, it is more important than ever for countries to learn from one another's best practices to bolster their resilience against election influence operations.

Although trust in democracy and trust in elections often go hand in hand, trust in democratic elections is precarious in many parts of the world. Domestic political polarization, the prevalence of false information online, and autocratic actors taking aim at democratic systems all make it harder for many voters to believe in the integrity of their elections. Foreign adversaries are ramping up the scale and sophistication of their tactics, becoming more brazen in their efforts to influence elections. The European Union (EU) Special Committee on Foreign Interference warned that foreign interference and disinformation, particularly by the Russian Federation and the People's Republic of China (PRC), are likely to "continue in ever-greater numbers and become more sophisticated in the run-up to the European Parliament elections." Adding fuel to the fire, the rise of easily accessible artificial intelligence (AI) tools exacerbates vulnerabilities that malign actors could exploit to undermine future elections. The PRC is already reportedly experimenting with AI tools to conduct campaigns to amplify societal division in the United States before its 2024 presidential elections. Other adversaries, such as Russia and Iran, could follow suit to influence other elections.

These challenges are compounded by social media companies' struggles to safeguard their platforms from information threats. Over the past year or more, a number of social media companies—notably X (formerly Twitter)—have rolled back some of their most constructive measures to uphold election integrity online. This includes disabling functions to report false election information, dissolving election integrity teams, and overhauling account verification services. Some companies have announced positive steps in response to widespread concern about election disinformation in 2024. These include Meta, which recently set up a team to tackle disinformation and AI abuse in the lead-up to the EP elections. However, others have not. These challenges, in addition to the introduction of newer, less tested platforms and tools such as Telegram, TikTok, Threads, and ChatGPT, increase concerns over whether information manipulation—obtaining and sharing information to disrupt democratic decision-making—could influence or lead to the disenfranchisement of voters ahead of the EP and other elections.

On the positive side, many countries increasingly recognize the importance of bolstering their resilience to information manipulation and safeguarding electoral integrity. In August 2023, the EU adopted the Digital Services Act. This sweeping legislation aims to foster safer online environments by holding technology companies accountable for

monitoring and removing harmful content from their platforms. In March 2024, the EU enacted the first framework on AI. Moreover, new EP rules on transparency and targeting of political advertising are intended to make election and referendum campaigns more transparent and resistant to interference. In addition to measures focused on the information space, the EU has protections to ensure the successful administration of the 2024 EP elections. For example, most of the EU's 27 national governments retain paper records of each vote, observe strong chain of custody procedures, and count votes manually. These critical safeguards enable verification of election results when skepticism or errors occur.

With relatively little time before many of the largest remaining 2024 elections, including the EP elections, this is not the time for most drastic changes. However, countries with upcoming elections can continue to make continual improvements until election day. For the future, countries should review and, if necessary, bolster their strategies to prepare for and counter harmful election narratives. Democracies can and do learn from each other about how to respond to threats and build trust among their populations. For example, EU member states could further bolster their information ecosystems ahead of the 2024 EP elections by looking at how other European countries have confronted similar issues.

This report offers snapshots of some best practices for continually building resilience against election influence operations adopted by five different European countries the last EP election in since 2019. The five case studies on the following pages—France, Sweden, Estonia, Bosnia and Herzegovina, and Ukraine—include some members of the EU and some non-members. For each of the five case studies, the paper will first showcase how the best practice bolstered the country's resilience against information manipulation ahead of a recent election. Each case study will be followed by broad guidance to help other countries adopt some or all of these practices into their own contexts, with the understanding that no two countries are alike. While there is no "one size fits all" approach, and the best practices presented may not work for every country, those looking to strengthen the integrity of their information environments for future elections should consider the lessons discussed below and how to incorporate them into their own operations.

This paper is not directed at any one country or election. Nor is it intended to cast doubt on the integrity of upcoming elections, particularly those, like the 2024 EP elections, that have a history of ensuring that the results reflect voters' choices. Instead, it serves as a reminder that election information defenses must evolve continuously, and it provides ideas for how countries can do this in the short and long-term.

Case Studies

France: *Bolster the government's ability to identify and counter foreign influence operations.*

France's experience illustrates ways to counter election disinformation. In the country's 2017 presidential election, frontrunner Emmanuel Macron—a pro-European centrist—became the target of a coordinated Russian influence campaign to undermine his candidacy against the right-wing Marine Le Pen, Moscow's preferred candidate. Months before the election, a fake website posing as a reputable Belgian news agency (that was later traced to a Russian troll factory) reported that Saudi Arabia was financing his campaign. The post generated more than 10,000 likes, shares, and comments on Facebook. Macron was again targeted when hackers affiliated with Russian military intelligence stole internal emails and documents from his campaign team and released them online, along with fraudulent emails, two days before the second round of voting during a legally mandated 44-hour pre-election media blackout. The so-called "Macron leaks" did not significantly impact the outcome of the election, in which Macron received 66% of the votes. However, France learned from this experience and took proactive steps to further bolster future elections from information manipulation.

In preparation for its next major election cycle, the 2022 presidential and general elections, France developed a unit to detect, monitor, and counter foreign information operations intended to undermine the country's stability. Before launching the unit, called Viginum, the government created safeguards to protect privacy rights and freedom of speech. This includes regulations on how Viginum collects and uses social media data. Viginum's research is restricted to open-source data; it is prohibited from interacting with other users, entering private groups, or creating avatars. The inter-ministerial Ethics and Scientific Committee, established within the General Secretariat for National Defense and Security, also supervises all of Viginum's work.

Before Viginum began working on the 2022 elections, it conducted a landscape review of foreign digital interference in other elections. Viginum representatives met with France's three election oversight bodies—the National Commission for the Control of the Electoral Campaign, the Constitutional Council, and Arcom—to better understand how elections are administered and kickstart collaboration. They also consulted German agencies about threats to Germany's 2021 general elections and tested Viginum's monitoring capabilities by tracking French-language public debate about the German elections so it could prepare for issues that it could leverage in the information environment of the French elections.

Viginum began its monitoring operations for the 2022 elections in November 2021. Throughout the campaign cycle, Viginum staff worked closely with Objectif Désinfox, a fact-checking initiative of Agence France-Presse and Google, to characterize flagged content as false or misleading. Viginum also established direct lines of communication with the social media platforms so it could ask them about influence campaigns, identify situations that required further discussion, and request that they flag suspicious incidents. Starting in February 2022, Viginum regularly sent reports

describing the campaigns it had detected during the election period to the three election oversight bodies, as well scheduled a hearing with them in April to go over specific information manipulation attempts.

Viginum's communication with different French institutions ensured that they were able to take robust measures to counter information manipulation during the election. During the election cycle, Viginum identified 60 inauthentic occurrences on digital platforms. Of those, five met the definition of foreign interference, including a campaign—that gained traction among domestic right-wing accounts—that suggested that the French government was using voting machines from the Canadian-US firm Dominion Voting Systems to skew election results in favor of Macron. Viginum alerted the Ministry of the Interior, which issued a public refutation of the claim. Despite a number of other false claims targeting candidates and the voting process, largely amplified by domestic social media accounts, none appear to raise significant doubts about the electoral outcome.

How can this best practice work elsewhere? A government unit that exposes and counters foreign influence operations could be an invaluable tool for protecting a country's elections and democracy more broadly. However, creating units to monitor the public information space may prompt legitimate concerns about government overreach and potential breaches of individuals' freedom of speech and privacy. Therefore, governments should give such units clear mandates and ensure they can work within the relevant legal framework and avoid infringing on people's civil liberties.

To mitigate those concerns, the French unit, and similar ones established in other countries—including Sweden's Psychological Defense Agency and the United States' Global Engagement Center—have created strict guidelines on what the units will monitor. They focus only on foreign influence and do not monitor the activities of domestic entities. France also created clear regulatory safeguards. These ensure that Viginum respects citizens' digital rights and personal privacy, including how it collects and uses personal data. A well-qualified ethical and scientific committee supervises its work.

Although not all governments have the resources to create units to identify and counter foreign influence operations, they can still pursue similar efforts via other means. For example, many non-governmental organizations (NGOs), social media platforms, news outlets, and other key stakeholders have initiatives to monitor influence operations or possess the tools to do so. Supporting and building on the work of those partners by funding or collaborating on projects, especially before elections, could also be beneficial. Doing so could generate feedback on information threats similar to that of a dedicated government unit at a fraction of the cost. Such cross-sectoral collaboration can also be a valuable strategy for defending the electoral information environment.

Sweden: *Adopt a whole of society framework to bolster resilience to withstand information manipulation.*

Like France, Sweden is a global leader in developing best practices to counter election disinformation. In response to Russia's interference in the 2016 US presidential elections and other European races"—notably the 2017 German federal and French presidential elections—Sweden, a frequent target of Kremlin-sponsored disinformation,

prioritized its information influence defenses. Rather than attempting to halt the creation and spread of disinformation, Sweden adopted a whole of society approach to build the resilience of institutions and society overall to withstand influence activities. That approach improved the country's security posture against both foreign and domestic disinformation actors.

To safeguard Sweden's 2018 general election against disinformation campaigns, the country's Civil Contingencies Agency (MSB) provided election authorities with knowledge, education, and tools to understand foreign influence threats, vulnerabilities in the electoral system, and potential response methods. This included developing a comprehensive training package for election officials to counter disinformation and election security threats. The package was shared with county administrative boards across the country. The MSB also piloted an in-person training for election authorities from all municipalities of Västra Götaland county. With mandates to counter homegrown disinformation, the election authorities drew on the training, knowledge, and support provided by the MSB to counter foreign and domestic purveyors of false information. These readiness activities, which benefited approximately 14,000 civil servants and election officials, helped ensure that the 2018 election ran smoothly notwithstanding a cyberattack on the Swedish Election Authority that generated a flood of homegrown political mis- and disinformation.

Building on this 2018 success, Sweden doubled down on its whole of society efforts in preparation for the 2022 general election by launching the Psychological Defense Agency (MPF). Like France's Viginum, the MPF leads Sweden's monitoring of foreign influence efforts. However, the agency has an equally important second role, directing initiatives to strengthen Swedish society's overall resilience to information manipulation.

Amid increased tension with Moscow following Sweden's bid to join NATO, the MPF was on high alert for potential interference in the 2022 election. To better protect the election from potential information threats, the MPF set out to increase public capacity to identify mis- and disinformation. Five months before the election, it launched the "Don't be fooled" (*bli inte lurad*) education campaign to raise awareness of threats from foreign influence operations and encouraged Swedes to think about the sources and publishers of information before sharing it online. The campaign website provides educational videos, one-pagers, and even a free online course on how to resist foreign influence. The agency plans to expand its public education programs for the public by teaming with a university to create a master's program in information resilience.

The Swedish government directed additional efforts toward other key stakeholders. For example, the MSB published its handbook for communicators to help journalists and other media actors to better identify and respond to false information when assessing information from both foreign and domestic sources. Likewise, in the months leading up to the 2022 election, MPF staff educated Swedish political parties about the possibility that they might become targets of disinformation campaigns and to advise on guarding against such campaigns.

Ultimately, Sweden's 2022 election did not experience the anticipated degree of foreign interference. Regardless, the country's success in bolstering resilience against foreign disinformation during elections is reflected both in its high voter turnout (84%) and general satisfaction with the country's democratic institutions (79%).

How can this best practice work elsewhere? With influence campaigns becoming more and more sophisticated and widespread, it is more important than ever that critical election stakeholders—from election management

bodies to the media and voters—can identify and defend themselves against information threats. Adopting a whole of society framework, as Sweden did, for countering information manipulation, particularly during elections, is key to building resilience by fortifying defenses across all sectors of society, strengthening partnerships for sharing information and tools, and fostering trust within the community.

Governments that adopt such a whole of society framework should begin with a landscape review of the vulnerabilities that different stakeholders and sectors of society face. Doing so may kickstart collaboration between government and non-government partners across various sectors, help identify priority areas, and assess the feasibility of implementing plans.

In addition to trying to reach various segments of society, governments that adopt a whole of society approach should consider diverse proactive measures. A comprehensive framework should incorporate activities that address communication, resilience, disruption, and regulation rather than covering each theme separately. This idea of an all comprehensive framework is exemplified by the MPF's two primary responsibilities: to both disrupt foreign influence campaigns and create initiatives to build resilience against them. Since Sweden adopted its whole of society framework, countries that have followed suit include Estonia, Finland, and Latvia.

Estonia: *Invest in fact-based journalism and other disinformation resilience programs for segments of society that are most at risk of being targeted by influence campaigns.*

Estonia is another country in which to look for best practices on countering election disinformation. Despite having an Internet voting system some security experts view as controversial and being a regular target of Russian cyber and influence operations since regaining its independence in 1994, Estonia has established itself as a digital powerhouse and transitioned to a well-functioning electoral democracy. Estonia provides most public services online, continuously refines and upgrades them, and makes consistent efforts to bolster resilience against information manipulation among segments of Estonian society that are most at risk. Those efforts often focus on Estonia's Russian-speaking population.

Russian-speakers account for 27% of Estonia's population, many of whom are ethnic Russians who settled in the country during the time of the Soviet Union. Until 2023, the majority of Estonia's Russian-speakers obtained news from Russian-language stations controlled by Moscow. In part for this reason, Russian state media routinely targets the country's Russian-speaking population with influence campaigns designed to widen fissures with the Estonian majority. The Bronze Soldier incident is a prime example. In 2007, Estonia became the first victim of the Kremlin's modern influence tactics after a Soviet statue, a flashpoint for competing nationalist narratives, was removed from the center of Estonia's capital, prompting multi-day riots.

Understanding this challenge, Estonia sought to offer alternatives to Russian media and engage with its Russian-speaking minority. In 2015, Estonia's public broadcaster launched a Russian-language television channel, ETV+,

alongside a studio in Narva, where 95% of residents speak Russian and over 30% hold Russian passports. The government also offered Estonian language and cultural courses to reduce susceptibility to Russian state narratives.

Estonia's efforts to bolster resilience against pro-Kremlin disinformation in its Russian-speaking population became more urgent after Russia's invasion of Ukraine, a little over a year before the county's March 2023 parliamentary elections. A staunch supporter of Ukraine, Estonia provided Kyiv nearly €500 million in defense assistance (1.4% of its GDP) and took in over 62,000 Ukrainian refugees. Unsurprisingly, the country experienced a surge in disinformation about the war, mainly in the form of Russian propaganda, in the run-up to the parliamentary elections. These narratives largely sought to create tension between the country's Russian and Estonian speaking communities by portraying Ukrainian refugees as "criminals," suggesting political links to Russia, and falsely reporting that Estonia was supplying arms to Ukraine.

To lessen the risk of these narratives influencing those most susceptible to them, Estonia coordinated closely with its media sector and invested in fact-based journalism for its Russian-speaking population. The Ministry of Culture distributed €1 million in funding to private media to improve Russian-language media coverage. With its allocation, *Postimees*, one of Estonia's most prominent newspapers, published a 24-page weekly Russian-language print edition, staffed by 25 Russian-speaking journalists hired to cover domestic and international news. Likewise, ETV+ invested in a daily evening program and a weekly foreign affairs program and a Russian-language version of the public broadcaster's video-on-demand platform. Other Estonian media outlets reported similar projects and staff hires.

While engaging with a population living in a separate information ecosystem is not easy, Estonia's strategy seems to be paying off. Despite widespread disinformation about the war in Ukraine, Russian-speakers' trust in Estonian media has increased and the share of non-ethnic Estonians who consider Russian media as "important sources of information" has dropped from 30% to 10% since Estonia's actions following the invasion of Ukraine, according to a poll commissioned by the government.

How can this best practice work elsewhere? A pluralistic, free, and truthful media landscape is vital to a vibrant democracy—even more so when the information environment is affected by disinformation and influence campaigns intended to undermine democratic institutions and processes. While no one is completely immune to information manipulation, some populations—particularly members of minority groups—may be at greater risk of being targeted to fuel discontent. Marginalized communities are often primary targets of hostile influence campaigns by the Kremlin, other authoritarian governments, and autocratic domestic actors to exacerbate societal cleavages and discord. Many actors' divisive tactics across Europe and elsewhere have intersectional impacts on elections and democratic processes. Continually building more inclusive societies and information environments can be a powerful response to such malign influence operations.

While Estonia prioritizes fact-based journalism for its Russian-speaking population, there are an array of other ways that governments can bolster resilience to influence campaigns among those most at risk. This includes supporting media literacy education, furthering partnerships or cooperation with respected organizations representing minority interests, and developing voter education programs aimed at boosting trust in election systems. Regardless of the

initiative, the most critical component for programs that target specific groups is that they empower communities and make them feel accepted and heard, rather than isolated.

Bosnia and Herzegovina: *Adopt a crisis communications strategy to preserve trust in the face of false and misleading information campaigns*

Bosnia and Herzegovina offers valuable lessons on countering disinformation and the importance of building a resilient and cohesive society to resist malign influence. The country's experiences combating disinformation throughout the electoral cycle are tied to a complex political landscape shaped by a fragile tripartite power sharing arrangement. Bosnia and Herzegovina's internal administrative structure was formed following a brutal aggression and war in the 1990s. The peace deal struck in 1995 in Dayton, Ohio divided the country into two entities: the Serb-dominated Republika Srpska and the Federation of Bosnia and Herzegovina with Croats and Bosniaks in majority. A tenuous balance among three constituent nations impedes quick responses to emerging threats, increasing susceptibility to the geopolitical interests of Russia and the PRC, in addition to neighboring Croatia and Serbia.

Entrenched, divisive rhetoric and narratives are creating an ongoing political crisis in the country, including in the run-up to recent Bosnia and Herzegovina's 2022 general election. Politicians' failure to agree on electoral reform were followed by disinformation alleging that the disagreement meant there was no legal basis for elections. Then, government actors obstructed adoption of the election budget, which must be secured 15 days after the date of the announcement of the election. As a result, the 2022 election was marred by deep political and social polarization, including significant disinformation campaigns, hate speech, and ethnic tensions. Russia-affiliated domestic political actors also spread malign messages. The election period, described by the Central Election Commission (CEC) as "the most turbulent so far," was punctuated by disinformation campaigns across social media platforms that inflamed social division and undermined trust in the election and the CEC itself. Ahead of the election, Russia leveraged support for separatism and openly supported the secessionist pro-Russian President of Republika Srpska Milorad Dodik. NATO Secretary General Jens Stoltenberg remarked, "We are concerned by the secessionist and divisive rhetoric as well as malign foreign interference, including Russia."

These occurrences were further exacerbated by challenges that many election management bodies (EMBs) face across the region, such as limited institutional capacity and budgetary constraints. Additionally, a series of direct online attacks on several female candidates and members of the CEC, mainly on social media, emphasized the gendered dimension of online hate speech and disinformation, and their negative impact on women's participation in political processes and inclusive elections.

The CEC responded to this challenging landscape by building institutional capacity and developing a proactive crisis communication strategy to anticipate and counter the highest-risk disinformation narratives ahead of the election. The CEC strengthened its capacity in part by incorporating the Crisis Communications and Combating Disinformation Playbook, developed by the International Foundation for Electoral Systems' (IFES) in partnership with the Brunswick Group. The lessons from the playbook were reinforced by tailored training on social media engagement for CEC staff. The playbook addresses gaps identified by a regional working group for EMBs on disinformation,

electoral integrity, and foreign influence convened by the IFES. The working group facilitated the development of relationships with technology firms and provided a platform for countries to learn from one another about shared challenges, good practices, and useful tools. The playbook outlines best crisis communications practices, such as building a sustainable rapid response process. This includes establishing an internal CEC disinformation response team, using early warning tools, conducting stakeholder outreach and education, activating networks for escalation protocols, and creating a rapid response checklist.

To prepare organizationally and build trust with voters, the CEC conducted an initial vulnerability assessment in advance of the 2022 election. The assessment identified potential high-risk false narratives that the CEC could expect and for which it could begin to formulate mitigation tactics. A risk matrix enabled the CEC to assess the threat level each narrative could pose to the integrity of the election and prepared responses to reduce susceptibility to them. A scenario planning exercise identified potential false narratives that could undermine the election and sow discord among ethnic groups. For example, one scenario accused the CEC of delaying the delivery of critical election materials, such as ballots, to a region populated largely by an ethnic group connected to the opposition. The scenario challenged the validity of the CEC's explanation about road closures due to extreme weather, using old photos of the roads in perfect condition. To counter this potential narrative, the CEC drafted interim statements, social media posts, and questions and answers targeting different audiences. To further support its response, the CEC developed a list of potential third-party spokespersons who could confirm the condition of the roads and refute the false claims.

The CEC's proactive preparation for the 2022 election helped ensure effective responses to false narratives across media, proactive communication with voters through social media and traditional media briefings, and the broadcasting of CEC sessions before, during, and after the election. The Organization for Security and Co-operation in Europe/Office for Democratic Institutions and Human Rights (OSCE/ODIHR) Election Observation Mission noted that the CEC "administered the election efficiently, transparently and within the legal deadlines" and "… enjoyed the confidence of most stakeholders."

How can these practices work elsewhere? As the ultimate authorities on elections, EMBs are the official resources for timely and accurate election information. This responsibility has become even more critical due to a rise in election-related disinformation, malign influence, and increasing polarization of the media environment. To mitigate these threats to electoral integrity, EMBs and other electoral stakeholders must act proactively and adopt crisis communications strategies to help them respond to false information and harmful narratives intended to undermine elections, as Bosnia and Herzegovina did in 2022. At the end of the day, the reputation of EMBs and other stakeholders hinges to a great extent on their ability to promote credibility and build trust in the electoral process. How well they do so can influence the outcome of an election—and a country's ability to preserve democracy.

In building their institutional crisis communication plans, EMBs should consider several key steps. These include identifying target audiences (for example, marginalized groups, such as ethnic minorities, women, young people, persons with disabilities) and their need for information, and developing communication plans that demonstrate core values to each audience to build trust systematically. Proactive, concise, consistent, and direct communication through the EMB's website or social media can decrease the risk of information being misinterpreted or taken out of context; it also enables EMBs to communicate in a timely manner, which is essential when responding to

harmful narratives. Establishing relationships and maintaining consistent communication with voters throughout the electoral cycle increases the likelihood that the electorate receives messages with trust, particularly during periods of crisis. Such seemingly simple skills such as using social media to communicate with the electorate are critical for EMBs to formulate timely, effective messaging that aligns with their values and target audiences. An effective crisis communication strategy also highlights the fact that no response is also a response—although perhaps not a desirable one.

EMBs must also be aware of their election systems' main vulnerabilities. As Bosnia and Herzegovina demonstrated, conducting self-assessments of institutional weaknesses and identifying potential risk scenarios can enable EMBs to get ahead of possible narratives, develop appropriate responses, and proactively communicate important messages. EMBs can apply the assessment to the country context to isolate common disinformation themes and anticipate scenarios that might be used to discredit public institutions and sow doubt or mistrust among citizens. Early self-assessments and crisis scenario planning build institutional confidence and preparedness that can decrease the time needed to respond to the appearance of an intentionally damaging narrative. That in turn reduces the likelihood of disinformation reaching and influencing large numbers of people.

EMBs should also develop risk matrices or escalation protocols to assess the severity of potential harmful narratives and determine the appropriate level of response. To do so, EMBs should focus predominantly on three areas: a narrative's potential impact, its credibility, and how quickly it spreads. The severity of the narrative should determine the response and communication strategy.

Ukraine: *Leverage robust, cross-sectoral coordination, particularly on emerging technology, to counter malign influence.*

As a preeminent target of the Kremlin's malign interference for decades, Ukraine's hard-won experience in advancing democracy offers several lessons for defending the electoral information environment, including instances when Ukraine has been unable to hold its elections at ordinary intervals. Since the Revolution of Dignity in 2013 and Russia's illegal annexation of Crimea in 2014, Ukraine has been at war with Russia on two major fronts—an escalatory kinetic conflict, alongside a persistent and increasingly complex battle fought predominantly in the information space. Over the past decade, Ukraine has developed a comprehensive framework to defend its electoral processes—and its society more broadly—from the impacts of Kremlin interference and malign influence efforts. While the country has achieved many successes in building information resilience in recent years, a core pillar of Ukraine's information integrity resilience is deep cross-sectoral cooperation—particularly on emerging technology, including AI and machine learning for detection and response—among civil society, government institutions, media, academia, and the private sector.

Heading into Ukraine's 2020 local elections, the country's information environment was tainted by an upsurge in Russian disinformation. These challenges, including the Kremlin's tactics, sought to destabilize the country with disinformation about issues such as the COVID-19 pandemic. Fear about safety concerns was sown through the mainstream media, including prominent TV channels, and social media. The narratives were crafted to undermine the

legitimacy of the Ukrainian state and its institutions, weaken ties between Ukraine and its partners in the West, and promote a positive image of the Russian government. Russia, however, underestimated the long-term preparedness building and cooperation of various Ukrainian sectors.

To counter these narratives, Ukraine created deep networks of cooperation across various sectors of society for sharing lessons learned and highlighting best practices for countering false narratives. Ukraine's civil society has been instrumental in re-orienting itself to advance the country's narrative response capabilities by increasingly providing timely, measured, factual responses to harmful narratives around elections. Consequently, this has also expanded the capacity of independent media to accurately cover these narratives. Organizations such as Detektor Media and StopFake, which monitored election campaigns ahead of the 2020 election, have debunked numerous false Russian narratives since 2014. Those efforts have helped Ukrainians distinguish between fact and fiction.

One successful example of cross-sectoral coordination is the e-platform, HelpSMI, which was created specifically for Ukraine as a communication platform connecting journalists and experts from various fields, civil society, academia, and local businesses. The platform supports democracy building, promotes freedom of speech, and counters malign narratives by providing journalists and media outlets with trusted sources and reliable information from experts gathered on one platform. HelpSMI helped uncover a range of issues, including bribes by a local politician one year ahead of Ukraine's 2020 elections, how illicit funding circulated during parliamentary and presidential elections in 2019, and the debunking of false narratives about Stepan Bandera, which are often used by Russia to paint Ukrainians as supporters of the Nazi regime.

The Ukrainian government also understood the need for better cross-sectoral cooperation with other parts of society to successfully counter malign narratives. Ahead of the 2020 local elections, President Volodymyr Zelenskyy announced to the 75th United Nations General Assembly that Ukraine was ready to set up "the headquarters of the International Office for Countering Disinformation and Propaganda in Kyiv. There is no longer the concept of someone else's war. Our planet is no longer so big … when disinformation and fake news can influence global markets, stock exchanges, and even the electoral process." In March 2021, the Ukrainian government realized these plans by establishing the Center for Countering Disinformation (CCD) within the National Security and Defense Council. The CCD is dedicated to debunking manipulative and misleading Russian narratives, including across social media platforms. It develops reports, articles, and refutations of prominent disinformation narratives that further strengthen public resilience to disinformation. The CCD also fosters cross-sectoral cooperation with civil society organizations such as StopFake and others.

Shortly after the CCD was established, the Center for Strategic Communication was created under Ukraine's Ministry of Culture and Information Policy as "one of the mechanisms for countering disinformation, by joint efforts of the state and civil society." The center focuses on cross-sectoral cooperation with civil society to amplify their work with the general public, conducting joint information campaigns to build public resilience to malign narratives, and facilitating dialogue between the state and civil society organizations to develop regulatory frameworks. In close cooperation with civil society, the center created the debunking page, "Spravdi", which researches, analyzes, and reports on new false narratives being spread in Ukraine and abroad. In 2021, the center, in cooperation with more than ten non-governmental organizations from Ukraine and abroad, analyzed how the Kremlin spread malign narratives about COVID-19 in Ukraine during the 2020 election year. The success of Spravdi provided the Ukrainian

public with verified information that helped them navigate this complicated information space, which included over 250,000 fake messages about COVID-19 across Ukrainian social networks in 2020.

Ukraine's media monitoring has helped increase its public's media literacy and enabled Ukrainians to make more informed choices during the electoral process. However, it takes significant manpower and time to sort through the amount of news online. Additionally, civil society organizations often have financial constraints that make it difficult, if not impossible, to reach broad swaths of the public. As a result, some organizations started using AI in order to increase their capacity as well as enhance their cooperation with the government and private sector. After Russia's 2022 invasion, Ukraine leveraged emerging technologies to further expand cross-sectoral cooperation between civil society, government and the private sector. Government agencies and ministries built relationships with start-ups and private companies, using the latter's software to swiftly detect and counter Kremlin disinformation on a country-wide level. Start-ups such as Osavul and Mantis Analytics, created in response to the invasion, began to employ large language models and natural language processing to counter the Kremlin's disinformation narratives about Ukraine. Adopting this new technology, helped Ukrainian agencies quickly identify potential harmful narratives and disseminate factual information before they gained traction.

How can these practices be used elsewhere?

Ukraine's approach in fostering robust cross-sectoral cooperation among civil society, government institutions, media, academia, and the private sector demonstrates how countries can build resilient and holistic frameworks to combat disinformation. As the National Endowment for Democracy's report notes, "civil society organizations should leverage common values and diverse skill sets to form cooperative networks that have the sophistication and speed to combat" the scale of information threats to electoral processes. The creation of synergies among various sectors of society can lead to a more informed electorate that trusts public administration and has a high degree of literacy in recognizing malign narratives. However, even the best-staffed organizations across sectors may have limited capacity to monitor emergent disinformation narratives across the global media ecosystem. Ukraine offers valuable lessons for other countries on how a proactive approach in leveraging technology for good can also help build capacity across various sectors. Countries across the region can draw inspiration from the Ukrainian case study, utilizing new technology and machine learning to accelerate identifying harmful narratives and strengthen cross-sectoral cooperation. Just as AI and other new emerging technologies offer malign actors tools to undermine elections, with proper safeguards they can also offer EMBs and other critical election stakeholders potential opportunities to help them better defend elections.

Although Ukraine was unable to use these technological advances in the postponed 2024 presidential and parliamentary elections, its ability to counter malign Russian narratives has enabled the country to better protect its democracy. The war in Ukraine catalyzed the country's governing institutions to further modernize and fortify, reducing vulnerability to Russia's malign influence. Ukraine's blooming, multi-faceted, integrated response can be described as "total democratic resilience". Through its comprehensive and multidisciplinary approach, Ukraine adopted a broader framework for information resilience than exists in many European countries, including EU member states. Many countries can learn from this example in defending the integrity of their elections.

Conclusion

Information operations that cast doubt on legitimate election outcomes are major threats to electoral integrity and the foundation of democracy. Autocratic actors are conducting more persistent and sophisticated election influence campaigns across the world. Emerging developments—such as the proliferation of accessible AI tools—are likely to exacerbate the current challenges with maintaining the integrity of the information environment ahead of the June 2024 EP elections, as well as other elections throughout Europe and around the world.

The electoral information environment across Europe faces evolving threats from foreign and domestic actors. Autocratic actors' electoral interference strategies are increasingly integrated and multifaceted, with many malign actors increasingly coordinating their efforts. As autocratic actors continue to refine their influence tactics, it will be essential for European countries and others to adopt a similarly holistic approach. This includes working collectively across all sectors of society and learning from the experiences of others facing similar challenges. While there is no "one size fits all" approach, now is the time for European countries and their partners to review and adapt the tools in their arsenals to combat election influence operations. Countries can mount a strong defense of their democratic processes by continually learning from each other and working proactively across sectors. The five best practices described in this report are just a few ways European countries, and other countries facing similar threats, can bolster their preparedness and ensure resilience in the face of information-related threats ahead of future elections. How well European countries and others are able to do so will be critical to the foundation of democracy and electoral processes across the region for years to come.

About The Alliance for Securing Democracy at GMF:

The Alliance for Securing Democracy (ASD) at the German Marshall Fund of the United States (GMF) is a nonpartisan initiative that develops comprehensive strategies to deter, defend against, and raise the costs on autocratic efforts to undermine and interfere in democratic institutions. ASD has staff in Washington, DC, and Brussels, bringing together experts on disinformation, malign finance, emerging technologies, elections integrity, economic coercion, and cybersecurity, as well as Russia, China, and the Middle East, to collaborate across traditional stovepipes and develop cross-cutting frameworks.

securingdemocracy.gmfus.org | gmfpress@gmfus.org

About The International Foundation for Electoral Systems:

The International Foundation for Electoral Systems (IFES) is a global, nonpartisan organization that advances democracy for a better future. IFES collaborates with civil society, public institutions, and the private sector to build resilient democracies that deliver for everyone. As a global leader in the promotion and protection of democracy, IFES's technical assistance and applied research develops trusted electoral bodies capable of conducting credible elections; effective and accountable governing institutions; civic and political processes in which all people can safely and equally participate; and innovative ways in which technology and data can positively serve elections and democracy. Since 1987, IFES has worked in more than 145 countries, from developing to mature democracies.

ifes.org | media@ifes.org

About the Authors:

Daria Azariev North (@DarAzarievNorth)is a senior program manager for Europe and Eurasia at IFES with more than 10 years of experience in democracy building and transatlantic cooperation. In this role, she oversees the program design and implementation of a broad portfolio in the region, working with electoral stakeholders from the Western Balkans, Eastern Partnership, and Visegrad 4 countries to build their capacity in responding to persistent and emerging challenges to democratic resilience. She provides thought leadership on programming related to countering disinformation and malign foreign influence in elections, as well advancing women's empowerment and youth civic engagement. She spearheaded the launch of the European Working Group for election management bodies on social media, disinformation, and electoral integrity in 2020 and has led the development of IFES's Crisis Communications and Countering Disinformation Playbook as a global tool.

David Levine (@davidalanlevine) is the senior elections integrity fellow at ASD at GMF, where he assesses vulnerabilities in electoral infrastructure, administration, and policies. David is also an advisory committee member for the Global Cyber Alliance's Cybersecurity Toolkit for Elections, an advisory council member for The Election Reformers Network, a member of the Election Verification Network, and a contributor to the Fulcrum. Previously, he worked as the Ada County, Idaho Elections Director, managing the administration of all federal, state, county, and local district elections.

Krystyna Sikora (@krysia_18) is a research assistant for the ASD at GMF, where she supports research on election integrity and information manipulation. Prior to joining ASD, she played professional soccer in Poland for two years. Krystyna holds a master's degree in Eurasian, Russian, and East European studies from Georgetown University. Her studies there centered on right-wing populism, disinformation, and democratic decline in Central and Eastern Europe, with a focus on Poland. She also holds a bachelor's degree in political science and a certificate in policy journalism and media studies from Duke University.

Nikoleta Diossy is a senior program officer for IFES' Regional Europe Office in Prague. In this capacity, she plays a pivotal role in engaging with stakeholders across Central and Eastern Europe, the Western Balkans, and the Baltics to foster resilient democracies and promote electoral integrity and inclusivity. Her areas of specialization include combatting foreign interference in electoral processes and advocating for gender equality within democratic frameworks. She holds a master's degree in International Relations and European Studies from Metropolitan University in Prague, supplemented by a one-year program at Central European University in Budapest where she focused on political science and international affairs.

Disclaimer/ Cover Photo Credit:

Disclaimer: The views expressed in this publication are the views of the author(s) alone.
Cover photo credit: VanderWolf Images | Adobe Stock