Hybrid CoE Research Report 12

Countering hybrid threats to elections: From updating legislation to establishing collaboration networks

Hybrid CoE

Sebastian Bay – March 2024

Hybrid CoE Research Reports are thorough, in-depth studies providing a deep understanding of hybrid threats and phenomena relating to them. Research Reports build on an original idea and follow academic research report standards, presenting new research findings. They provide either policy-relevant recommendations or practical conclusions.

Two errors corrected on 20240319. On page 11, the incorrect formulation "North Macedonian presidential election" corrected to "presidential election of North Macedonia", and on page 12, the incorrect formulation "Macedonian elections" corrected to "elections in North Macedonia".

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 | www.hybridcoe.fi

ISBN 978–952–7472–96–5 (web)
ISBN 978–952–7472–97–2 (print)
ISSN 2737–0860 (web)
ISSN 2814–7219 (print)

March 2024

Cover photo: Sergey Tinyakov / shutterstock.com

Hybrid CoE's mission is to strengthen its Participating States' security by providing expertise and training for countering hybrid threats, and by enhancing EU-NATO cooperation in this respect. The Centre is an autonomous hub for practitioners and experts, located in Helsinki, Finland.

Contents

Abstract

This Hybrid CoE Research Report provides a thorough analysis of hybrid threats to elections, with a specific focus on physical attacks, disinformation campaigns, and cyberattacks that pose a threat to the integrity of democratic processes. The report examines past incidents, categorizes different types of threats and actors, and assesses future risks. It recommends updating legislation to address emerging threats, assessing and mitigating weaknesses in election infrastructure, actively engaging media and politicians to counter disinformation, and establishing robust collaboration networks for rapid threat detection and response. These measures protect electoral integrity and bolster public confidence in democratic processes. The report duly underscores the urgency of implementing these robust defence strategies to safeguard the democratic process against evolving multifaceted threats.

1. Introduction

In recent years, efforts to undermine democratic elections have intensified, involving both foreign and domestic entities. These malicious activities encompass a wide range of tactics, including cyberattacks, online disinformation campaigns, and even physical assaults, all aimed at manipulating and destabilizing the democratic process.

Before the 2019 European elections, the European Commission highlighted the importance of protecting democratic systems within the European Union, and classified attacks on electoral systems as hybrid threats that must be confronted. The Commission acknowledged the rise of extensive online disinformation campaigns, sometimes orchestrated by foreign entities with the intent to undermine and delegitimize elections, and advocated for the EU to utilize all available measures to safeguard its democratic processes against manipulation.[1]

Since 2019, the threats against elections have increased due to the deteriorating security situation in Europe since the illegal Russian full-scale invasion of Ukraine, and the rise in domestic election interference. During the past few years, numerous attacks on democratic elections have been recorded.[2] A recent US intelligence report, shared with over 100 countries, highlights Russia's efforts and intent to undermine trust in the democratic process worldwide using spies, hackers, social media, and state-run media.[3]

Apart from foreign election interference, there has also been a surge in domestic threats to elections. According to cybersecurity and law enforcement officials, disinformation campaigns and threats to poll workers from domestic sources have emerged as a significant concern. Since the 2020 US presidential election, there have been numerous reports of poll workers being threatened, harassed, or assaulted.[4] The Election Integrity Partnership noted that domestic actors had spread the bulk of disinformation about the US 2020 election, aimed at undermining public confidence in elections.[5]

According to the Digital Media Observatory, false narratives about voter fraud, foreign influence, and unfair practices were disturbingly prevalent during at least 11 European elections in 2023. These narratives primarily revolved around the allegations of voter fraud or alleged unfair practices, which likely aimed to invalidate the election results and delegitimize democratically elected representatives.[6]

As the 2024 European elections approach, threats to democratic integrity underscore the urgent need for decisive, comprehensive strategies to enhance the security of European electoral integrity and democratic debates. In 2023, the European Parliament stressed the importance of enhancing the protection of European elections and urged electoral management bodies to prioritize risk mitigation and strengthen their resistance in the face of increasingly complex election threats.[7] Strengthening the EU's defences against interference is crucial to

1 European Commission, "Securing Free and Fair European Elections."
2 Insikt Group, "Aggressive Malign Influence Threatens to Shape US 2024 Elections."
3 Landay and Lewis, "US Intelligence Report Alleging Russia Election Interference Shared with 100 Countries."
4 Siddiqui and Bing, "U.S. Security Officials Worry about Homegrown Election Threats."
5 Stanford Internet Observatory et al., "The Long Fuse: Misinformation and the 2020 Election."
6 Panizio, "Disinformation Narratives during the 2023 Elections in Europe."
7 European Parliament, "European Parliament Resolution of 1 June 2023 on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation (2022/2075(INI))."

maintaining public trust in elections and ensuring the legitimacy of electoral outcomes.

1.1 Aim and purpose of the report

This report aims to present a thorough analysis of the hybrid threats that may pose a risk to upcoming elections. It is designed to provide election officials with a detailed understanding of the potential threats that may arise during the elections and assist them in developing a strong framework to counter such threats.

To this end, the report examines hybrid threats against elections in Western countries (from 2016 to 2023) and analyzes the tactics and strategies employed by responsible actors. In addition, the report provides a framework for countering hybrid threats towards elections, which includes a range of measures such as improved cybersecurity, enhanced cooperation and coordination, and the development of effective response protocols to mitigate the impact of threats.

Finally, the report offers general advice that can be used to strengthen European resilience against hybrid threats to elections. This advice aims to improve election security and prevent the manipulation of the democratic process, thus ensuring that upcoming elections are free, fair, and transparent.

2.2 Method, material and limitations

The report offers a comprehensive analysis of election security based on desk research supported by discussions with election security practitioners, as well as the author's first-hand experience managing Sweden's national election protection efforts for the 2018 and 2022 national elections.

The author's practical involvement in overseeing Sweden's election security during two national elections serves as guidance and as a reference point for understanding and improving election security. However, it is essential to note that the Swedish experience is unique to its electoral system's specific conditions and characteristics. Therefore, not all findings and conclusions drawn from the Swedish context may directly apply to other countries with different electoral systems and conditions.

2. Hybrid threats to elections

Hybrid threats in the context of elections are diverse and sophisticated, encompassing cyberattacks on election infrastructure, disinformation campaigns, and physical attacks that seek to disrupt the electoral process. This section is dedicated to dissecting these threats, understanding their sources, and exploring their diverse forms.

Through a literature review, the section examines instances of hybrid threats to the conduct of elections. The goal is to describe how these threats have manifested during previous elections and to outline a generic threat assessment for the European elections in 2024.

2.1 Types of hybrid threats to elections

Threats to elections can be broadly categorized into three areas: threats to the conduct of elections, threats to trust in the conduct of elections, and threats to the will and ability to vote.[8]

Threats to the conduct of elections seek to interfere with the proper functioning of elections by threatening or harming election officials, or sabotaging or manipulating the electoral process.

Threats to trust in the conduct of elections aim to undermine trust in elections by spreading disinformation, or physically targeting the process to create vulnerabilities that can be leveraged for information influence purposes.

Threats to the will and ability to vote target voters in an attempt to influence their intention to vote, as well as by undermining their ability to vote correctly, thereby disenfranchising groups of voters.

Threats can be carried out through physical attacks, cyberattacks, or information influence activities – individually or in combination. Often, a combination of all these types of threats is used, such as cyberattacks that create a vulnerability that antagonists exploit for malicious influence activities targeting the credibility of elections, ultimately leading to threats and violence against election officials and the physical conduct of the elections.

This report classifies attacks on elections that were reported between 2016 and 2023 into five different types, which include:

1. attacks on election officials,
2. attacks on election infrastructure,
3. attacks on the election results,
4. cyberattacks, and
5. information influence activities.

This classification helps better identify the attack vector, even if the purpose of the attacks could fall within any of the three attack categories mentioned above.

2.2 Reported attacks on elections 2016–2023

This section provides an overview of notable attacks on elections from 2016 to 2023. Although the review is not exhaustive, it emphasizes significant attacks that exemplify the strategies and attack vectors employed. The focus is on illustrating the diversity of attacks and their implications for electoral processes. By describing critical incidents, the section aims to shed light on the evolving nature of election-related threats and the multifaceted challenges they present to maintaining the integrity of democratic systems.

8 Bay et al., "Hot mot svenska allmänna val – Exempel och scenarier för valadministrationen"; Bay, Fjällhed, and Pamment, "A Swedish Perspective on Foreign Election Interference."

2.2.1 Attacks against election officials

A study by International IDEA has illuminated alarming trends facing electoral officials globally. According to the study aggregating data from 21 countries, election officials are increasingly targeted with disinformation and various forms of aggression. The IDEA study further shows that these attacks are strategic and aimed at undermining the credibility of democratic processes and the autonomy of institutions such as electoral management bodies[9] (EMBs). The study also highlights the specific vulnerability of women to gender-based disinformation, a tactic that often evades online moderation and fact-checking.[10] International IDEA's research underscores that beyond damaging individuals, these tactics are part of a broader strategy to undermine democracy.

A Reuters investigative series titled "Campaign of Fear" highlights a worrying pattern of intimidation and threats against US election officials, primarily driven by baseless election fraud claims. These officials, from poll workers to high-ranking state officers, have faced a barrage of threats, including physical violence, torture, and death, with some leading to drastic personal safety measures like going into hiding. The series also underscores the media's significant role in amplifying these unfounded claims, contributing to the surge in threats against these workers.[11]

A Brennan Center survey found that one in six US election officials have personally experienced threats, with a notable number leaving their jobs due to safety concerns.[12] The FBI warned in October 2022 of unusual levels of threats to election workers. These threats have included racist, gendered harassment, and death threats, prompting some election officials to hire personal security or flee their homes.[13] A Swedish Defence Research Agency study reported similar threats in various countries. These include voter aggression, racism, and harassment against election workers in different settings, including polling stations and online environments. The study also detailed threats against election officials, harassment, violence, and racist behaviour, emphasizing the growing global challenge of maintaining election integrity amid such threats.[14]

2.2.2 Attacks on election infrastructure

Threats to physical election infrastructure worldwide, from subtle disruptions to bomb threats and direct attacks, have become a critical concern for electoral integrity and safety. The US Capitol attack on 6 January, 2021, and the unrest in Brazil's capital on 8 January, 2023,

9 An EMB is an organization or body that is legally responsible for managing all or parts of the conduct of elections in a country. EMBs are often referred to as an Election Commission, Election Authority, Election Agency, Department of Elections, Electoral Council, Election Unit or Electoral Board. A country can have several EMBs responsible for different electoral processes, e.g., at the regional and local level.

10 Bicu and Hyowon, "Between Sexual Objectification and Death Threats"; International IDEA and Bicu, "The Information Environment Around Elections."

11 Reuters, "Campaign of Fear."

12 Brennan Center for Justice, "Poll of Election Officials Shows High Turnover Amid Safety Threats and Political Interference."

13 U.S. Department of Justice, "Office of Public Affairs | Readout of Election Threats Task Force Briefing with Election Officials and Workers | United States Department of Justice."

14 Bay et al., "Hot mot svenska allmänna val – Exempel och scenarier för valadministrationen."

are stark examples of political unrest escalating into assaults on democratic institutions. These events, fuelled by misinformation and distrust in electoral systems, symbolize the erosion of trust in the electoral process and the dangerous impact of disinformation.[15]

In Sweden, during the general election in 2022, disinformation surrounding mobile polling stations likely led to an arson attack, further highlighting the vulnerability of election infrastructure to misinformation.[16] Similarly, during the 2020 US presidential election, the TCF Center in Detroit, a vote-counting location, became a hotspot for unrest when angry protesters incited by fraud claims disrupted the counting process.[17]

Bomb threats to polling stations have also been a concern, particularly in the US and Poland. For instance, the state of Georgia experienced threats across ten counties during the 2020 US presidential election,[18] and Poland experienced three bomb threats during its 2023 election.[19] In Poland, the previous orchestration of bomb threats by foreign intelligence services indicates a broader strategy of destabilizing key state institutions and sowing discord through bomb threats during critical events.[20]

2.2.3 Attacks on the election results

While there have been multiple attacks on election infrastructure in recent years and a range of conspiracy theories regarding election fraud,[21] there are very few verifiable reports of attempts to manipulate the election results directly.[22] A notable exception is the #stopthecount campaign in the United States in 2020, which resulted in an attack on the final certification of votes in the US Congress.[23] It is unclear to what extent state-led cyberattacks on US election infrastructure attempted to alter the election results or undermine the electoral system and trust in it. A US congressional report concluded that the attacks did not impact the election results.[24]

Recorded attempts to influence election outcomes include family voting, unauthorized

15 Boadle, Funakoshi, and Wolfe, "Riots at the Brazil Capital"; Thompson, "Final Report of the Select Committee to Investigate the January 6th Attack on the United States Capitol."
16 Kaati and Shrestha, "Digitala diskussioner och de svenska valen 2022."
17 Hutchinson, Karson, Rubin, and Pereira, "Group Tries to Disrupt Ballot Counting at Detroit Convention Center."
18 Dillon, "Threats of Violence on Polling Locations in 10 Georgia Counties."
19 "Polish Police Say Three Warsaw Polling Stations Had Bomb Alerts."
20 Alliance For Securing Democracy, "Polish Authorities Reveal That Russia's Military Intelligence Service Was behind Bomb Threats against Polish Schools."
21 Eggers, Garro, and Grimmer, "No Evidence for Systematic Voter Fraud"; Cohen, "6 Conspiracy Theories about the 2020 Election – Debunked," CBS News; Qiu, "Fact-Checking the Breadth of Trump's Election Lies"; Ohio State University, "Major Pending Election Cases | Case Tracker."
22 Bay et al., "Hot mot svenska allmänna val – Exempel och scenarier för valadministrationen"; Reuters Fact Check, "Re-Examining How and Why Voter Fraud Is Exceedingly Rare in the U.S. Ahead of the 2022 Midterms"; Brennan Center for Justice, "Debunking the Voter Fraud Myth."
23 Thompson, "Final Report of the Select Committee to Investigate the January 6th Attack on the United States Capitol."
24 Select Committee on Intelligence, "Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts Against Election Infrastructure."

assistance at polls, proxy voting fraud, impersonation, coercive transportation to polling stations, and vote buying. Notably, none of these incidents have been attributed to foreign actors. Instead, they have been primarily organized by individuals or politicians at the local level.[25]

2.2.4 Cyberattacks

The threat of cyberattacks on election infrastructure is multifaceted and stems from both foreign and domestic sources. Foreign adversaries, such as Russia, have demonstrated their ability to target and compromise election systems, as evidenced by their interference in the 2016 US presidential election. Cyberattacks may disrupt the voting process, sow discord among voters, or even manipulate election results.[26]

Russia's interference in the 2016 US presidential election included a significant effort to target and compromise US election infrastructure by attacking voter registration databases, voting software and hardware suppliers, as well as local and regional election management systems.[27] In the years since the 2016 election, Russia has continued to target US election infrastructure. In 2021, the National Intelligence Council issued an assessment that Russia is using a range of measures to influence US elections, including cyber operations to target election infrastructure.[28]

In Europe, the cybersecurity of election infrastructure has also been a cause for concern. In 2017, Russia targeted the French presidential election with a multi-pronged campaign of cyberattacks, disinformation, and social media manipulation. In 2019, hackers targeted the Romanian National Agency for Cybersecurity to disrupt the country's elections. During the presidential election of North Macedonia in 2019, a ransomware attack disrupted the state election committee's website for three days, affecting access to voter registration and email servers. DDoS attacks have occurred against election-related institutions in several countries, including during Moldova's parliamentary election in 2019, Ukraine's presidential election in 2019, and the Swedish general elections in 2018 and 2022.[29]

The rising cyber threat posed by domestic actors, including extremist groups, disgruntled individuals, and hacktivists, is also a cause for considerable concern. Recent incidents involving unauthorized access to and dissemination of voting machine data in the United States underscore the problem. These breaches, often fuelled by misinformation and conspiracy theories, threaten the integrity of the voting infrastructure and erode public confidence in the electoral process.[30]

2.2.5 Information influence activities

False and misleading information targeting the electoral process or institutions responsible for conducting general elections is a growing concern. This includes allegations of electoral fraud and spreading false and misleading information to undermine confidence in election processes.

25 Bay et al., "Hot mot svenska allmänna val – Exempel och scenarier för valadministrationen."
26 Select Committee on Intelligence, "Report of the Select Committee on Intelligence".
27 Ibid.
28 National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections."
29 Bay et al., "Hot mot svenska allmänna val – Exempel och scenarier för valadministrationen."
30 AP News, "Breaches of Voting Machine Data Raise Worries for Midterms."

The misinformation has been spread by both domestic and foreign actors – often in symbiosis.

The Digital Media Observatory's Task Force on the 2024 European Parliament Election has reported that false narratives concerning voter fraud, foreign influence, and unfair practices were alarmingly widespread in at least 11 European countries during 2023. These false narratives mainly centred around accusations of voter fraud or alleged unfair practices, which were likely attempts to undermine democratically elected representatives' legitimacy and to discredit the election system. Worryingly, the use of AI to fabricate election fraud evidence was identified in 2023.[31]

Reports from the US Intelligence Services revealed that several foreign actors had attempted to increase public mistrust in the US election process in 2020 and 2022.[32] Pro-Kremlin disinformation campaigns have targeted US and European elections since at least 2014, including the Bulgarian, Dutch, Austrian, Italian, French, German, Catalan, Czech, Ukrainian, Slovakian, and European Parliament elections, as well as the elections in North Macedonia and the Brexit referendum, to mention just a few.[33]

Election-related disinformation can take many forms, as exemplified by the 2018 US midterm elections, during which voters in various states received text messages with false information about polling stations. In 2020, Iranian cyber actors posed as an American right-wing organization and spread threatening messages to voters registered with the Democratic Party. In North Macedonia, during a referendum in 2018, disinformation was spread on social media urging citizens to "burn their vote" to reduce voter participation. During the 2020 US presidential election, American voter groups were also targeted with disinformation about the reliability of mail-in voting.[34]

The Election Integrity Partnership has identified several key narratives in election-related disinformation campaigns. These include false claims of widespread voter fraud and rigged processes, narratives aimed at voter suppression through misinformation about polling stations and requirements, and efforts to delegitimize election results by alleging fraud or theft. Misinformation about voting procedures and security is common, as are complex conspiracy theories implying foreign interference or covert control. Additionally, exaggerated or false narratives about intimidation and safety at polling stations are used to discourage voting and create a sense of chaos.[35]

A recent report by the Alliance for Securing Democracy explores how AI tools could exacerbate vulnerabilities that malign actors may exploit to undermine the integrity of elections. The report assesses that the use of AI could further fuel election subversion narratives and attempts at election interference by enabling

31 Panizio, "Disinformation Narratives during the 2023 Elections in Europe."
32 National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections"; National Intelligence Council, "Foreign Threat to the 2022 Elections."
33 Kalenský, "Russian Disinformation Attacks on Elections: Lessons from Europe."
34 Bay et al., "Hot mot svenska allmänna val – Exempel och scenarier för valadministrationen."
35 Stanford Internet Observatory et al., "The Long Fuse"; Election Integrity Partnership, "Election Official Handbook."

disinformation producers to readily fabricate images, audio, and video at scale to support election denialist narratives.[36]

2.3 Threat actors

Elections are targeted by threat actors seeking to influence outcomes, sow discord, or undermine public trust in democratic institutions. These actors range from states and state-sponsored entities to independent hackers, extremist groups, and malign domestic political actors.

All of these actors can operate through various channels, often amplifying each other. Identifying and countering these diverse threats requires a multifaceted and vigilant approach to protect the integrity of elections. The following two sections detail some known actors and their modus operandi.

2.3.1 Foreign actors

Russia has a well-documented history of interfering in elections to undermine the integrity of democratic institutions, influence public opinion, and create discord. It has used sophisticated cyberattacks, hack-and-leak operations, state-sponsored media and covert social media campaigns to propagate disinformation. Russian interference tactics have included attacks on election infrastructure to compromise the integrity of the electoral process, cause confusion, and undermine public confidence in election outcomes. Russia has also employed tactics designed to undermine the credibility of elections, such as spreading false narratives about voter fraud, election rigging, and other claims that cast doubt on the legitimacy of election outcomes. Russian state-controlled media outlets and covert social media operations have disseminated disinformation to influence public opinion and exacerbate social divisions.[37]

Iran has used online platforms extensively to disseminate election-related propaganda and disinformation. It has also used cyberattacks to target the digital infrastructure of elections in an attempt to undermine the integrity of the electoral process.[38]

China's approach to influencing elections has been less aggressive, with an emphasis on shaping global narratives to favour its long-term strategic interests. China has also leveraged its economic influence, state-controlled media and social media manipulation to promote narratives favourable to its political and economic interests.[39]

2.3.2 Domestic actors

Local actors, such as malign domestic political actors and individual activists, are a growing threat to elections. Local actors use tactics similar to foreign actors, such as disinformation and

36 Gorman and Levine, "The ASD AI Election Security Handbook."

37 National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections"; Landay and Lewis, "US Intelligence Report Alleging Russia Election Interference Shared with 100 Countries"; Kalenský, "Russian Disinformation Attacks on Elections: Lessons from Europe"; Insikt Group, "Aggressive Malign Influence Threatens to Shape US 2024 Elections."

38 National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections"; Insikt Group, "Aggressive Malign Influence Threatens to Shape US 2024 Elections"; United States Institute for Peace, "Report: Iran Accelerates Cyberattacks."

39 National Intelligence Council, "Foreign Threat to the 2022 Elections"; Insikt Group, "Aggressive Malign Influence Threatens to Shape US 2024 Elections"; Kurlantzick, "China's Growing Attempts to Influence U.S. Politics."

propaganda, to manipulate voter perceptions.[40] Social media platforms have been a primary battleground for domestic actors, who have spread disinformation about the conduct of elections and engaged in online harassment campaigns targeting election officials and politicians. Voter suppression and intimidation tactics have been used to discourage certain voter groups from participating in the electoral process. Such tactics have involved spreading false information about voting procedures, questioning voter eligibility, or creating physical or psychological barriers to voting. Recently, cyberattacks have been used more frequently by local actors to target the credibility of the electoral system.[41]

Addressing the threat posed by local actors is challenging since their actions often fall into legal and ethical grey areas, making it harder to regulate and counteract them. A balanced approach is required to protect democratic processes while preserving free speech and political participation. Efforts to counteract local interference should therefore include enhancing public awareness and implementing measures grounded in robust legal and regulatory frameworks.

40 Siddiqui and Bing, "U.S. Security Officials Worry about Homegrown Election Threats"; Bay et al., "Hot mot svenska allmänna val – Exempel och scenarier för valadministrationen"; AP News, "Breaches of Voting Machine Data Raise Worries for Midterms"; Insikt Group, "Aggressive Malign Influence Threatens to Shape US 2024 Elections."

41 Bay et al., "Hot mot svenska allmänna val – Exempel och scenarier för valadministrationen"; Cassidy, "Breaches of Voting Machine Data Raise Worries for Midterms"; Insikt Group, "Aggressive Malign Influence Threatens to Shape US 2024 Elections."

3. Countering hybrid threats to elections

The field of election security is constantly evolving, with international organizations, governments and electoral management bodies (EMBs) worldwide working to improve election security in response to escalating threats. However, there is still a lack of established methods, procedures, and best practices for building resilience and countering threats to the election process.

This section draws on the experience of Swedish election protection efforts,[42] case studies,[43] available literature,[44] discussions with subject matter experts, and lessons identified during tabletop exercises organized by Hybrid CoE. The recommendations and suggestions presented are intended as general guidance for governments and EMBs.

3.1 Framework for countering hybrid threats to elections

In a discussion paper on protecting elections, Sead Alihodžić defines election protection as "efforts to prevent, withstand or recover from negative occurrences that may undermine the integrity of electoral processes and results. In that respect, the protection of elections is considered part of a broader effort to promote electoral integrity".[45]

Various strategies exist to enhance electoral integrity. Typically, countries establish legal and institutional frameworks, such as election laws and independent electoral management bodies. However, these measures may not always be enough to protect electoral integrity as complex electoral processes and antagonistic actors make elections vulnerable to threats, risks and crises. Therefore, the skill of governments, EMBs and ultimately electoral administrators in managing dynamic situations is crucial for the conduct of safe and credible elections.[46]

In practice, election protection is about applying well-known methods of risk management, resilience-building and crisis management to elections. Risk management involves creating procedures to identify and prevent potential negative events that an organization may face. Building resilience focuses on strengthening an organization or system to sustain operations during times of stress and shocks resulting from the risks that do materialize. In contrast, crisis management is mainly concerned with recovering from disruptions and re-establishing normalcy after a crisis.[47]

According to Alihodžić, it is important that election protection efforts are "led by national organizations that are well versed in applying

42 LaForge, "Sweden Defends Its Elections against Disinformation, 2016–2018"; Bay, Fjällhed, and Pamment, "Defending Democracies"; Valmyndigheten, "Verksamhetsskyddsanalys för allmänna val"; Valmyndigheten, "Valsäkerhet | Valcentralen"; Bay et al., "Incidenter under genomförandet av allmänna val i Sverige – Valen 2018 och 2019."

43 International IDEA, "Protecting Elections"; Brattberg, "European Lessons for Tackling Election Interference"; U.S. Election Assistance Commission, "Election Security"; Bay et al., "Hot mot svenska allmänna val – Exempel och scenarier för valadministrationen."

44 Alihodžić, *Protecting Elections*; Arnaudo et al., "Combating Information Manipulation"; The Kofi Annan Foundation, "Protecting Electoral Integrity in the Digital Age"; Levine, Johnson, and Dean Wilson, "Lessons from Other Democracies"; International IDEA, "Protecting Elections."

45 Alihodžić, *Protecting Elections*.

46 Cf. Alihodžić, *Protecting Elections*.

47 Alihodžić, *Protecting Elections*.

risk management, resilience building and crisis management methods".[48] Lessons drawn from Sweden's experience also highlight the importance of collaboration among various governmental bodies, with the EMB at the forefront, guiding, organizing, and often executing strategies. Such coordination is essential for adapting to new challenges, enhancing resilience, and ensuring that the electoral process is robust against disruptions.

In the current threat environment, election protection must be a continuous process, ranging from assessing the situation to updating legislation and election procedures, and preventing, responding to, and recovering from attacks on the election process. The framework outlined below consists of nine key action areas for enhancing the national capability to counter hybrid threats to elections.

3.1.1 Legislating

Protecting elections against hybrid threats requires a robust and evolving legal framework, as all governmental actions must be firmly grounded in law. This is a continuous effort, recognizing that the nature of threats is constantly evolving, and that legislation must adapt accordingly.[49]

In Sweden, a 2020–2021 parliamentary commission study on election security led to new laws enhancing officials' authority to manage polling station disruptions.[50] In the US, increasing threats against election officials have spurred legislative action. Michigan's attorney general has pledged to prosecute threats against officials, while Maine and Vermont are increasing penalties for such threats. Washington State has passed a bill classifying harassment of election workers as a felony, and at the federal level, the proposed legislation aims to double penalties for intimidating election officials.[51]

While establishing a legal framework is the first critical step in securing elections against hybrid threats, it is also an ongoing effort. As threats evolve, so must the legislation, ensuring that electoral systems remain resilient and capable of confronting these multifaceted challenges effectively.

3.1.2 Vulnerability assessment

There are various methods and protocols that an organization can use to identify and assess risks and vulnerabilities, which are often institutionalized under a government-wide policy for risk management.[52] Risk analysis involves a detailed account of potentially adverse events, their likelihood and impacts, and an evaluation of whether the risk can be eliminated, reduced, or left as is. On the other hand, vulnerability assessments identify weaknesses in a process and suggest ways to mitigate them.[53]

Risk analysis is best suited to events that can be assessed based on likelihood and consequences, such as recurring environmental risks. Vulnerability analyses, on the other hand, are

48 Ibid.

49 Cf. Legge, "Att bemöta påverkan mot genomförandet av allmänna val: En studie av det rättsliga ramverket för åtgärder som syftar till att bemöta påverkan mot genomförandet av allmänna val."

50 2020 års valutredning, "Säkerhet och tillgänglighet vid val."

51 Larsen and Ramos, "Election Worker Intimidation."

52 Cf. Alihodžić, *Protecting Elections*.

53 Winehav and Nevhage, "FOI:s modell för risk- och sårbarhetsanalys (FORSA)."

more appropriate for rare events that are difficult to estimate in terms of probability.[54] Given the unpredictable nature of hybrid threats to elections, low levels of risk acceptance, and the need to create resilient operations, vulnerability assessments need to be a central pillar of any election protection effort.[55] However, it is not relevant to study vulnerability in general; rather, it is essential to link vulnerability assessments to a specific event, threat, or risk source. Therefore, a vulnerability assessment requires a threat assessment to identify potential threats to the election system.[56] This assessment should be provided to stakeholders early on to facilitate effective assessment, planning, and response.[57]

Vulnerability assessments in election security involve identifying risks and evaluating the weaknesses in the election infrastructure that threat actors could exploit, encompassing a broad range of factors from the security of physical voting locations to the resilience of IT systems against cyber threats. A vulnerability assessment in election security typically entails several key steps:[58]

- **Identification of critical assets:** This involves listing all critical processes and components of the conduct of the election, such as voter registration, ballot storage and transportation, voting, vote counting and tabulation, result transmission, information and communication systems.
- **Threat identification:** Analyzing potential threats to the election, including cyber attacks, physical security breaches, insider threats, and misinformation campaigns.
- **Vulnerability detection:** Evaluating any weaknesses in the election system, such as software vulnerabilities, inadequate physical security measures, or lack of staff training, which could be exploited by a threat actor.
- **Impact analysis:** Assessing the potential impact of identified vulnerabilities being exploited, considering factors such as the disruption of voting, data breaches, or loss of public trust.
- **Risk assessment:** Combining the information on vulnerabilities and impacts to understand the risk level of different aspects of the election process. Risk assessment enables effective prioritization of mitigation efforts.
- **Mitigation strategies:** Developing and implementing strategies to mitigate identified risks, such as enhancing cybersecurity measures, improving physical security, and conducting staff training sessions.
- **Continuous monitoring and updating:** Regularly monitoring the election infrastructure for new vulnerabilities and updating the assessment as needed, especially in response to emerging threats or technological changes.

This process is iterative and should be conducted regularly to ensure that election security keeps pace with evolving threats. This requires

54 Ibid.
55 Valmyndigheten, "Verksamhetsskyddsanalys för allmänna val."
56 Winehav and Nevhage, "FOI:s modell för risk- och sårbarhetsanalys (FORSA)."
57 Valmyndigheten, "Verksamhetsskyddsanalys för allmänna val."
58 Ibid.

collaboration among various stakeholders, including election officials, cybersecurity experts, and law enforcement, to ensure a comprehensive understanding of potential vulnerabilities and the development of robust strategies to mitigate them.

3.1.3 Strengthening resilience

Building on vulnerability assessments, enhancing the resilience of the election system is often required. While adjusting the legal framework for election administration can be a lengthy and continuous process, immediate steps can often be taken to fortify election systems.[59] Resilience-building measures can be categorized as detection-oriented, prevention-oriented, and management-oriented protective measures.[60]

- **Detection-oriented protective measures** involve implementing surveillance systems, conducting regular audits, and utilizing intrusion detection. The goal is to ensure timely identification of any anomalies or breaches in the election process.
- **Prevention-oriented protective measures** involve physical and digital barriers to delay or prevent attacks. Enhanced cybersecurity protocols, firewalls, and multi-factor authentication systems are implemented. Physical measures can include secured facilities for ballot storage and robust transportation security for election materials.
- **Management-oriented protective measures** involve a rapid and effective response to incidents. Training staff in crisis management, having a dedicated response team for cybersecurity incidents, and coordinating with law enforcement agencies for physical security threats are key components.

To mitigate cyber threats to elections, election officials need to take several measures. They must upgrade their election systems to meet rigorous cybersecurity standards and enforce robust cybersecurity protocols. Election officials and staff should also receive comprehensive cybersecurity training to effectively recognize and mitigate potential threats.[61]

Additionally, ongoing training for staff in cybersecurity, emergency protocols, and misinformation handling is essential to prevent, handle and mitigate the effects of any attacks. Collaborations with supporting agencies, contractors, and security experts ensure a unified approach to election security. Regularly updating and practising emergency response and recovery plans prepares the election system to manage and mitigate the impact of any security incidents effectively.[62]

3.1.4 Communicating and educating

Electoral management bodies (EMBs) stand at the forefront of combatting the effects of electoral information influence activities, such as disinformation. They are uniquely positioned to foster a climate of trust and credibility by disseminating accurate and reliable electoral information, and building enduring relationships with diverse stakeholders, including voters,

59 Valmyndigheten, "Verksamhetsskyddsanalys för allmänna val."
60 Ibid.
61 CISA, "Best Practices for Securing Election Systems."
62 Valmyndigheten, "Verksamhetsskyddsanalys för allmänna val."

media personnel, political figures, and election officials.[63]

Effective communication is crucial for enhancing the resilience of the election system. Through clear and credible messaging, EMBs have the opportunity to build and maintain public trust, effectively dismantling disinformation narratives and safeguarding the electoral process against undue influence. To effectively address the challenge of electoral disinformation and enhance the integrity of the democratic process, recent research has identified a variety of strategies that promote resilience and trust.[64]

By prioritizing the dissemination of accurate and reliable electoral information, EMBs can establish a foundation of trust and credibility among a wide range of stakeholders. This approach not only involves sharing factual content but also cultivating lasting relationships that help protect the electoral ecosystem against misinformation. Such an approach emphasizes the importance of actively engaging with key audiences such as media, politicians, and voters to inform them about the election system and the protective measures.[65] Well-informed journalists and media play a critical role in maintaining the credibility of the election system by providing accurate, fact-based reporting. Educating journalists about the nuances of the election process and the security measures enables them to discern and debunk misinformation effectively. Informed reporting, in turn, contributes to more resilient public discourse, reduces the impact of disinformation campaigns, and bolsters public trust in the electoral process. Therefore, investing in media literacy and providing clear, factual information for journalists is key to safeguarding the credibility of elections.[66]

Educated politicians also become crucial gatekeepers in protecting election integrity. Their accurate understanding of the election system enhances their resilience to election-related disinformation, and containing disinformation is vital to mitigate its impact. By not amplifying false information, they reduce its influence, maintaining the credibility and integrity of the electoral process.[67]

Additionally, EMBs should consider implementing educational initiatives designed to equip broad demographics with the skills necessary to discern and resist disinformation regarding the conduct of elections. Partnering with reputable fact-checking organizations can also enhance EMBs' ability to quickly identify and correct electoral myths and falsehoods, duly amplifying the availability of accurate information and boosting public confidence in the electoral process.[68]

To effectively respond to active threats, there is a need to develop the capacity to withstand, assess, but also – importantly – to reassure the

63 Myndigheten för samhällsskydd och beredskap (MSB), "Att möta informationspåverkan"; Election Integrity Partnership, "Election Official Handbook"; Arnaudo et al., "Combating Information Manipulation."
64 Ibid.
65 Levine, Johnson, and Dean Wilson, "Lessons from Other Democracies"; Arnaudo et al., "Combating Information Manipulation."
66 Ibid.
67 Cf. Nimmo, "The Breakout Scale."
68 Myndigheten för samhällsskydd och beredskap (MSB), "Att möta informationspåverkan"; Election Integrity Partnership, "Election Official Handbook"; Arnaudo et al., "Combating Information Manipulation."

public of the election system's integrity through prepared and practised incident communication.[69] Moreover, it is vital to convey a strong message that the election system is well-protected and prepared for potential threats. This not only serves to deter antagonists by demonstrating readiness and robust defences, but also reassures stakeholders that there will be consequences for any malicious actions.[70]

Proactive communication should highlight the continuous improvements in election security, explain the processes to detect and mitigate threats, and underscore the legal repercussions of election interference. The goal should be to create an informed electorate and a well-informed set of stakeholders who can actively contribute to the security and credibility of the electoral process.[71]

3.1.5 Cooperation

Effective cooperation among various authorities and entities is crucial to ensure the integrity of elections. To this end, the European Commission has recommended that member states establish national election cooperation networks.[72] These networks provide a platform for electoral authorities to collaborate with other entities on election security matters. Such cooperation is essential for detecting threats promptly and enforcing rules.

The European cooperation network on elections, established in 2019, exemplifies this approach. Representatives from member states' authorities meet to discuss various topics crucial for free and fair elections. The network facilitates practical exchanges on election security to address potential risks and solutions for building resilient electoral and democratic systems across the EU.[73]

A national election cooperation network should involve all government entities with a role in protecting the conduct of elections. Election cooperation networks should ensure joint situational awareness and a focused collaborative effort in protecting elections.[74] Lessons learned from the Swedish Election Cooperation Network indicate that such a network can effectively be used to facilitate:

- Joint mapping of election infrastructure, which involves identifying vulnerabilities and potential threats to the system.
- Collaboratively developing strategies to address identified risks.
- Equipping all involved actors with the necessary tools to support election protection efforts.
- Conducting joint exercises to prepare for various scenarios.
- Incident reporting, joint situational awareness, and joint operational responses during elections.

69 Cf. Belfer Center for Science and International Affairs, "Election Cyber Incident Communications Plan Template."
70 Bay and Snore, "Protecting Elections: A Strategic Communications Approach."
71 Myndigheten för samhällsskydd och beredskap (MSB), "Att möta informationspåverkan"; Election Integrity Partnership, "Election Official Handbook"; Arnaudo et al., "Combating Information Manipulation."
72 European Commission, "Securing Free and Fair European Elections."
73 European Commission, "European Cooperation Network on Elections."
74 European Commission, "Securing Free and Fair European Elections."

Lessons identified from recent Swedish elections underline the value of these networks. Having a government entity or an election management body lead ensures a consistent focus over time. Additionally, the need for these networks extends before, during, and after elections – to assess, prepare, identify, respond, and recover and improve, respectively.

The cooperation should also extend to the European level, with national networks effectively interacting with the European network. This broader collaboration enhances the overall capacity to protect European elections against a wide range of threats, ensuring the security and integrity of the democratic process.

3.1.6 Exercises

Exercises are essential in ensuring the security of elections.[75] They are practical tools for EMBs, interagency collaboration, and government-wide coordination. Such exercises are crucial in identifying vulnerabilities, enhancing response capabilities, and refining strategies for potential attacks. The nature and scope of these exercises can vary, but experience shows that full-scale exercises are particularly effective in unearthing real-world challenges and weaknesses within the system.[76]

Exercises provide a realistic setting to assess how well various components of the election system work together under stress, and to identify any flaws or gaps in procedures. The primary objective of running an exercise is to test and evaluate the effectiveness of existing security measures and response protocols. While any type of exercise is beneficial, full-scale exercises simulating a real event as closely as possible often reveal real-world challenges and problems more effectively. These exercises should simulate election scenarios as closely as possible, including potential threats and planned responses.[77]

Implementing red-team exercises, where a group actively tries to exploit system vulnerabilities, can be particularly valuable as this approach can test the actual capabilities of the election system to withstand and respond to attacks, offering a realistic assessment of readiness.[78] Setting up an effective exercise regime involves planning, clearly defining objectives, and developing scenarios that reflect potential threat models such as cyberattacks, physical security breaches, or disinformation campaigns. Collaboration is essential in this process, necessitating the involvement of various stakeholders such as cybersecurity teams, law enforcement, and communication experts.[79]

Post-exercise debriefing and analysis are as crucial as the exercise itself. This phase involves thoroughly reviewing the outcomes, allowing participants to identify strengths and weaknesses in their response strategies. Insights gained from these exercises should inform continuous improvements in protocols, training, and overall security measures.[80]

Regularly scheduled exercises, becoming progressively complex, ensure that EMBs and collaborating agencies are consistently prepared

75 CNA, "Using Exercises to Identify Election Security Risks."
76 Ibid.
77 Ibid.
78 Cf. Bay, Twetman, and Batrla, "Camouflage for the Digital Domain."
79 CNA, "Using Exercises to Identify Election Security Risks."
80 Ibid.

for evolving threats. Aligning these exercises with the election cycle and changes in the threat landscape ensures ongoing relevance and effectiveness. By implementing a structured exercise regimen, EMBs and government agencies can improve their preparedness for real-world challenges, enhancing the overall security and integrity of the election process.

3.1.7 Detection

Establishing incident reporting, early warning, and detection mechanisms is an important component in the election security framework. This step emphasizes the necessity for developing the capabilities and collaborative efforts needed to identify any threats to the election process. The ability to detect and respond to threats promptly hinges on the efficient functioning of three mechanisms. [81]

Firstly, developing robust incident reporting systems within EMBs is essential. These systems should be designed to capture and prioritize unusual activities or potential threats quickly. A well-defined process for reporting incidents ensures that anomalies can be identified and addressed swiftly and effectively.[82]

Secondly, the establishment of an early warning capability is crucial. This should be capable of monitoring various potential threats, from cyber-related incidents to physical security breaches. This requires a blend of technological tools and human expertise to analyze patterns and signals that could indicate a potential threat.[83]

Collaboration plays a significant role in broadening the scope of threat detection. By partnering with other agencies, including cybersecurity firms, law enforcement, and intelligence agencies, EMBs can leverage a wider network of information and expertise. This collaborative approach enhances the ability to detect diverse threats impacting the election process.[84]

Moreover, an independent assessment of the information environment, particularly regarding disinformation about election fraud, is also important for evaluation purposes after the election. This independent evaluation helps to objectively describe the election process and assess the detection mechanisms' effectiveness, providing valuable insights for future improvements.

Monitoring needs to encompass both the information and the physical environments. The integration of these two aspects is essential to respond effectively to digital threats that may have the potential to escalate physically. Bridging the gap between digital and physical threat response mechanisms ensures a comprehensive approach to election security.[85]

3.1.8 Responses

Responding to threats necessitates a collaborative approach with relevant agencies,

81 Arnaudo et al., "Combating Information Manipulation"; Election Integrity Partnership, "Election Official Handbook"; Myndigheten för samhällsskydd och beredskap (MSB), "Att möta informationspåverkan."
82 Ibid.
83 Ibid.
84 Ibid.
85 Arnaudo et al., "Combating Information Manipulation"; Election Integrity Partnership, "Election Official Handbook."

where an effective assessment of incidents and coordinated responses are crucial. Responding includes responses in the physical, cyber and information domain. This can encompass everything from coordinating with police to reinforce the physical protection of assets, introducing measures to mitigate the effect of threats and harassment of election workers, to countering ongoing cyberattacks and issuing statements, media advisories or conducting investigations to counter the spread and impact of disinformation.

Responding quickly and effectively to threats requires a unified approach among national, regional, and local agencies. Different agencies, including cybersecurity, law enforcement, and intelligence services, need to work together to evaluate the threat level and determine the necessary response. Operational task forces within the framework of the election cooperation networks play a significant role in ensuring a well-rounded and informed response. These task forces facilitate information sharing and resource allocation, enhancing the capacity to address emerging threats.[86]

The response mechanism also relies heavily on the ability of agencies to support one another. Given the magnitude of potential attacks, there might be a significant need to pool government resources to respond to these threats. Such responses should be prepared and practised in advance to ensure an effective operation, which requires established routines and protocols, enabling agencies to effectively provide or receive assistance. Such mechanisms are fundamental when an agency faces an overwhelming threat or lacks specific capabilities, ensuring that the necessary support is readily available. Coordinating responses across different levels of government is another critical aspect of this step. National-level coordination provides strategic direction and the necessary resources, while regional and local agencies often act as first responders. This multi-tiered coordination ensures that responses are prompt, efficient, and tailored to the specific requirements of the situation.[87]

In essence, responding to threats to election security is about creating a comprehensive response system where agencies are prepared to act independently and in support of one another. This approach is vital to maintaining the integrity and security of the electoral system, ensuring it remains resilient in the face of diverse and evolving threats.

3.1.9 Recovery and evaluation

In the phase of recovery and evaluation in election security, the focus shifts towards restoring normalcy to the election process by addressing and rectifying the immediate impacts of any threats or attacks. It also involves a comprehensive evaluation of the incident and its response, followed by incorporating the lessons learned into future security planning and strategies.[88]

Recovery involves immediately repairing any physical or digital damage, re-establishing secure communications, and ensuring that all aspects of the electoral system function correctly. The assessment phase involves a detailed

86 Bay, Fjällhed, and Pamment, "Defending Democracies"; LaForge, "Sweden Defends Its Elections against Disinformation, 2016–2018"; Brattberg, "European Lessons for Tackling Election Interference"; Arnaudo et al., "Combating Information Manipulation."

87 Ibid.

88 Alihodžić, *Protecting Elections*.

analysis of the incident to understand its nature, the effectiveness of the response, and any gaps in the existing security measures. It is essential to evaluate the entire incident, including the steps taken before, during, and after the event, to identify successes and improvement areas.[89]

These findings are fundamental to refining and strengthening election security strategies, and it is crucial to publish them to maintain public trust and support in the election process. Transparency in how incidents are handled, and the lessons learned from them reinforce public confidence in the electoral system's integrity.

89 Ibid.

4. Conclusions

The complex and ever-evolving landscape of hybrid threats to elections poses a significant challenge to the integrity of democratic processes. A range of ill-intentioned actors from state-sponsored groups to domestic individuals and groups have targeted elections to harm the credibility of a core function of democracy. Acknowledging the presence of actors with the intent and capability to influence upcoming elections, it becomes imperative for election administrations to implement measures to counter these threats proactively. There must be a concerted and proactive effort by European states to safeguard the electoral process against interference, ensuring that the democratic rights of EU citizens are upheld in a secure and trustworthy electoral environment.

This report provides a detailed overview of hybrid threats to elections and recommends that governments focus on nine key action areas for enhancing government capability to counter hybrid threats. The recommended responses underscore the importance of legislative review, vulnerability assessments, strengthening the physical and digital infrastructure of elections, enhancing resilience against disinformation, and conducting thorough exercises and evaluations. The report also emphasizes a collaborative approach and advocates integrating efforts across government to safeguard electoral integrity. By implementing these recommendations, it is possible to bolster the resilience of elections against the sophisticated challenges posed by hybrid threats, ensuring the preservation of public trust and the security of electoral processes.

Disinformation and cyberattacks, particularly those aimed at undermining public trust and compromising election infrastructure, represent the most imminent threats to upcoming elections in Europe. The rapid development of AI and its potential misuse by antagonists generate significant uncertainty regarding future risks, requiring a flexible approach that can adapt to emerging threats. European officials should prioritize strengthening cybersecurity defences for electoral systems, enhancing public awareness campaigns to combat disinformation, and building capacity to identify and counter disinformation-fuelled threats and violence in the physical domain.

Emphasizing transparency and accountability in electoral systems, this report ultimately calls for a sustained commitment to protecting democratic principles, ensuring that electoral processes remain secure and equitable for all, and thereby safeguarding the democratic heritage for future generations.

5. References

2020 års valutredning. "Säkerhet och tillgänglighet vid val." SOU 2021:96, 2021. https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2021/12/sou-202196/.

Alihodžić, Sead. *Protecting Elections: Risk Management, Resilience-Building and Crisis Management in Elections.* International Institute for Democracy and Electoral Assistance (International IDEA), 2023. https://doi.org/10.31752/idea.2023.44.

Alliance For Securing Democracy. "Polish Authorities Reveal That Russia's Military Intelligence Service Was behind Bomb Threats against Polish Schools." Alliance For Securing Democracy (blog). https://securingdemocracy.gmfus.org/incident/polish-authorities-reveal-that-russians-military-intelligence-service-was-behind-bomb-threats-against-polish-schools/.

Arnaudo, Daniel, Samantha Bradshaw, Hui Hui Ooi, Kaleigh Schwalbe, Amy Studdart, Vera Zakem, and Amanda Zink. "Combating Information Manipulation: A Playbook for Elections and Beyond." The International Republican Institute, September 28, 2021. https://www.iri.org/resources/combating-information-manipulation-a-playbook-for-elections-and-beyond/.

Bay, Sebastian, Alicia Fjällhed, and James Pamment. "A Swedish Perspective on Foreign Election Interference." In *Defending Democracies: Combating Foreign Election Interference in a Digital Age.* Oxford: Oxford University Press, 2021.

Bay, Sebastian, and Guna Snore. "Protecting Elections: A Strategic Communications Approach." Riga, Lettland: NATO Strategic Communications Centre of Excellence, 2019. https://stratcomcoe.org/cuploads/pfiles/nato_report_-_protecting_elections_1.pdf.

Bay, Sebastian, Jessica Appelgren, Patrik Thunholm, Elsa Isaksson, and Johannes Lindgren. "Hot mot svenska allmänna val – Exempel och scenarier för valadministrationen." Stockholm, Sweden: FOI, 2022. https://www.foi.se/rest-api/report/FOI-R--5298--SE.

Bay, Sebastian, Patrik Thunholm, Sofia Olsson, Jessica Appelgren, and Gila Paziraei. "Incidenter under genomförandet av allmänna val i Sverige – Valen 2018 och 2019." Stockholm, Sweden: FOI, 2022. https://www.foi.se/rest-api/report/FOI-R--5297--SE.

Bay, Sebastian, Henrik Twetman, and Michael Batrla. "Camouflage for the Digital Domain." NATO StratCom CoE, 2020. https://stratcomcoe.org/publications/camouflage-for-the-digital-domain/59.

Belfer Center for Science and International Affairs. "Election Cyber Incident Communications Plan Template." Belfer Center for Science and International Affairs, 2018. https://www.belfercenter.org/publication/election-cyber-incident-communications-plan-template.

Bicu, Ingrid, and Park Hyowon. "Between Sexual Objectification and Death Threats: Electoral Officials All over the World Face Unprecedented Levels of Disinformation, Aggression and Harassment," November 24, 2022. https://www.idea.int/news/between-sexual-objectification-and-death-threats-electoral-officials-all-over-world.

Boadle, Anthony, Minami Funakoshi, and Julia Wolfe. "Riots at the Brazil Capital." Reuters, January 18, 2023. https://www.reuters.com/graphics/BRAZIL-POLITICS/RIOTS/gkplwxqggvb/.

Brattberg, Erik. "European Lessons for Tackling Election Interference." Carnegie Endowment for International Peace. Accessed December 22, 2023. https://carnegieendowment.org/2020/08/18/european-lessons-for-tackling-election-interference-pub-82561.

Brennan Center for Justice. "Debunking the Voter Fraud Myth." New York, USA: New York University School of Law, 2017. https://www.brennancenter.org/sites/default/files/analysis/Briefing_Memo_Debunking_Voter_Fraud_Myth.pdf.

———. "Poll of Election Officials Shows High Turnover Amid Safety Threats and Political Interference," April 25, 2023. https://www.brennancenter.org/our-work/analysis-opinion/poll-election-officials-shows-high-turnover-amid-safety-threats-and.

Cassidy, Christina A. "Breaches of Voting Machine Data Raise Worries for Midterms." AP News, September 16, 2022. https://apnews.com/article/2022-midterm-elections-technology-colorado-donald-trump-voting-95b862c0cb66aac446a213aace504776.

CISA. "Best Practices for Securing Election Systems," 2024. https://www.cisa.gov/best-practices-securing-election-systems.

CNA. "Using Exercises to Identify Election Security Risks," 2023. https://www.cna.org/centers-and-divisions/ipr/emo/election-security-workshops-and-exercises.

Cohen, Li. "6 Conspiracy Theories about the 2020 Election – Debunked." CBS News, January 15, 2021. https://www.cbsnews.com/news/presidential-election-2020-conspiracy-theories-debunked/.

Dillon, Denise. "Threats of Violence on Polling Locations in 10 Georgia Counties." FOX 5 Atlanta, January 4, 2021. https://www.fox5atlanta.com/news/threats-of-violence-on-polling-locations-in-10-georgia-counties.

Eggers, Andrew C., Haritz Garro, and Justin Grimmer. "No Evidence for Systematic Voter Fraud: A Guide to Statistical Claims about the 2020 Election." *Proceedings of the National Academy of Sciences 118*, no. 45 (November 9, 2021): e2103619118. https://doi.org/10.1073/pnas.2103619118.

Election Integrity Partnership. "Election Official Handbook: Preparing for Election Day Misinformation." Election Integrity Partnership. https://www.eipartnership.net/2020/how-to-prepare-for-election-day-misinformation.

European Commission. "European Cooperation Network on Elections," 2023. https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/eu-citizenship-and-democracy/democracy-and-electoral-rights/european-cooperation-network-elections_en.

———. "Securing Free and Fair European Elections." Brussels, Belgium: European Commission, September 12, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0637&from=EN.

European Parliament. "European Parliament Resolution of 1 June 2023 on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation (2022/2075(INI))," June 1, 2023. https://www.europarl.europa.eu/doceo/document/TA-9–2023–0219_EN.html.

Friel, Katie, and Jasleen Singh. "Voter Intimidation and Election Worker Intimidation Resource Guide." Brennan Center for Justice, October 28, 2022. https://www.brennancenter.org/our-work/research-reports/voter-intimidation-and-election-worker-intimidation-resource-guide.

Gorman, Lindsay, and David Levine. "The ASD AI Election Security Handbook." Alliance For Securing Democracy, February 8, 2024. https://securingdemocracy.gmfus.org/the-asd-ai-election-security-handbook/.

Hutchinson, Bill, Kendall Karson, Olivia Rubin, and Ivan Pereira. "Group Tries to Disrupt Ballot Counting at Detroit Convention Center." ABC News, November 5, 2020. https://abcnews.go.com/Politics/group-disrupt-ballot-counting-detroit-convention-center/story?id=73981354.

Insikt Group. "Aggressive Malign Influence Threatens to Shape US 2024 Elections." *Recorded Future*, December 14, 2023. https://go.recordedfuture.com/hubfs/reports/ta-2023–1214.pdf.

International IDEA. "Protecting Elections," 2023. https://www.idea.int/project/protecting-elections.

International IDEA, and Ingrid Bicu. "The Information Environment Around Elections." https://www.idea.int/theme/information-communication-and-technology-electoral-processes/information-environment-around-elections.

Kaati, Lisa, and Amendra Shrestha. "Digitala diskussioner och de svenska valen 2022," 2022.

Kalenský, Jakub. "Russian Disinformation Attacks on Elections: Lessons from Europe." Washington, D.C.: Foreign Affairs Subcommittee on Europe, Eurasia, Energy, and the Environment, July 16, 2019. https://www.congress.gov/116/chrg/CHRG-116hhrg37051/CHRG-116hhrg37051.pdf.

Kurlantzick, Joshua. "China's Growing Attempts to Influence U.S. Politics." Council on Foreign Relations, October 31, 2022. https://www.cfr.org/article/chinas-growing-attempts-influence-us-politics.

LaForge, Gordon. "Sweden Defends Its Elections against Disinformation, 2016–2018." Innovations for Successful Societies. Princeton, USA: Princeton University, 2020.

Landay, Jonathan, and Simon Lewis. "US Intelligence Report Alleging Russia Election Interference Shared with 100 Countries." Reuters, October 20, 2023, sec. United States. https://www.reuters.com/world/us/us-intelligence-report-alleging-russia-election-interference-shared-with-100–2023–10–20/.

Larsen, Liz, and Julian Ramos. "Election Worker Intimidation." Berkeley Public Policy, 2023. https://gspp.berkeley.edu/research-and-impact/policy-initiatives/democracy-policy-initiative/policy-briefs/election-worker-intimidation.

Legge, Maria Refors. "Att bemöta påverkan mot genomförandet av allmänna val: En studie av det rättsliga ramverket för åtgärder som syftar till att bemöta påverkan mot genomförandet av allmänna val." Stockholm, Sweden: FOI, 2022. https://www.foi.se/rest-api/report/FOI-R--5449--SE.

Levine, David, Kevin Johnson, and Rachael Dean Wilson. "Lessons from Other Democracies: Ideas for Combatting Mistrust and Polarization in US Elections." Alliance For Securing Democracy, June 15, 2023. https://securingdemocracy.gmfus.org/election-lessons/.

Myndigheten för samhällsskydd och beredskap (MSB). "Att möta informationspåverkan : handbok för kommunikatörer," December 2018. https://www.msb.se/sv/publikationer/att-mota-informationspaverkan--handbok-for-kommunikatorer/.

National Intelligence Council. "Foreign Threat to the 2022 Elections." Washington, D.C.: National Intelligence Council, December 23, 2022. https://www.odni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf.

———. "Foreign Threats to the 2020 US Federal Elections," 2021. https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

Nimmo, Ben. "The Breakout Scale: Measuring the Impact of Influence Operations." Brookings, 2020. https://www.brookings.edu/articles/the-breakout-scale-measuring-the-impact-of-influence-operations/.

Ohio State University. "Major Pending Election Cases | Case Tracker." https://electioncases.osu.edu/case-tracker/.

Panizio, Enzo. "Disinformation Narratives during the 2023 Elections in Europe." Florence, Italy: European Digital Media Observatory, 2023. https://edmo.eu/2023/12/13/disinformation-narratives-during-the-2023-elections-in-europe/.

Qiu, Linda. "Fact-Checking the Breadth of Trump's Election Lies." *The New York Times,* August 17, 2023, sec. U.S. https://www.nytimes.com/2023/08/17/us/politics/trump-election-lies-fact-check.html.

Reuters. "Campaign of Fear." Reuters, June 11, 2021. https://www.reuters.com/investigates/section/campaign-of-fear/.

———. "Polish Police Say Three Warsaw Polling Stations Had Bomb Alerts." October 16, 2023, sec. Europe. https://www.reuters.com/world/europe/polish-police-say-three-warsaw-polling-stations-had-bomb-alerts-2023–10–15/.

Reuters Fact Check. "Re-Examining How and Why Voter Fraud Is Exceedingly Rare in the U.S. Ahead of the 2022 Midterms." Reuters, June 2, 2022. https://www.reuters.com/article/idUSL1N2XP2AI/.

Select Committee on Intelligence. "Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts Against Election Infrastructure." Washington, D.C., 2020. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

Siddiqui, Zeba, and Christopher Bing. "U.S. Security Officials Worry about Homegrown Election Threats." Reuters, October 17, 2022, sec. United States. https://www.reuters.com/world/us/us-security-officials-worry-about-homegrown-election-threats-2022–10–17/.

Stanford Internet Observatory, Center for an Informed Public, Digital Forensic Research Lab, and Graphika. "The Long Fuse: Misinformation and the 2020 Election," 2023. https://doi.org/10.25740/TR171ZS0069.

The Kofi Annan Foundation. "Protecting Electoral Integrity in the Digital Age," 2020. https://www.kofiannanfoundation.org/app/uploads/2020/05/85ef4e5d-kaf-kacedda-report_2020_english.pdf.

Thompson, Bennie G. "Final Report of the Select Committee to Investigate the January 6th Attack on the United States Capitol." Washington, D.C.: U.S. House of Representatives, 2022.

United States Institute for Peace. "Report: Iran Accelerates Cyberattacks," July 31, 2023. http://iranprimer.usip.org/blog/2023/may/03/report-iran-accelerates-cyberattacks.

U.S. Department of Justice. "Office of Public Affairs | Readout of Election Threats Task Force Briefing with Election Officials and Workers | United States Department of Justice," August 1, 2022. https://www.justice.gov/opa/pr/readout-election-threats-task-force-briefing-election-officials-and-workers.

U.S. Election Assistance Commission. "Election Security," October 20, 2022. https://www.eac.gov/voters/election-security.

Valmyndigheten. "Valsäkerhet | Valcentralen," December 28, 2023. http://valcentralen.val.se/valsakerhet.4.29e9cb2617d171257e68d8.html.

———. "Verksamhetsskyddsanalys för allmänna val." Sundbyberg, Sweden: Valmyndigheten, 2021. https://valcentralen.val.se/valsakerhet.4.29e9cb2617d171257e68d8.html.

Winehav, Magnus, and Björn Nevhage. "FOI:s modell för risk- och sårbarhetsanalys (FORSA)." Stockholm, Sweden: FOI, 2022. https://www.foi.se/rest-api/report/FOI-R--3288--SE.

Appendix 1 – Useful resources

As the field of election security is maturing and evolving, there is also a growing body of resources available to election security professionals. This appendix lists a selection of useful resources for countering hybrid threats to elections.

Election security

ACE – The Electoral Knowledge Network – Election security
ACE project election security guidance and recommendations.
Election Security: Threats and Analysis – ACE Project

Australian Electoral Integrity Assurance Taskforce
Information about the Australian Integrity Assurance Taskforce.
Electoral Integrity – Australian Electoral Commission (AEC)

Swedish Election Authority – Valcentralen (Swedish)
Collection of election security resources for the Swedish election administration.
Valsäkerhet – Valcentralen

Canadian Election Authority – Election Integrity and Security
Information about Canadian election security strategy and election protection efforts.
International Electoral Activities – Elections Canada

Norwegian Election Authority – Valgmedarbeiderportalen (Norwegian)
Collection of election security resources for the Norwegian election administration.
Sikkerhet og beredskap – Valgmedarbeiderportalen

IFES Cyber and Information Integrity
IFES Election security resources for cyber security and information integrity.
Cyber and Information Integrity – IFES

International IDEA – Protecting elections
Information and materials on the Protecting Elections project, which started in January 2023 and is expected to be finalized in December 2025. IDEA has also developed a Risk Management in Elections Guide, as well as a discussion paper on risk management, resilience-building and crisis management in elections.
Protecting Elections – International IDEA
Risk Management in Elections: A Guide for Electoral Management Bodies – International IDEA
Protecting Elections: Risk Management, Resilience Building and Crisis Response – International IDEA

United States Election Assistance Commission
EAC's latest election security resources for election officials, as well as resources for election official security.
Election Security Preparedness – EAC
Election Official Security – EAC

Cyber security for election authorities

Belfer Center for Science and International Affairs
The Belfer Center has developed practical guides for election professionals regarding cybersecurity best practices, especially regarding cyber incident communication.
State and Local Election Cybersecurity Playbook
Election Cyber Incident Communications Coordination Guide
Election Cyber Incident Communications Plan Template

Canadian Centre for Cyber Security
The Canadian Centre for Cyber Security has released a fourth iteration of its Cyber Threats to Canada's Democratic Process report, which considers cyber threat activity and cyber-enabled influence campaigns that affect democratic processes and elections.
Cyber Threats to Canada's Democratic Process: 2023 Update – Cyber.gc.ca

The Canadian Cyber Security Playbook guides election authorities on anticipating, mitigating, and responding to threats that are specific to Canada's democratic processes. The playbook introduces baseline cyber security measures and best practices.
Cyber Security Playbook for Elections Authorities – Cyber.gc.ca

The Alliance for Securing Democracy at the German Marshall Fund
The Alliance for Securing Democracy has published a handbook that explores how AI tools could exacerbate vulnerabilities that malign actors may exploit to undermine the integrity of elections. The handbook also suggests steps for further protecting elections against AI threats.
The ASD AI Election Security Handbook

International IDEA
International IDEA has developed a report with a collection of 20 case studies, which provides lessons for election authorities seeking to strengthen their defences against cyberattacks.
Cybersecurity in Elections – International IDEA

International Foundation for Election Systems (IFES)
IFES has developed two guides for electoral cyber security: "The Cybersecurity and Elections Primer" provides an overview of cybersecurity in elections, while "Understanding Cybersecurity Throughout the Electoral Process: A Reference Document" expands on the Primer to provide

a more in-depth understanding of key concepts of cybersecurity for elections.
Cybersecurity: Fundamental to Elections – IFES

UK National Cyber Security Centre (NCSC)
NCSC has produced a number of cyber security resources for elections. They offer advice for local election authority IT teams, including reminders about good cyber security practices for the systems that support the delivery of UK elections. NCSC also offers an annual threat assessment and general defending democracy guidance on raising awareness of the cyber threats to democratic processes, institutions, and the people involved in them.
Defending Democracy – NCSC Annual Review 2023 – Election case study
Defending Democracy – NCSC
Election Guidance for Local Authorities – NCSC

U.S. Cybersecurity and Infrastructure Security Agency (CISA)
CISA provides a number of cyber security resources for EMBs, such as best practices for securing election systems and a cyber security toolkit and resources for election protection.
Best Practices for Securing Election Systems – CISA
Cybersecurity Toolkit and Resources to Protect Elections – CISA

U.S. National Institute of Standards and Technology (NIST)
NIST conducts research into election system cybersecurity challenges and identifies standards, guidelines and technologies that can improve the security of these systems. NIST also provide a road map to help local election officials prepare for and respond to cyber threats that could affect elections.
Election Security Research and Projects – NIST
Cybersecurity Guidelines – NIST

Countering information manipulation

The International Republican Institute et al.
The International Republican Institute (IRI), the National Democratic Institute (NDI), and the Stanford Internet Observatory (SIO) have developed a playbook for elections that helps actors to identify, respond to, and build long-term resilience to election-related information manipulation.
Combating Information Manipulation: A Playbook for Elections and Beyond

MIT Election Lab
A white paper produced by MIT Election Lab reviewing the factors that promote or undermine public confidence in election results and election systems. The white paper also offers advice by considering the impact of different approaches to improving public confidence in elections.
Communicating with voters to build trust in the U.S. election system

The Kofi Annan Foundation
A report by the Kofi Annan Commission on Elections and Democracy in the Digital Age examines and reviews the opportunities and challenges for electoral integrity created by technological innovations. The report also offers recommendations on how to engage, empower and educate voters, and how to strengthen the integrity of elections.
Kofi Annan Foundation Report 2020

General advice on countering information manipulation
Several guides and frameworks have been developed to counter information influence activities. Among the more prominent ones are the handbook Countering Information Influence Activities, RESIST 2, ABCDE, DISARM and the Debunking Handbook. Recently, the Carnegie Endowment for International Peace published an evidence-based policy guide on Countering Disinformation Effectively. These resources provide comprehensive guidance on effectively countering information influence activities.

Election security case studies and reports

The Alliance for Securing Democracy at the German Marshall Fund
Countering the Weaponization of Election Administration Mistakes
Deterring Threats to Election Workers
Ideas for Combatting Mistrust and Polarization in US Elections
Taiwan's Election: 2024's Canary in the Coal Mine for Disinformation against Democracy

Carnegie Endowment for International Peace
European Lessons for Tackling Election Interference

The Digital Media Observatory
Task Force on the 2024 European Parliament Election

International IDEA case studies and reports
Timor-Leste: Resilient Elections Built on Experience
Varieties of Electoral Integrity Risk: Protecting Elections in Brazil
Protecting Electoral Integrity: The Case of South Africa
Protecting Democratic Elections Through Safeguarding Information Integrity
Challenges for electoral officials in the information environment around elections

Princeton: Innovations for Successful Societies
Defending the Vote in France: Acts to Combat Foreign Disinformation 2021–2022
Defending the Vote in Estonia: Creating a Network to Combat Disinformation 2016–2020
Sweden Defends Its Elections against Disinformation, 2016–2018
Colombia's National Civil Registry Launches Anti-Disinformation Initiative 2018–2019
Fact-Checkers Unite to Set the Record Straight: The Redcheq Alliance and Information Integrity

Author

Sebastian Bay is a project manager and researcher specializing in national security, hybrid threats, election integrity, disinformation, and online harms. His election expertise is grounded in managing and leading the Swedish election protection efforts for the 2018 and 2022 Swedish general elections, focusing on mitigating threats and ensuring electoral security. He has authored several reports on election security for the Swedish Defence Research Agency (FOI) and the NATO Strategic Communications Centre of Excellence, and written extensively on combatting foreign election interference in general. He has a background with the Swedish Election Authority, the Swedish Defence Research Agency, NATO StratCom COE, the Swedish Civil Contingency Agency, and the Swedish Armed Forces. He holds a bachelor's degree in intelligence analysis and a master's degree in political science from Lund University, Sweden.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats