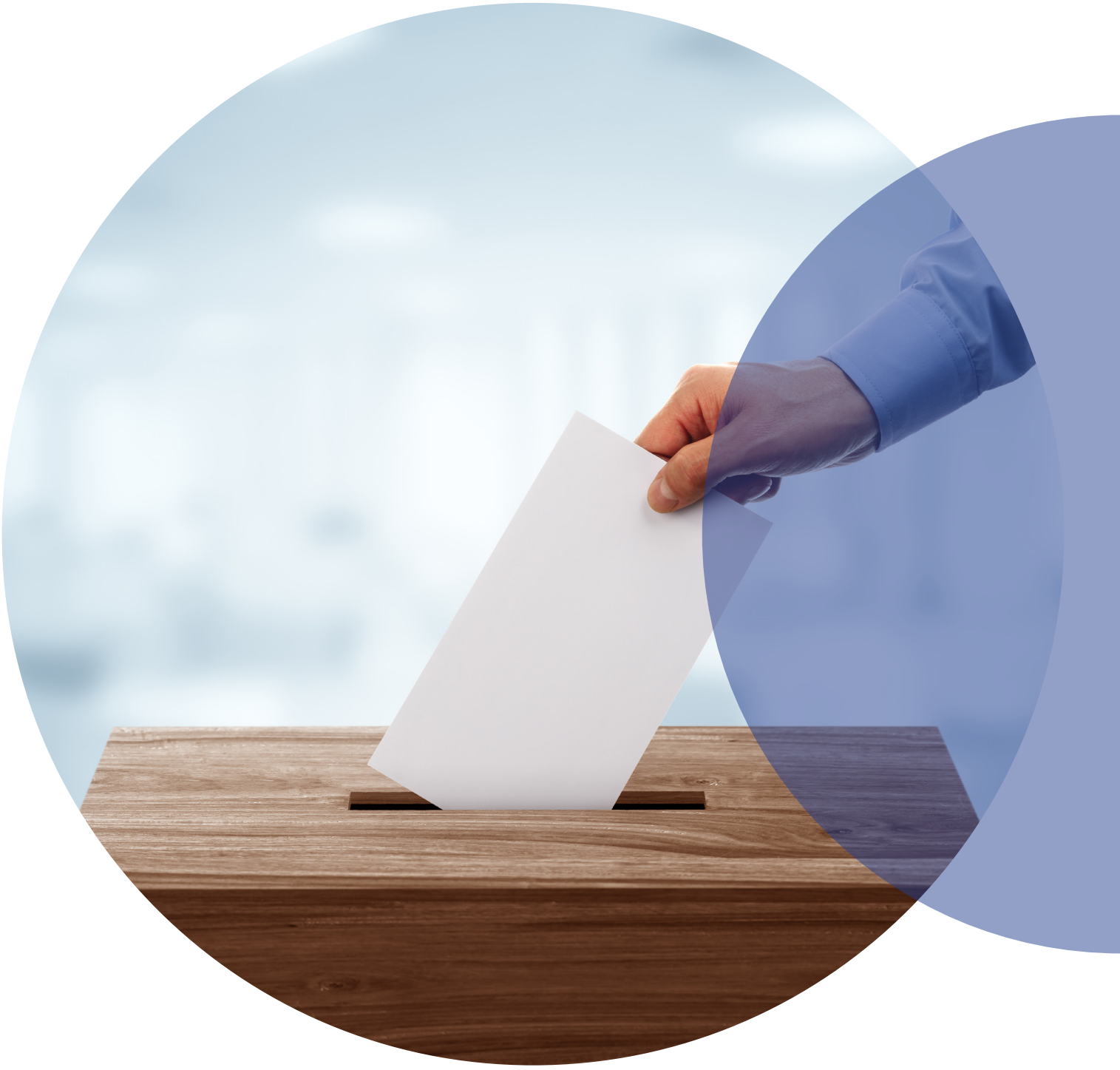
Hybrid CoE Research Report 10

Preventing election interference: Selected best practices and recommendations



Hybrid CoE

Veronika Krátka Špalková & Andrej Poleščuk –
September 2023

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.

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

ISBN 978–952–7472–78–1 (web)
ISBN 978–952–7472–79–8 (print)
ISSN 2737–0860 (web)
ISSN 2814–7219 (print)

September 2023

Cover photo: Brian A Jackson / 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

List of charts

Executive summary

This research shows that efforts to influence elections from abroad are more likely to take place through voter manipulation over the long term rather than through direct attacks on the election system. In consequence, this means that protective measures should focus more on the overall resilience of the population to foreign influence than is currently the case in most states. Our main research questions are therefore: What measures do states take to protect electoral processes in the field of information and cyber security? At what intervals prior to elections are these measures taken? Are these measures effective? For now, states focus more on cyber security than on information security. Cyber threats are more concrete and understandable for decision-makers, and the topic is not politically sensitive.

Most of the actions that the states included in this research can take to protect their elections more effectively can be carried out at any time, regardless of the election cycle. This does not mean, however, that states actually implement measures during this period. On the contrary, we found that regardless of the election cycle, there are several measures that states could – and should – take to protect elections in the long term.

States that were not found to act as proactively in safeguarding their elections as their counterparts started implementing the first measures only a few months before the elections. States were found to implement most of the protective activities in the weeks leading up to and during the elections, when safeguarding focused on securing the electoral system, preparing ballots, informing citizens about the practicalities of elections, and training electoral commissions.

Only a few of the states under study implemented protective measures long after the elections. Their approach to elections is still rather unique in that their protection system is set to work until the new leaders are in office, while in most states protection systems function only until the votes are counted and the election results are published.

Long-term measures were also found to be lacking at the legislative level. In many states, there is no legislation or legal definition of hybrid threats or disinformation, which means that there are no specific laws or regulations in place to combat them effectively. As a result, in many states included in this research, there is a significant gap between the nature of the threat and the ability of governments to effectively counter it through legal means.

Introduction

Ever since the Kremlin launched a new information offensive following the Russian annexation of Crimea in 2014, and the subsequent deterioration of relations with the West, foreign actors such as Russia, Iran, and China have increased their election interference activities. Examples range from meddling in the American presidential election in 2016,[1] the Brexit referendum in the same year,[2] Russian meddling in the French presidential election in 2017,[3] cyberattacks on state institutions to paralyse them,[4] and constant disinformation and influence operation campaigns.[5]

In response to this new form of foreign interference, many states in the European Union and NATO have intensified their preparedness for threats such as cyberattacks against election infrastructure and malign disinformation campaigns. This report aims to collect and categorize the best practices from a number of European Union and NATO countries – Canada, the Czech Republic, Estonia, Finland, France, Germany, Latvia, Lithuania, Poland, Slovenia, Spain, Sweden, the United Kingdom, the United States – and two close allies which are not members – Ukraine and Taiwan.

Given that the goal of the research report is to present the most effective measures in place for protecting elections, not all countries included in the report will be represented equally. The research was conducted uniformly across all countries, but some of them have more sophisticated election protection systems and have established more rules, and hence the examples of effective measures come from those countries. A summary table in the Annex[6] lists the measures taken by all countries included in the research.

Interviews with experts from all involved countries and detailed desk research have been used to analyze the states' approaches to cyber and information security, and their cooperation with the private sector and civil society. The focus is on the measures that these states apply to protect their electoral processes. The measures were categorized according to their type (cyber security measures and information security measures) and the period during which

1 Abigail Abrams, 'Here's What We Know So Far About Russia's 2016 Meddling', *TIME*, 18 April, 2019, https://time.com/5565991/russia-influence-2016-election/. [Unless indicated otherwise, all links were last accessed on 18 August 2023.]

2 Stephen Castle. 'U.K. Ignored Russia's Interference in Democratic System, Report Finds', *The New York Times*, 21 July, 2020, https://www.nytimes.com/2020/07/21/world/europe/uk-russia-report-brexit-interference.html.

3 Natalie Nougayrède, 'Spectre of Russian influence looms large over French election', *The Guardian*, 12 April, 2017, https://www.theguardian.com/world/2017/apr/12/russian-influence-looms-over-french-election.

4 'Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure', CISA, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22–110a.

5 Voice of America, 'Foreign Election Disinformation Campaigns Well Underway, Researchers Say', 2022, https://www.voanews.com/a/foreign-election-disinformation-campaigns-well-underway-researchers-say-/6789393.html.

6 The table in Annex 1 does not seek to capture every single action but rather to highlight the key activities. Blank boxes should not be taken necessarily to indicate that the state takes no action in the relevant area.

they are applied during an election year. The analysis resulted in a list of policy recommendations to be applied to safeguard electoral processes.

The findings are mainly based on official strategic documents of individual countries, the formulation of legal acts related to cyber security, elections, and political party financing. An important part of the research is also the various official guidelines issued by different authorities in different countries to provide information about elections and their progress. Official information campaigns and training materials in the field of cyber and information security were also a source of information.

The election protection research in this paper is not exhaustive. For example, actual cases of actions that countries have taken and how successful they have been would certainly merit further research.

Methodology

This study uses qualitative research methods (content analysis of documents and texts, semi-structured interviews) to make the most accurate observations possible on measures to safeguard electoral processes in selected countries. It is based on detailed desk research and interviews with experts in the field in each of the countries covered. The study focuses on selected Participating States of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE): Canada, the Czech Republic, Estonia, Finland, France, Germany, Latvia, Lithuania, Poland, Slovenia, Spain, Sweden, the United Kingdom, and the United States. In addition, it includes two countries that are in the frontline of foreign interference activities: Ukraine and Taiwan.[7]

In the first phase, preliminary interviews were conducted with experts on the topic of foreign interference in elections in general, regardless of their nationality. This was an effective way to gain insights into the issue, and to make contacts for further interviews with experts in individual countries for the desk research phase.

In the second phase, a framework with two broader focus areas was created. The first focused on the domains identified as posing the greatest risk to the security of electoral processes: cyber and information. The second focused on future developments in safeguarding electoral processes: cooperation with the private and non-profit sectors.

In the third phase, country-specific countermeasures were collected. For each country, desk research was conducted first, after which local experts were approached. The expert interviews were crucial for ensuring that the interpretation of the data was correct, and to gain access to information not discoverable otherwise. The goal was to obtain as much information as possible about the specific measures implemented to protect elections in the areas of cyber and information security, and to ascertain whether the countries were working with the private and/or non-profit sector to do so.

The fourth and final research phase consisted of cataloguing the collected measures. A complete list of measures in all areas and countries can be found in the Annex.

7 The analyzed countries were selected by Hybrid CoE. Given the scope of the report, it was not possible to cover all of Hybrid CoE's Participating States in a single report. Around one-third of the Participating States were selected based on two principles: a) an informed guess as to which countries have been the most active in this regard since 2014; b) their representative regional distribution. On top of the selected Participating States, two countries with the most "frontline" experience of election meddling – Ukraine and Taiwan – were included because their unique situation is believed to offer insights for Hybrid CoE's Participating States.

Overview of the countermeasures

This section describes the measures that the countries take in the areas of cyber and information security. The measures are classified into four time periods according to the phase in which they are implemented:

1) measures taken regardless of the election cycle;
2) measures taken 3 to 12 months before elections;
3) actions taken less than 3 months before elections; and
4) measures taken during and after elections.

In each period, key objectives were identified that different states want to achieve in protecting elections from foreign interference. Within each key objective, individual activities that different states undertake to accomplish the objective were identified. These are described in detail for those countries with the best experience or that have been applying them for a long time. A summary table is included in the Annex.

The first set of measures describes actions aimed at ensuring the integrity of elections, which are not tied to any particular election cycle. The measures are grouped into four key objectives: preparing the election system and infrastructure; preventing election interference through foreign financing; building citizens' resilience to foreign influence; and limiting the possibilities of foreign information influencing. Each key objective can be achieved with specific activities, such as preparing the voting system and registers.

The second set of measures describes actions to be taken 3 to 12 months before elections, which are grouped into two key objectives: preparing and securing the voting infrastructure, and raising awareness of threats related to elections. Specific activities include, for example, penetration testing of election systems, protection of voter databases and candidate registers, and cyber and information security training for election staff.

The third set of measures are to be taken less than three months before elections, and they fall under the key objective of informing the public about the practicalities of upcoming elections. Specific activities include, for example, official awareness campaigns.

The fourth set of measures includes those to be taken during and after elections. These measures fall under two key objectives: ensuring a smooth and secure election process and ensuring the establishment of new leadership without distrust in the election results. Specific activities may include ensuring the physical security of committees and voters, and ensuring transparent vote counting.

Measures applied regardless of the election cycle

Most of the countries consider the protection of elections to be a matter of concern a few weeks beforehand and only until the election results are announced. Thus far, only a few countries are implementing safeguarding measures throughout the election year. Their systems are also designed to function in the immediate post-election period.

Four key objectives that fall into this period were identified as:

1. Preparing the electoral system and infrastructure
2. Preventing election interference through foreign financing
3. Building citizens' resilience to foreign influence
4. Limiting the possibilities of foreign actors to conduct information influencing

For each objective, specific activities were identified that states are carrying out to achieve the objective. For each activity, an example of how countries implement it is also described.

Key objective 1: Preparing the electoral system and infrastructure

In the 21st century, almost every country uses some sort of electronic system as part of their election infrastructure (i.e., voting, counting the ballots, presenting and publishing the results), which is why it is essential to prepare an electoral system. Preparatory measures consist of several elements, such as the technologies used in the electoral system and their area of use.

This section presents best practices from countries where information system technologies are most widely used. Activities to support the objective of preparing the election infrastructure include:

- Activity 1: Preparation of the voting system/software
- Activity 2: Preparation of the registers
- Activity 3: Testing the security of political parties' websites

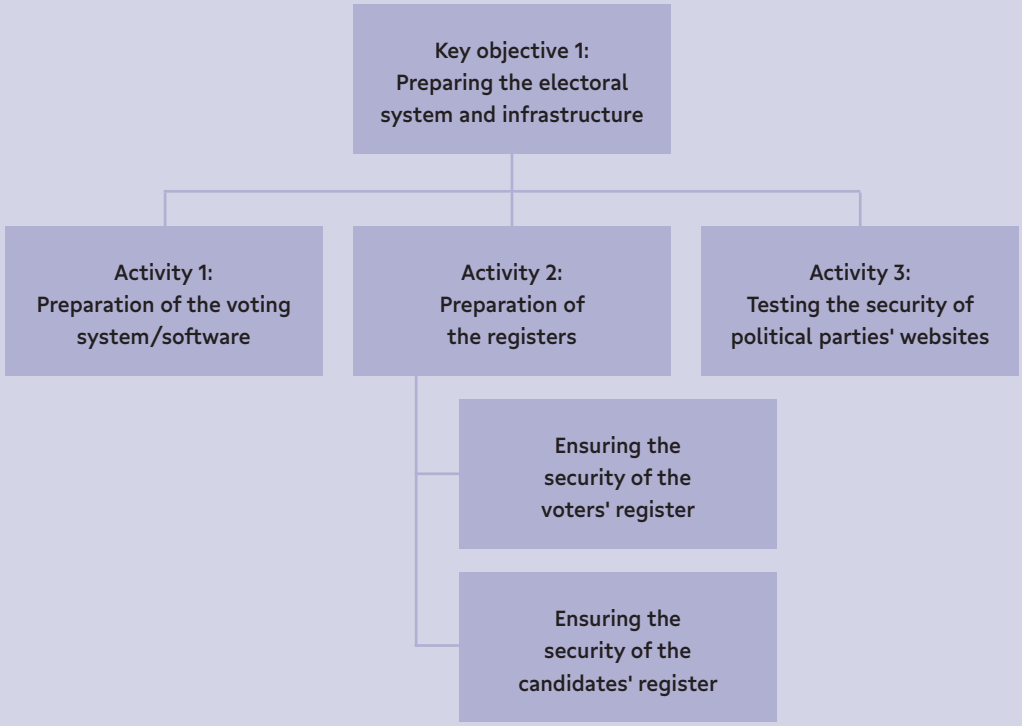
Activity 1: Preparation of the voting system/software

Most of the countries undertake various pre-election preparatory activities directly related to the voting system or software. However, only a few of them start this preparatory work earlier than a year before the election. One of the countries preparing well in advance is Estonia, which we present as an example of best practices in preparing a voting system/software.

Since the early 2000s, Estonia has been developing a digital society, e-Estonia, where citizens can effortlessly exercise their democratic rights and access bureaucratic services provided by the state and the government online.

Estonia has become one of the most advanced countries in the world in terms of the digitalization of government services. In fact, 99% of public services are provided online, with the exception of marriage, divorce, and inheritance proceedings. Thanks to the high level of digitalization, the country has been able to hold

Chart 1. Preparing the electoral system and infrastructure



elections online since 2005 (with the first talks about the system taking place in 2001).[8] Voters can use the e-vote system or a pen and paper alternative for all elections in the country.

The preparation of the infrastructure is carried out in cooperation with the Information System Authority (RIA), the primary state institution responsible for the nation's digital infrastructure, which maintains public trust as a central pillar of digital service design and governance. The protection of Estonian elections begins with a setup phase, focused on registering candidates (see the section below), updating a database of voters, and preparing the voting software. To avoid the risk of hackers exploiting undetected bugs in the software, Estonia develops new software for every election.

Activity 2: Preparation of the registers

In most countries, it is customary to use registers for different purposes during elections, such as registering voters and candidates. To prevent registers from being attacked by a malign actor, they must be kept up to date and protected.

Elections Canada is the election agency of Canada, which conducts federal elections and referendums in the country.[9] It also provides training on elections, cooperates with government agencies, and maintains the Electors Registration Database.[10] At the federal level, Canada's elections are conducted manually while voter databases are electronic. Voter registration databases are cloud-based in certain provinces and territories (Alberta, British Columbia, Northwest Territories, Prince Edward Island, and Saskatchewan), which puts them at greater risk of external manipulation than traditional, offline registers.

8 Piret Ehin, Mikhel Solvak, Jan Willemson, and Priit Vinkel, 'Internet voting in Estonia 2005–2019: Evidence from eleven elections', *Government Information Quarterly*, Volume 39, Issue 4, October (2022), https://www.sciencedirect.com/science/article/pii/S0740624X2200051X.

9 Ibid.

10 Ibid.

The Canadian Communications Security Establishment (CSE)[11] has stated that the main goal of malign actors is to prevent citizens from registering as voters, prevent them from voting, tamper with election results, and steal voter databases. To improve the security of the databases, CSE provides Elections Canada with all the necessary assistance and capabilities to protect the election infrastructure,[12] including cybersecurity advice, guidance on how to protect its systems and networks from cyber threats, and even the disruption of malicious cyber activity aimed at the election infrastructure, if needed.[13]

Ukraine is another example of a country with a robust preparatory protection system. First, the Central Evidence of Voters system is designed to protect the voter database from unlawful manipulation (i.e., the editing or removal of voters' personal information). All voters can check information not only about themselves but also about a limited number of other voters.[14]

Second, Ukraine does preparatory work through the Central Voters Committee (CIK), a permanent collegial state body of the Central Election Commission with the power to organize the preparation and conduct of all elections in the country.[15] Protection of the Committee's infrastructure is multi-layered. For example, protection against the unauthorized entry and/or deletion of data is achieved by:

- the required simultaneous use of two keys to access the State Register;
- recording every change in the data on each voter in the service fields of the registry;
- publicity about the database.

There is also additional protection against the unauthorized transfer of data from the registry. This goal is achieved by:

- special encryption and tamper-proof CDs, which are transferred to subjects of the electoral process (political parties);
- restricted access to the data on the servers where the information resides;
- the inability to use the register database to produce voter lists without the involvement of the CIK.

Activity 3: Testing the security of political parties' websites

Election systems as well as political parties' websites must be tested to ensure that they work under critical conditions and pressure. Lithuania provides a good example of regular

11 'Cyber Threats to Canada's Democratic Process', Communications Security Establishment, n.d., https://www.cyber.gc.ca/sites/default/files/cyber/publications/cse-cyber-threat-assessment-e.pdf.

12 'CSE: Annual Report 2021–2022', Communications Security Establishment, https://www.cse-cst.gc.ca/sites/default/files/2022–06/cse-annual-report-2021–2022-e_0.pdf.

13 Ibid.

14 Bill no. 2536-VI 'On the State Register of Voters', https://zakon.rada.gov.ua/laws/show/698–16#n49. Article 10 (2) speaks about the possibility to check the accuracy of information about "yourself and other voters". One example is the possibility to request information from an institution on behalf of a voter that has mobility limitations (see Art. 21 (2) of the Bill). Such access can only be granted with the consent of that person in order to protect the personal data of other voters.

15 Decree 'On approval of the Regulations of the Central Election Commission', 26 April, 2005 No. 72, https://act.cvk.gov.ua/acts/pro-zatverdzhennya-reglamentu-tsentralnoi-viborchoi-komisii.html.

security testing. The Lithuanian National Cyber Security Centre (NCSC) conducts regular security testing of the websites of political parties and election infrastructure systems and provides online training and education programmes for politicians and candidates. Ensuring the security of political party websites is a largely unique measure given that most of the countries included in this research do not have any such measures in place. It is important to note that the NCSC is trusted to provide such measures.

However, the fact that a state institution offers to secure political parties' websites does not mean that political parties in all countries would take advantage of the offer.

In the US, the capacities and capabilities of the government and election agencies to provide security for political parties' websites and their communication channels do exist but are not used by political actors, mainly due to a lack of trust or a wide range of non-unified jurisdictions. The US election system is a highly decentralized system with nearly 9,000 jurisdictions. Due to this decentralization, no broader preventive protection measures for elections can be applied, and they largely occur on a voluntary basis. Federal government agencies and officials are cooperating with local authorities (i.e., officials and local governments) on how to protect their infrastructure during elections. The forms of cooperation include training in basic cybersecurity principles. For example, the Cybersecurity and Infrastructure Security Agency (CISA) provides basic security training for political parties on securing parties' voting infrastructure, providing them with threat assessment briefs, as well as information on risks that can arise from malign foreign actors.

Despite the fact that the Department of Homeland Security (DHS) and CISA have sufficient knowledge and capacity to provide political parties and candidates with the assistance mentioned above, the high level of distrust between the political parties and federal authorities prevents many of them from taking advantage of such assistance.

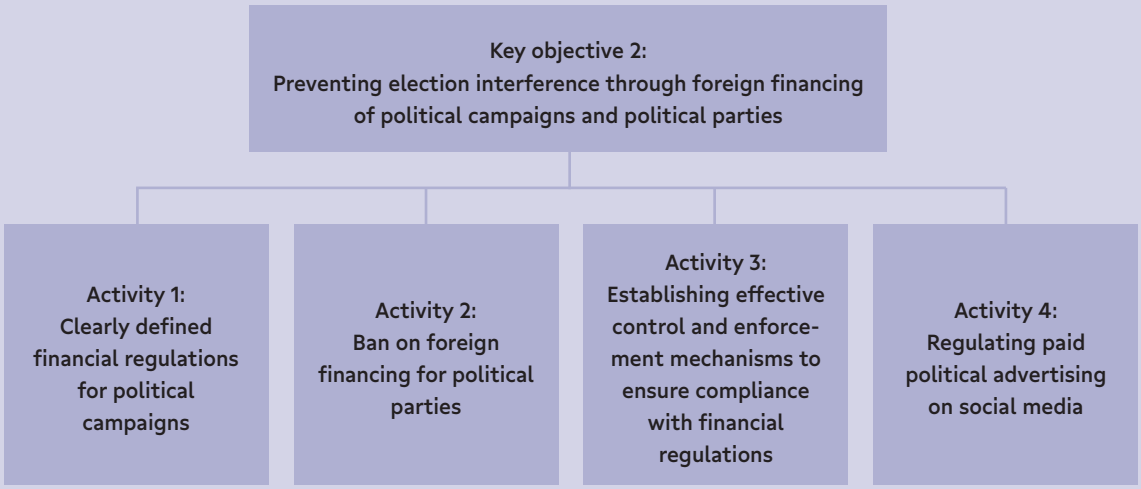
Key objective 2: Preventing election interference through foreign financing of political campaigns and political parties

Due to globalization and the rapid evolution of information technologies, the world is more interconnected than ever before. It is easier for both state and non-state actors to engage with one another. This heightened interconnectedness has also increased the risk of malign influencing.

The goals of such malign influencing may differ and depend on the intention of the influencing actor. It can begin by exerting more economic leverage within the targeted country to capture or influence the political course of society. Influencing the electoral process by financing political parties and candidates can lead to the election of politicians best suited to the interests of foreign malign actors.

The researched countries are democracies that have respect for the rule of law, which is one of the main principles of free and open societies. The rule of law implies that countries will apply measures based on adopted

Chart 2. Preventing election interference through foreign financing of political campaigns and political parties



legislation, in accordance with basic human rights, and that all individuals, institutions and entities will be held accountable with regard to laws that are publicly promulgated, equally enforced and independently adjudicated. In this section, we will focus on measures that we consider effective in preventing undue influence on elections through foreign financing of political campaigns:

- Activity 1: Clearly defined financial regulations for political campaigns
- Activity 2: Ban on foreign financing for political parties
- Activity 3: Establishing effective control and enforcement mechanisms to ensure compliance with financial regulations
- Activity 4: Regulating paid political advertising on social media

Activity 1: Clearly defined financial regulations for political campaigns

While most of the countries have set limits on spending, Lithuania has regulated the financing of political campaigns. The regulations apply to participants in the electoral process, politicians and political parties in each of the 60 municipalities, and are based on the number of voters in each municipality.

Canada has similar rules restricting the scale of financial contributions. The Canada Elections Act limits the amount of money that political candidates and parties can receive as donations from Canadian citizens.[16] For example, in 2021, the annual limit was set at 1,675 Canadian dollars. Limits were the same for candidates and registered political parties and their leaders.

Activity 2: Ban on foreign financing for political parties

The financing of political parties is regulated not only by the amount of money that one can donate, but also by who can donate. Most of the countries under study have regulations prohibiting foreign financing of political parties and candidates.

Foreign financing is also forbidden in Lithuania and Canada. In Lithuania, the purpose of this is to secure the election process and limit the influence of foreign actors. In Canada, only Canadian citizens are allowed to donate

16 'Limits on Contributions – 2022', Elections Canada, https://www.elections.ca/content.aspx?section=pol&dir=lim&document=lim2022&lang=e.

to political parties, their leaders, and candidates.[17]

Stricter rules are applied in the United States.[18] Not only are foreign nationals forbidden to make donations and contributions to political parties, but they are also prohibited from participating in the decision-making process of election-oriented activities. This law is applied at all levels of US elections – federal, state, and local. The only exceptions are Green Card holders who have a permanent residence permit.[19] These rules apply in the long term, holding parties and candidates accountable in the weeks before and after elections.

Activity 3: Establishing effective control and enforcement mechanisms to ensure compliance with financial regulations

States must have the capacity to enforce their financial regulations in the event of a breach. The United States provides an illustration of how even quite strict rules can be applied. The Federal Election Commission (FEC) "has exclusive jurisdiction over the civil enforcement of the federal campaign finance law".[20] When considering whether the election law has been breached, the FEC takes into account and analyzes audits,[21] complaints, referrals, and self-submissions. When the FEC concludes that election rules have been violated, it can fine[22] the persons responsible for the violation. In addition to foreign nationals who have contributed to political campaigns, fines can also be imposed on politicians and members of their staff who accepted donations from foreign nationals. Moreover, a wilful violation of Federal Election Law can lead the FEC to refer the violation to the Department of Justice, which may initiate criminal charges for such a violation. A referral from the FEC is not always necessary, however, as the Department of Justice can initiate prosecutions on its own initiative.

Activity 4: Regulating paid political advertising on social media

Due to the popularity and influence of social media, almost every political party and candidate have started to use social media as a platform for political and electoral campaigns. Social media also benefits those actors who wish to remain anonymous and hide foreign financing from the public and state institutions.

Several countries have reacted to this new reality by establishing rules for political campaigns, as has the EU. The European Union recently introduced new legislation that also applies to political advertising. The Digital Services Act (DSA) encompasses a wide range of advertising, including digital marketing, issue-based advertising, and political ads. It operates

17 'Political Financing, Spending, and Advertising Safeguards', Elections Canada, n.d., https://www.elections.ca/content.aspx?section=vot&dir=int%2fpol&document=index&lang=e.

18 'Foreign Nationals', Federal Election Commission, n.d., https://www.fec.gov/help-candidates-and-committees/foreign-nationals/.

19 Ibid.

20 'Enforcing federal campaign finance law', Federal Election Commission, n.d., https://www.fec.gov/legal-resources/enforcement/.

21 'Audit Reports', Federal Election Commission, n.d., https://www.fec.gov/legal-resources/enforcement/audit-reports/.

22 §111.24 Civil Penalties, Code of Federal Regulations, https://www.ecfr.gov/current/title-11/chapter-I/subchapter-A/part-111/subpart-A/section-111.24.

in conjunction with existing regulations such as the General Data Protection Regulation (GDPR), which already establishes guidelines on user consent and the right to reject targeted digital marketing.

Under the DSA, two new restrictions have been implemented for targeted advertising on online platforms. Firstly, it prohibits the targeting of minors through profiling. Secondly, it prohibits targeted advertising based on sensitive personal data categories like sexual orientation or religious beliefs. These regulations aim to empower users by enhancing their understanding of the ads they encounter and facilitating informed decision-making. Users receive transparent information about the motives behind targeted advertising, the advertiser's identity, and clear indications distinguishing sponsored content from organic platform posts.[23]

Of the countries studied, in Lithuania political parties and candidates are obliged to label their advertisements as 'political' if they are used for campaigning. Any sponsored posts on social media must also be labelled with clear information on who paid for the post.

A more detailed approach has been taken in Canada. A provision added to the Canada Elections Act in 2018 defined online platforms and required them to comply with a digital advertising registry to which all partisan and election advertising must be added. The obligation to do so is created on the day the advertisement is placed online.[24] Failure to comply with this obligation can lead to administrative fines and other penalties. The decision on penalties is made by the Commissioner of Canada Elections, which has the jurisdiction to ensure that political parties and candidates comply with election rules and legislation.[25]

Key objective 3: Building citizens' resilience to foreign influence

In order to maintain election security, states are undertaking a number of activities to improve the overall resilience of citizens to foreign interference. Making society more resilient in this respect includes reducing citizens' vulnerability to disinformation and cyberattacks, as well as increasing their ability to work effectively with information and to think critically. Hence, activities include awareness campaigns, as well as information and cyber security education and training programmes. However, such activities should take place continuously, regardless of elections, which is why this objective is included in the first period.

This key objective is divided into two basic levels according to their area of focus:

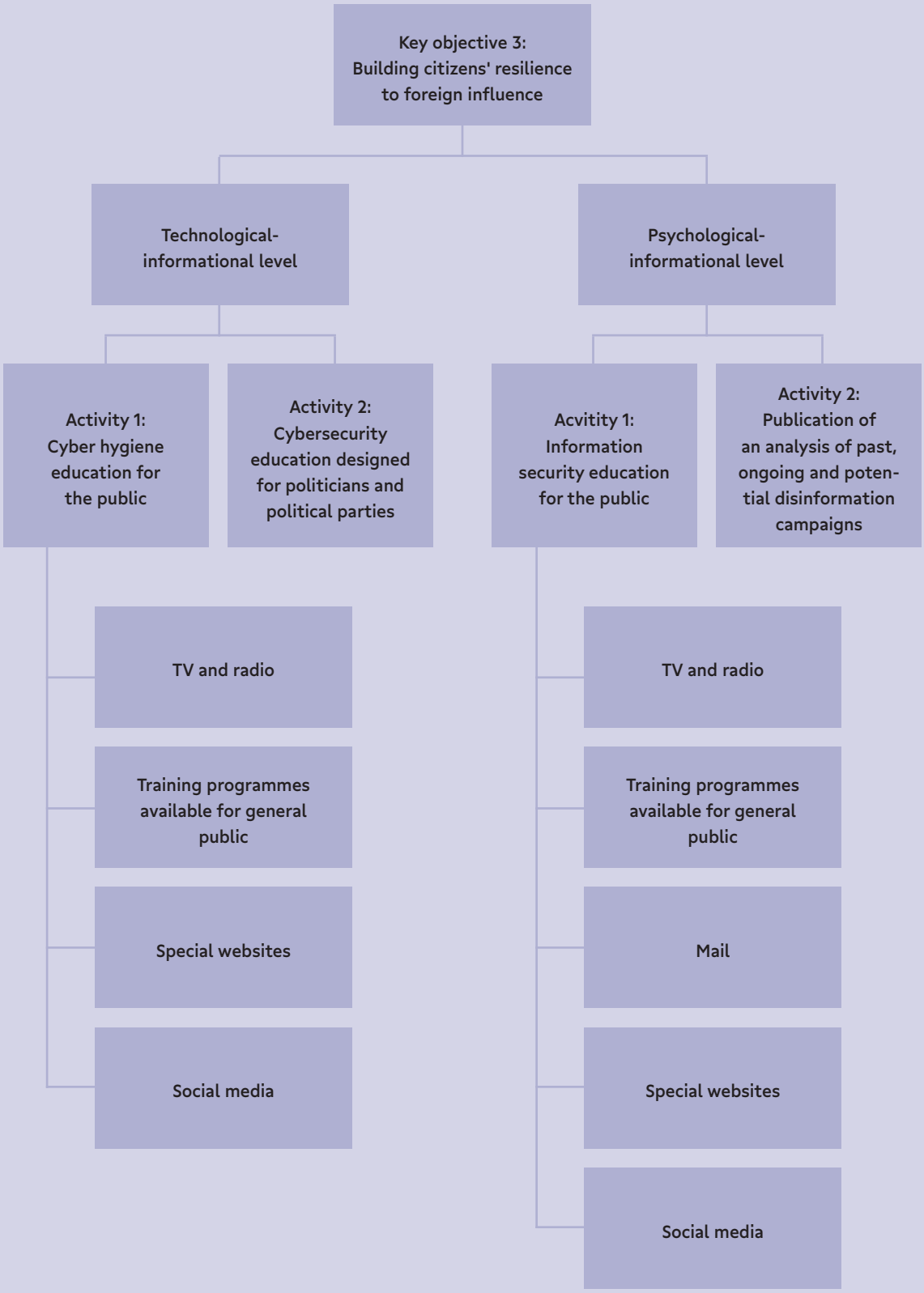
1) The technological-informational level, including activities related to cyber security.
   - Activity 1: Cyber hygiene education for the public
   - Activity 2: Cybersecurity education designed for politicians and political parties
2) The psychological-informational level, including activities related to the information security and media literacy of the population.

23 'Questions and Answers: Digital Services Act', European Commission, 25 April, 2023, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348.

24 'Registry Requirements for Political Ads on Online Platforms', Elections Canada, n.d., https://www.elections.ca/content.aspx?section=pol&dir=regifaq&document=index&lang=e.

25 Ibid.

Chart 3. Building citizens' resilience to foreign influence



- Activity 1: Information security education for the public
- Activity 2: Publication of an analysis of past, ongoing and potential disinformation campaigns

Technological-informational level

The technological-informational level includes two education-related activities that the states included in this study have carried out to make their citizens more aware of cyber threats.

Activity 1: Cyber hygiene education for the public

Educating citizens on cyber security is crucial as our daily lives become increasingly digitized. In the context of an election year, the basic cyber hygiene of citizens becomes even more relevant. Educating the general public about cyber hygiene should ensure that citizens have the necessary skills for safeguarding their cyber security both in terms of prevention (use of a VPN, antivirus software, etc.) and evaluating potentially hostile content, such as phishing attempts and fraudulent emails, SMS and phone calls. Training programmes could be organized individually, and as online webinars or information campaigns on cyber-related topics.

An example of a sophisticated cybersecurity training system is the Finnish system. The Finnish cybersecurity education model is based on the Finnish Cybersecurity Strategy of 2013,[26] which emphasizes, among other things, the education of the whole society in this area. Educational and training programmes are created according to the needs of various groups in society, such as seniors, managers of institutions, businesspeople, officials, educators, students, and others. The basic rule is that education in this field must be available to all.

The National Defence Training Association of Finland (MPK), established in 1993, is a national training organization that trains and educates citizens to be prepared for and to survive dangerous situations in everyday life and under exceptional conditions, including cyberattacks. It organizes basic courses on cyber security open to all citizens, and special training for professionals.[27] It is also a good example of cooperation with NGOs and the private sector as the Association works closely with other volunteer organizations conducting security training, educational and informational work.[28] Other NGOs are also involved, such as the Finnish Association for the Welfare of Older Adults, which is involved in cybersecurity education in Finland and has created a learning model on cyber security for senior citizens.[29]

In addition, teachers' ongoing education in Finland includes content related to information and cyber security. This effort is coordinated through the Ministry of Education and Culture, in partnership with the Finnish National Agency for Education.[30]

Some EU member states are cooperating, sharing experiences, and helping each other in

26 Finland's Cyber security Strategy, Government Resolution 24.1.2013, Secretariat of the Security Committee, https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.
27 'What is the MPK?', n.d., https://mpk.fi/en/.
28 'Finland (FI)', CYBERWISER.eu, n.d., https://www.cyberwiser.eu/finland-fi.
29 'Kyberturvallisuus on digitaalisen maailman turvallisuutta' [Cyber security is the security of the digital world], Vanhustyön keskusliitto, 11.10.2022, https://vtkl.fi/kyberturvallisuus-on-digitaalisen-maailman-turvallisuutta.
30 'Finland (FI)', CYBERWISER.eu, n.d., https://www.cyberwiser.eu/finland-fi.

implementing this activity. For example, Finland will create an educational package to make cyber security a civic skill across the European Union through a three-year project conducted by Aalto University and the Ministry of Transport and Communications.[31] In today's digital age, where people are constantly connected to the internet and more and more personal and sensitive data is stored and transmitted online, it has become crucial to maintain good cyber hygiene practices to protect people and data from cyber threats. Hence, cyber hygiene should be a basic skill for all citizens, and states are responsible for teaching it to them.

Besides educational and training activities, information campaigns also have the potential to reach citizens through various communication channels, including those who are not interested in educational programmes. An example of such a campaign is the so-called Cyber Security Awareness Month, an initiative which many countries around the world, including the US, have joined.[32] The initiative is part of the CISA's Cybersecurity Awareness Program, which is a national public awareness effort that increases the understanding of cyber threats and empowers the American public to be safer and more secure online. It encourages Americans to view internet safety as a shared responsibility at home, in the workplace, and in communities.[33] The European Union has also announced the same initiative, with individual member states joining in their own way.[34] October has been designated European Cyber Security Month (ECSM), an annual campaign aimed at promoting cyber security among individuals and organizations in the EU. The campaign provides up-to-date online security information, raises awareness by sharing good practices, and is overseen by the European Union Agency for Cybersecurity (ENISA) and the European Commission.[35]

Activity 2: Cybersecurity education designed for politicians and political parties

One of the main ways foreign powers try to influence elections is through long-term manipulation of citizens and their voting behaviour. In addition to disinformation campaigns, the "leaking" of classified or non-public information is a common method of manipulation. Foreign malign actors usually gain access to such information through hacking attacks on candidates, politicians or political parties, or public institutions at various levels.

States can respond to this threat in several ways, from long-term training programmes on securing data and the personal correspondence of politicians, political candidates and political parties to security briefings focused on cyber security around elections.

31 'Finland creates an educational package to make cybersecurity a civic skill across the European Union', Aalto University News, 8 February, 2022, https://www.aalto.fi/en/news/finland-creates-an-educational-package-to-make-cybersecurity-a-civic-skill-across-the-european.

32 'Cybersecurity Awareness Month', CISA, n.d., https://www.cisa.gov/cybersecurity-awareness-month.

33 'About the CISA Cybersecurity Awareness Program', CISA, n.d., https://www.cisa.gov/about-cisa-cybersecurity-awareness-program.

34 'European Cybersecurity Month — ENISA', ENISA, n.d., https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/european-cyber-security-month.

35 'European Cybersecurity Month — ENISA', ENISA, n.d., https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/european-cyber-security-month.

A good example of such practice is Canada. In order to protect the voting system, the Canadian Election Office (The Office of the Chief Electoral Officer, commonly known as Elections Canada)[36] cooperates with the government and its agencies, such as the Communications Security Establishment (CSE), to strengthen the cyber capacities of their election infrastructure. Safeguards are also in place to protect politicians and political parties, their data and infrastructure. As the CSE has stated, the main threats to this category are cyber espionage towards political parties, blackmailing, embarrassing or discrediting candidates, and stealing or manipulating party databases. To prevent this from happening, the CSE provides politicians and political parties with cyber advice and guidance, but also provides political parties with classified briefings on potential threats.[37]

Psychological-informational level

The psychological-informational level includes activities that entail increasing citizens' awareness of how foreign powers may influence elections through disinformation and propaganda campaigns. The two activities at this level focus on information security education, one on citizens' awareness of information security, and the other on the availability of data-based information on past, ongoing and potential disinformation campaigns.

Activity 1: Information security education for the public

Information security in this context refers to citizens' ability to identify disinformation and information influencing, to search for reliable information, and to verify information in case of doubt. In this sense, information security is closely connected with media literacy and critical thinking, pointing to citizens' ability to handle information prudently. Such an ability is necessary for preserving democracy in a time of massive disinformation and propaganda campaigns, especially during elections. However, ordinary citizens do not learn how to handle information carefully from day to day, which is why it is necessary for states to carry out these activities permanently, regardless of elections.

Specific activities that belong to this group are public education programmes, and information campaigns on television, radio, social networks and websites.

Sweden is working to build overall civil resistance to foreign interference, which requires long-term measures to also be taken outside the election year. The Swedish model assumes that electoral interference is part of a wider strategy of foreign powers, which is duly taken into account in safeguarding electoral processes. Therefore, Sweden does not limit itself to protecting the country's elections only during the election period, but also implements long-term measures immediately after elections. Such measures include awareness campaigns on various topics that could be used in disinformation campaigns, or educating citizens in media literacy. However, these activities are more intense during an election year.

At the beginning of 2022, the Swedish government established the Psychological Defence Agency (PDA), the main mission of which is

36 'Our Mission, Mandate and Values', Elections Canada, n.d., https://www.elections.ca/content.aspx?section=abo&dir=mis&document=index&lang=e.

37 'Combatting foreign interference', Government of Canada, 2020, https://www.canada.ca/en/democratic-institutions/news/2019/01/combatting-foreign-interference.html.

to lead the coordination and development of Sweden's psychological defence: "The purpose of psychological defence is to safeguard our open and democratic society, the free formation of opinion, Sweden's fundamental freedoms and ultimately our independence. The psychological defence identifies, analyses, prevents, and counters foreign malignant information influence activities and other disinformation directed at Sweden or at Swedish interests. This could include attempts from foreign actors to weaken national resilience and the population's will to defend the country, or malignant influence aimed at changing people's perceptions or influencing behaviours and the decision-making in society."[38] Hence, the PDA is part of the coordinating body for both information campaigns and educational activities regarding foreign influence on citizens.[39]

An example of the PDA's long-term work is the national information campaign called *Don't be fooled*, which was created to raise awareness about false and deceptive information, and to provide people with tools to identify and understand it. It is a combination of an informational and an educational campaign, as in addition to providing information on how foreign information influencing works, it also provides educational activities through which Swedish citizens can learn the basic tools for recognizing disinformation and disinformation campaigns.[40]

Before the PDA, the fight against disinformation was under the remit of the Swedish Civil Contingencies Agency (SCCA). This agency is still operational, but it oversees other aspects of the protection of the Swedish state and nation, which fall under the so-called total defence model that Sweden implements. In 2018, for example, the SCCA developed an information manual for Swedes on how to behave in crisis situations, forming part of the *If Crisis or War Comes* information campaign,[41] where, among other things, they focus on how to deal with information in such situations and avoid being manipulated by disinformation or fake news. In addition to the online version, the guide was printed and mailed to every Swedish household.[42]

In 2019, the SCCA became an inspiration to other countries after creating and publishing *Countering Information Influence Activities: A Handbook for Communicators*, a manual describing the principles and methods of identifying, understanding, and countering information influence activities. The SCCA collaborated with Lund University on its creation and it is aimed primarily at communicators working in public administration. The SCCA writes in the introduction that it "should be considered supporting material for situations when an organisation suspects it has been exposed to an information influence campaign or is at risk of such an attack".[43]

38 'Our mission', The Swedish Psychological Defence Agency, 28 February, 2022, https://www.mpf.se/en/mission/.
39 'Frequently asked questions', The Swedish Psychological Defence Agency, 28 February, 2022, https://www.mpf.se/en/frequently-asked-questions/.
40 'Don't be fooled', The Swedish Psychological Defence Agency, n.d., https://www.bliintelurad.se/en/about-the-campaign/.
41 'If crisis or war comes', Swedish Civil Contingencies Agency (MSB), 2022, https://rib.msb.se/filer/pdf/30307.pdf.
42 Elisabeth Braw, 'What Sweden Can Teach Us About Fighting Fake News', *Prospect Magazine*, American Enterprise Institute, 12 January, 2022, https://www.aei.org/op-eds/what-sweden-can-teach-us-about-fighting-fake-news/.
43 *Countering information influence activities: A handbook for communicators* (Swedish Civil Contingencies Agency, 2018), https://www.msb.se/ribdata/filer/pdf/28698.pdf.

Another good example of a country that has developed a strategy for educating citizens in the field of information security is Canada. The Canadian Government supports media literacy programmes for the Canadian population via the Canadian Heritage Department.[44] These include the Digital Citizen Contribution Programme, one of three components of the Digital Citizen Research Programme, which aims to provide Canadian citizens with an understanding of online disinformation campaigns and create evidence-based approaches to policymaking.[45] The Canadian Government also finances and cooperates with local civil society organizations.[46]

Activity 2: Publication of analysis of past, ongoing and potential disinformation campaigns

It is important to analyze foreign information operations in order to understand how they arise, how they work, and which topics they cover. Good analysis can also help predict which topics have the potential to be used in disinformation campaigns. This is beneficial because it gives actors more time to react before a disinformation narrative goes viral. With more time, the information space can be filled with more accurate information, and the given topic framed in a way that makes it easier for ordinary citizens to understand.

However, the public should have access to analyses of disinformation campaigns in order to understand why state and non-state actors approach the topic in the way they do. Transparency should form the cornerstone of any democracy. Within this activity, states can take two consecutive steps. First, ensuring quality research on foreign information operations within their territory, either through experts in state institutions, through external organizations on a state contract, or through cooperation with non-profit organizations or academia. Second, states may regularly publish such research, along with an interpretation of the results, and communicate this information to the public.

In the USA, this activity is the responsibility of the Global Engagement Center (GEC). The establishment of the GEC dates back to 2011 when the Center for Strategic Counterterrorism Communications (CSCC) was established within the Department of State for the purpose of "supporting agencies in Government-wide public communications activities targeted against violent extremism and terrorist organizations".[47] In 2016, the CSCC was transformed into the Global Engagement Center, but its counterterrorism mission remained largely unchanged. The GEC's mission was expanded upon enactment of the National Defense Authorization Act for Fiscal Year 2017 to include the authority to

44 'Supporting Media Literacy to Stop the Spread of Online Disinformation', Canadian Heritage, 26 October, 2020, https://www.canada.ca/en/canadian-heritage/news/2020/10/supporting-media-literacy-to-stop-the-spread-of-online-disinformation.html.

45 'Digital Citizen Research Program', Government of Canada, n.d., https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html#a1b.

46 'From Access to Engagement: Building a Digital Media Literacy Strategy for Canada', Canada's Centre for Digital and Media Literacy, n.d., https://mediasmarts.ca/research-policy/access-engagement-building-digital-media-literacy-strategy-canada.

47 John S. McCain National Defense Authorization Act for Fiscal Year 2019, Section 1284, Modifications to Global Engagement Center, P.L. 115–232, https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

address other foreign state and non-state propaganda and disinformation activities.[48]

The GEC monitors the information space and analyzes patterns in false narratives that are spread by foreign actors. The GEC duly analyzes social media posts, their metrics, target audience and narratives. These analyses are forwarded to the US Department of State, embassies, and international partners.[49] The US Department of State will then report on the GEC's findings.

Lithuania is a good example of a different model as it does not have research capacities integrated into the state structures but has established strong relationships and cooperation with non-profit research organizations. For example, the Eastern Europe Studies Centre (EESC), an independent, non-profit think tank, focuses on the analysis of international political processes and Lithuania's role in them. The EESC brings together experts from various fields, publishes analyses, organizes events, and carries out international and national projects. The Centre was founded by the Government of the Republic of Lithuania and Vilnius University.[50] Among other things, the Disinformation Research Programme also operates within the EESC.[51] In addition to the EESC, the Lithuanian state cooperates with other organizations outside the state structure, such as the Disinformation Analysis Center (DAC), which is one of the most prominent CSOs in the country providing disinformation analysis to the public.[52]

As the examples above demonstrate, this activity can be approached differently depending on the context. Large countries such as the US may directly employ researchers to focus on the analysis of information operations within the state structure, while smaller countries such as Lithuania may establish close cooperation with the non-profit sector and universities. Academics and researchers from professional non-profit organizations can produce analyses directly commissioned by the state, if so required, while remaining independent.

Key objective 4: Limiting the possibilities of foreign information influencing

One of the main tools that malign actors use to influence open democratic societies and their election process is information. This was most recently demonstrated in the 2016 US presidential election, during the campaign for the Brexit referendum, and in the interference in the 2017 French presidential election, where pro-Russian forces actively supported opponents of Emmanuel Macron. There are plenty of tools for sharing implicit propaganda (e.g., Russia-owned RT [Russia Today] and Sputnik News operating in Western societies), and for promoting both foreign and domestic disinformation narratives that have even led to violence (e.g., the US Capitol riots in January 2021).

48 The White House Office of the Press Secretary, Executive Order 13584 – Developing an Integrated Strategic Counterterrorism Communications Initiative, September 9, 2011, https://obamawhitehouse.archives.gov/the-press-office/2011/09/09/executive-order-13584-developing-integrated-strategic-counterterrorism-c.

49 'About Us – Global Engagement Center', U.S. Department of State, n.d., https://www.state.gov/about-us-global-engagement-center-2/.

50 'About us – Eastern Europe Studies Centre', EESC, n.d., https://www.eesc.lt/en/about-us/.

51 'Disinformation Research Programme', EESC, n.d., https://www.eesc.lt/en/research-programmes/disinformation-research-programme/.

52 'About', Debunk.org, n.d., https://www.debunkeu.org/about.

Since then, almost every country has adopted more detailed countermeasures to combat information influencing. This description will be similar to key objective 2 (preventing election interference through foreign financing of political campaigns and political parties), and several legislative and non-legislative measures that have been adopted will be presented here.

The legislative activities and measures are:
- Activity 1: Adoption of legislation tackling dissemination of disinformation during an election period
- Activity 2: Complete ban on disinformation communication channels

The non-legislative activities and measures are:
- Activity 1: Establishing an incident reporting mechanism
- Activity 2: Cooperation with social networks to achieve self-regulation without legislative measures

Legislative measures

Activity 1: Adoption of legislation tackling dissemination of disinformation during an election period

After the presidential election in the United States in 2016, Canada started actively adopting laws to combat disinformation and influence operation campaigns, an example of which is Bill C-76 in 2018.[53] One of its aims is to prevent malign actors from spreading disinformation during the election period.[54]

Following the interference in the 2017 French presidential election, a stricter approach was adopted in France, which caused a stir among the French public. In 2018, the French Parliament adopted a bill against manipulation of information.[55] Despite the reservations of the French Constitutional Court, the bill is in force and enforced. One of its principles is that social media companies with more than five million users are obliged to be more transparent about sponsored content.[56] The competence of independent TV media and radio regulators in

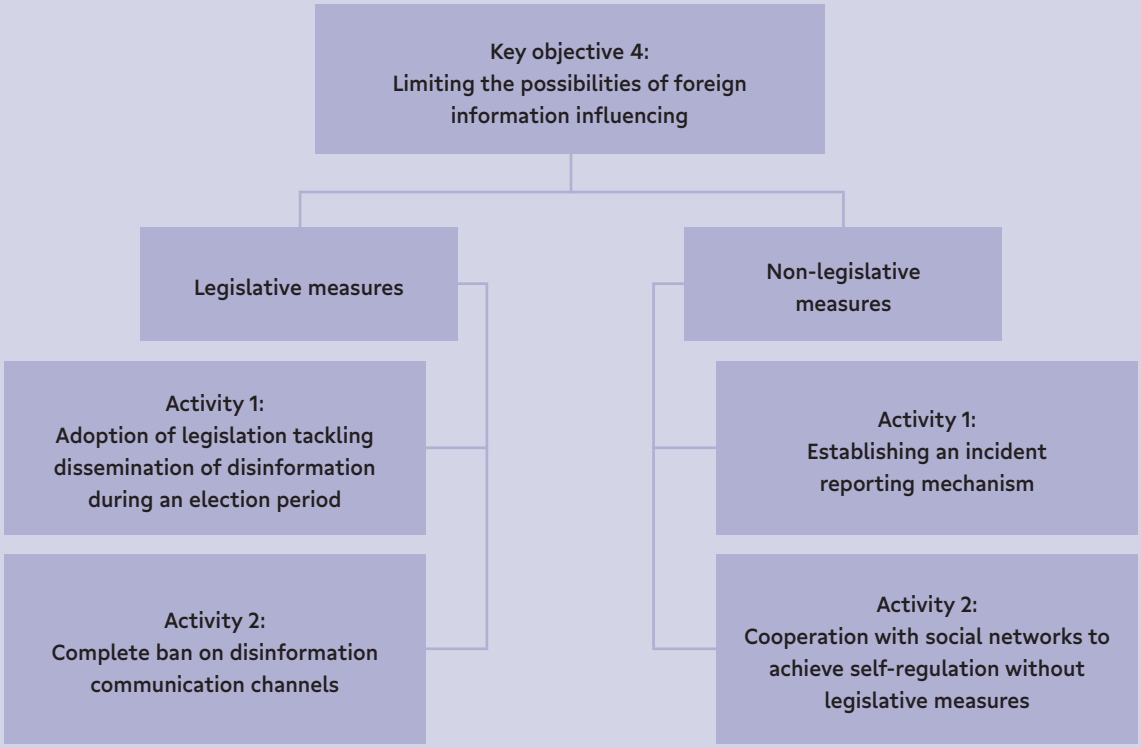
53 'An Act to amend the Canada Elections Act and other Acts and to make certain consequential amendments', 2018, Parliament of Canada, https://www.parl.ca/LegisInfo/en/bill/42-1/C-76.

54 The range of an election period depends on the election, with the minimum being 36 days and the maximum 50 days. See 'The 36-Day Election Calendar', https://www.elections.ca/content.aspx?section=vot&dir=bkg&document=ec90795&lang=e. According to provisions 91 a and b of the law, it is prohibited to make or publish a false statement to the effect that "a candidate, the leader of a political party or a public figure associated with a political party has committed an offence under an Act of Parliament or a regulation made under such an Act – or under an Act of the legislature of a province or a regulation made under such an Act – or has been charged with or is under investigation for such an offence; or to make or publish a false statement about the citizenship, place of birth, education, professional qualifications or membership in a group or association of a candidate, a prospective candidate, the leader of a political party or a public figure associated with a political party".

55 'LOI n° 2018–1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information' [Law relating to the fight against the manipulation of information], Légifrance, Republic of France, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559.

56 Marine Giullame, 'Combating the manipulation of information – a French case', Hybrid CoE Strategic Analysis, May 2019, pp. 3–5. https://www.hybridcoe.fi/wp-content/uploads/2020/07/HybridCoE_SA_16_manipulation-of-information_.pdf.

Chart 4. Limiting the possibilities of foreign information influencing



France was also strengthened. For the purposes of protecting society against malign information influence, the regulator can request a court to suspend the service.[57] Moreover, a new office, known as VIGINUM, was set up in response to the spread of disinformation and malign foreign influence. The purpose of the office is to monitor attempts by foreign actors to manipulate public opinion in the information space and in cyberspace.[58]

In August 2022, new legislation was adopted at the European level, which also deals with this issue, among other things. The so-called Digital Services Act (DSA) package modifies the rules of advertising and introduces greater transparency for users. At the same time, the user should have more freedom over which advertisements will be shown, which should ensure a wider range of options for influencing the displayed advertisement. This also affects political advertising.[59] Subsequently, in February 2023, the European Parliament adopted a report specifically on the transparency and targeting of political advertising, which should complement the DSA. The report also strengthens governance by improving cooperation between national authorities and calling for more harmonized penalties for infractions. Another piece of legislation is currently being discussed in the EU, which would make it easier for citizens to recognize political advertisements, including clearer information on why they are seeing the ad and who paid for it. New legislation also better defines and regulates different digital techniques, such as targeting, given the current lack of clarity on how advertisements are directed at users.[60]

57 Ibid.

58 'Viginum Année#1' [Viginum Year 1], Report, General Secretariat for Defence and National Security, http://www.sgdsn.gouv.fr/rapport_thematique/viginum-annee1/.

59 'European Parliament adopts report on political advertising', ALDE Party, 6 February 2023, https://www.alde-party.eu/european_parliament_adopts_report_on_political_advertising.

60 'Regulation on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC', The European Parliament, 2022, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/IMCO/DV/2022/06-15/DSA_2020_0361COD_EN.pdf.

Activity 2: Complete ban on disinformation communication channels

This uncommon measure is quite radical, and before Russia's full-scale invasion of Ukraine in February 2022, only the Baltic states had adopted it. Since then, all three Baltic states have banned several Russian- or Belarusian-related media outlets.[61] Considering their historical experience, geopolitical position and the significant Russian minorities living in all three Baltic states, this measure seems understandable.

The ban on Russian media channels RT and Sputnik now applies in all European Union countries following its decision, which was in response to the Russian invasion of Ukraine.[62] However, it should be noted that blocking communication channels must always be considered very carefully. It has been shown that blocking often has a very limited, temporary effect. Moreover, the legal basis for blocking certain communication channels could easily be exploited for political purposes.

In the Czech Republic, for example, eight disinformation websites listed by military intelligence were blocked immediately after Russia invaded Ukraine. The Czech domain provider decided to block them, but it did so upon the recommendation of the Czech government.[63] At the time, it was an extreme reaction to an extreme situation. Nevertheless, it soon became clear that such a measure only has a very limited and temporary effect. Within weeks, the blocked disinformation sites adapted to the new situation, created new domains, or switched to social media networks completely. Relatively soon, their traffic returned to pre-blocking levels.[64] On the other hand, the blocking of RT and Sputnik by the EU was somewhat successful, and the traffic on these channels is significantly lower than prior to the blocking.[65]

The question of the legality of censorship is difficult because it is closely linked to freedom of speech. There should be a legal basis for such measures, but one that is formulated in such a way that it cannot be politically abused. Such legislation should therefore contain a

61 'All Russia-Based TV Channels Banned in Latvia', Public broadcasting of Latvia, 6 June, 2022, https://eng.lsm.lv/article/features/media-literacy/all-russia-based-tv-channels-banned-in-latvia.a460236/;
'Four Russian and One Belarusian TV Channel Banned in Estonia', International Press Institute, 18 March, 2022, https://ipi.media/alerts/four-russian-and-one-belarusian-tv-channel-banned-in-estonia/; 'Lithuania Bans Russian, Belarusian TV Channels over War Incitement', Lithuanian National Radio and Television, 25 February, 2022, https://www.lrt.lt/en/news-in-english/19/1626345/lithuania-bans-russian-belarusian-tv-channels-over-war-incitement.

62 Foo Yun Chee, 'EU bans RT, Sputnik over Ukraine disinformation', Reuters, 2 March, 2022, https://www.reuters.com/world/europe/eu-bans-rt-sputnik-banned-over-ukraine-disinformation-2022-03-02/.

63 'Aeronet, Skrytá pravda i Protiproud. Sdružení CZ.NIC zablokovalo osm dezinformačních webů' [Aeronet, hidden truth and the countercurrent. The CZ.NIC Association blocked eight disinformation websites], iROZHLAS, 25 February, 2022, https://www.irozhlas.cz/zpravy-domov/dezinformace-ukrajina-rusko-spor-valka-weby-aeruoent-protiproud-prvnizpravy_2202251531_sto.

64 Josef Šlerka, 'Opatření proti konspiračním a dezinformačním webům přestávají fungovat' [Measures against conspiracy and disinformation sites stop working], Investigace, 12 May, 2022, https://www.investigace.cz/blokovani-konspiracni-weby-duben/.

65 Josef Šlerka, 'Blokování webu Sputnik News je v EU úspěšné' [Blocking of the Sputnik News website is successful in the EU], Investigace, 13 July, 2022, https://www.investigace.cz/sputnik-eu-blokovani/.

precise description of the criteria on the basis of which blocking can occur, together with a control system to prevent abuse. An example of such legislation is the EU's regulation of RT and Sputnik. Immediately after the start of Russia's full-scale invasion of Ukraine, the European Union approved another package of sanctions against Russia, including the blocking of both Russian propaganda channels. On 2 March 2022, the Council adopted EU Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilizing the situation in Ukraine. Part of this regulation is the blocking of Sputnik and RT English, RT UK, RT Spain, RT Germany, and RT France. It is important that the regulation contains a specific list of prohibited media, the blocking of which is properly justified in the text. At the same time, it is clearly stated that this is not a permanent ban, but one that will end when Russia's unprovoked and unjustified military aggression against Ukraine ends.[66]

Non-legislative measures

Activity 1: Establishing an incident reporting mechanism

Some years ago, Canada adopted the so-called Critical Election Incident Public Protocol (CEIPP), the purpose of which is to inform officials, organizations, and the public if they have been the target of an attack. At the core of the CEIPP are five senior officials, referred to as the Panel.[67] The protocol is applied during the caretaker period that usually starts several months before an election, but it can be shortened to several weeks.[68]

Activity 2: Cooperation with social media networks to achieve self-regulation without legislative measures

Sometimes, due to the strong economic power of major social media platforms, it is not always easy for states to apply legislation or the regulations necessary to reduce the space for information influencing by malign actors. In some cases, it is not easy due to constitutional constraints. One such constraint is in place in the US. As one of our interviewees from Homeland Security stated, the government cannot regulate social media companies in terms of making them delete disinformation. The government cooperates with companies on a voluntary basis and lets them apply their own rules in countering foreign influence operations.

The reason why the government cannot regulate information published online is because of the First Amendment of the US Constitution, which is very broad in also granting freedom of speech to social media companies (as a subject of law). This is also the reason why US government agencies are mainly focused on disinformation originating from abroad, as domestic actors are protected by the First Amendment.

66 'Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine', EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.065.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A065%3ATOC.

67 'Critical Election Incident Public Protocol', Government of Canada, 7 September, 2021, https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol.html.

68 Ibid.

Probably the biggest step forward in the field of cooperation with social networks is the introduction of the DSA by the European Union. The DSA applies rules for accountability, transparency, and public oversight of the impact of online platforms on the information space. It includes a regulatory framework for monitoring and ensuring accountability and transparency in response to emerging risks, and proposes rules to increase accountability in content moderation, advertising, and algorithmic processes of platforms. Major platforms are required to assess risks posed by their systems, including illegal content, products, and threats to public interests, fundamental rights, public health, and security. Accordingly, they must implement risk management tools to safeguard their services against manipulation.[69]

69 'Digital Services Act: Questions and Answers', Shaping Europe's digital future, European Commission, 24 April, 2023, https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers.

Measures to take 3 to 12 months before elections

Countries that do not implement any protective measures consistently usually start implementing the measures described above from 3 to 12 months before elections. This mainly concerns the preparation of the electoral infrastructure and system (key objective 4), a more intensive activity that follows from key objective 1 during the first period. From a cyber point of view, 3–12 months before elections, most countries focus on testing the security of their electoral infrastructure. The second level is the physical one, where the responsible authorities start working on the preparation of election ballots and ensuring their security. Key objective 5 refers to raising awareness among the public and election-specific population groups about informational threats related to the upcoming elections.

Accordingly, the period 3 to 12 months before elections includes two key objectives:

- Key objective 5: Intensifying activities to prepare and secure the voting infrastructure
- Key objective 6: Raising awareness of possible threats related to elections

Key objective 5: Intensifying activities to prepare and secure the voting infrastructure

Adding to the activities implemented under key objective 1, between 3 to 12 months before elections, some activities will be intensified, and others will begin. This key objective is divided into two levels relating to individual activities that states can undertake to make elections more secure. The first level is related to cyber security, and the second to the physical security of elections.

Cybersecurity level

At the cybersecurity level, states can undertake two activities to maximize the security of their election infrastructure: penetration testing, and intensifying protection of the voters' database.

Activity 1: Penetration testing of election system and infrastructure

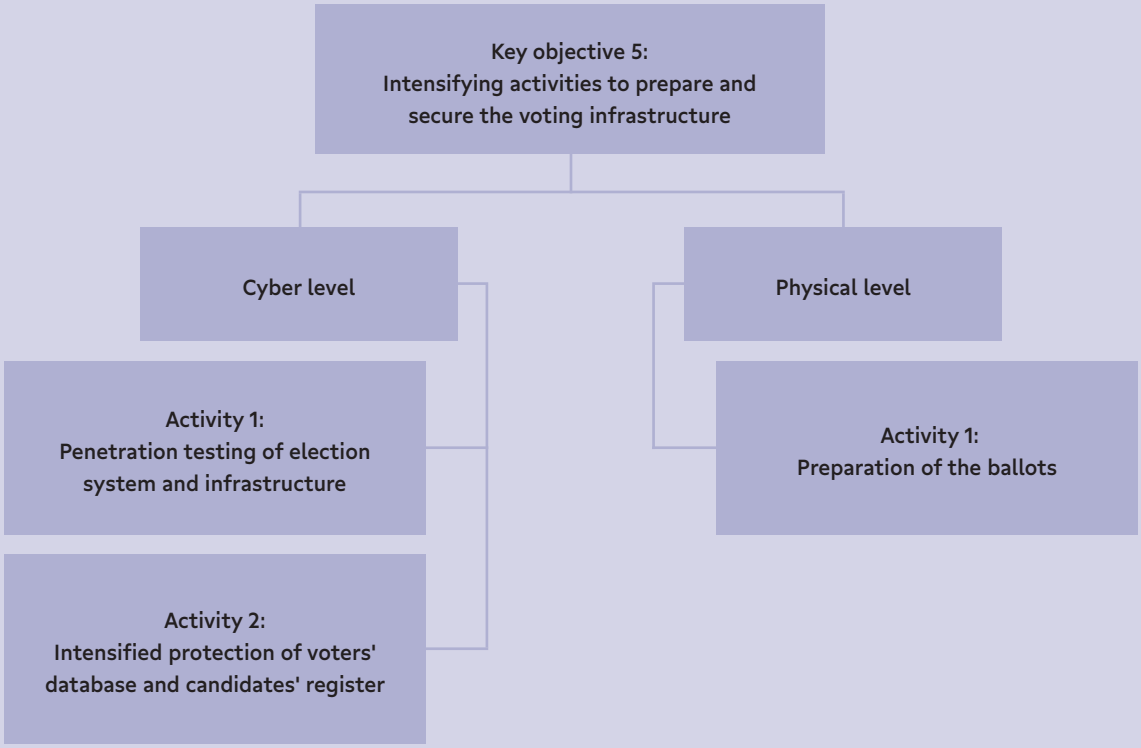
To ensure the cyber security of their electoral system and infrastructure, most countries conducted so-called penetration tests 3 to 12 months before elections. This entails the respective responsible institutions trying to attack their own systems in order to detect vulnerabilities in their cyber security, and then fixing them.

The Czech Republic is an example of a state that implements cybersecurity measures 3 to 12 months before an election, even though virtually no other security measures to protect elections are taken during the election year. The cybersecurity measures only apply to the websites on which the election results are published, and the infrastructure through which the results are delivered to these servers. This is the responsibility of the Czech Statistical Office,[70] which must comply with the conditions set by the Cybersecurity Act.[71] The testing includes a whole range of different types of penetration tests. Various private companies specialized in the issue are involved in this process. However, it is the only example of the private sector being involved in the protection of electoral processes in the Czech Republic.

70 'Competence of the CZSO in elections and a referendum', Czech Statistical Office, 2018, https://www.czso.cz/csu/czso/competence-of-the-czso-in-elections-and-a-referendum.

71 '82/2018 Sb. Vyhláška o kybernetické bezpečnosti' [Decree No. 82/2018, Cybersecurity Decree], 2018, Zákony pro lidi, https://www.zakonyprolidi.cz/cs/2018-82.

Chart 5. Intensifying activities to prepare and secure the voting infrastructure



Similarly, the Taiwanese electoral system is tested before elections under a public-private partnership with Chunghwa Telecom and its subsidiary, CHT Security. Chunghwa Telecom is Taiwan's largest telecommunications company, in which the state holds a minority stake. Cybersecurity solutions for the digital electoral system, including both hardware and software, are provided by CHT Security, a wholly owned subsidiary of Chunghwa Telecom. During the 2022 local elections, CHT Security mobilized 800 cybersecurity specialists and deployed them to the company's monitoring and command centres in the northern, central, and southern part of the island, as well as the Central Election Commission, municipal election commissions, and election operations centres.[72]

Activity 2: Intensified protection of voters' database and candidates' register

Electoral systems usually include voter and candidate registers, but the information they contain varies from country to country. They also differ in terms of who has access to the data, which can range from election committees only to all registered voters and candidates. Therefore, the level of protection is set accordingly. Countries are usually aware that digital voter databases need to be updated and cyber-protected continuously. However, the closer the election, the more intensive the work of national authorities responsible for cybersecurity during this period. For security reasons, the states included in this research do not publish specific information about how they cyber-secure their election infrastructure and election systems.

72 '(Rumour windball): Is electronic vote counting a black hole? Control the multiple anti-cheat mechanisms of elections together', Taiwan FactCheck Center, 18 November, 2022, https://tfc-taiwan.org.tw/articles/8451; '1,700 people mobilized for electronic vote counting in referendum. Central Election Commission: safe and transparent', Liberty Times Net, 2022, https://news.ltn.com.tw/news/politics/breakingnews/4096121.

Physical level

Activity 1: Preparation of the ballots
At the physical level, from 3 to 12 months before elections, the states focus on ensuring that elections are conducted safely through activities focused on ballots. With the exception of Estonia, the countries under study do not allow electronic voting. Usually, the conditions for election preparations are stated in the local election act.

A good example of a country that has a strict but transparent ballot preparation system is the United Kingdom. The UK Electoral Commission has drawn up precise guidelines on what must be on the ballot paper in order for it to be valid. The rules are as follows:

Ballot paper numbers should run consecutively, but do not have to start at '1'. Ballot paper numbers should be unique, and should not be reused; for example, the polling station, postal vote and tendered ballot papers should all be numbered differently.

The form of the reverse side of the ballot paper is prescribed and it must be ensured that the required information is included on the reverse side of the ballot paper in the specified format. There is no provision for putting any lines or other marks on the back of the ballot paper.

The unique identifying mark (UIM) can be made up of letters and numbers and could be a repeat of the ballot paper number with the addition of a prefix or suffix. The unique identifying mark can alternatively be a barcode. It is important to remember that the UIM is not the same as the official mark. The unique identifying mark:

- should be unique for each ballot paper
- can be re-used at the next poll
- must be printed on the back of the ballot paper.[73]

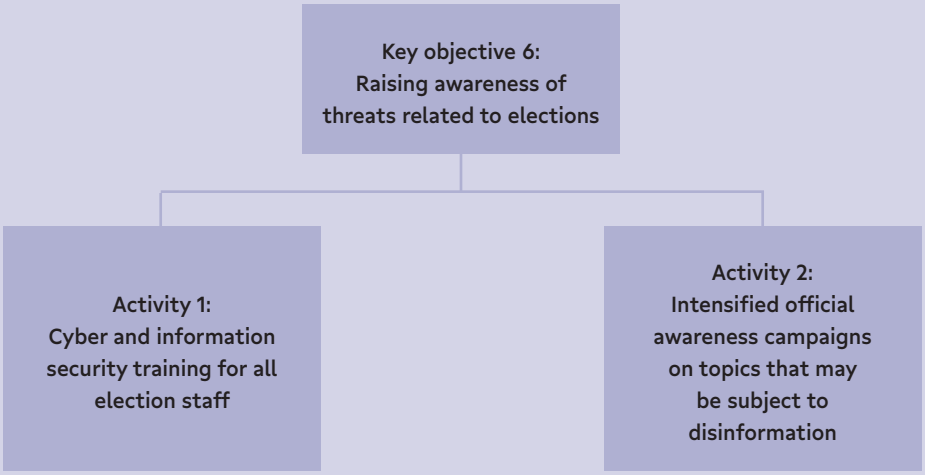
Key objective 6: Raising awareness of threats related to elections

This objective focuses on raising awareness of potential election-related threats and providing training for the public, politicians and election staff on how to prepare for and respond to them, if necessary. Training activities in the first period focus on prevention via general cyber and information security, but just before the election, activities are carried out to strengthen people's abilities to respond to specific election-related risks. Activities undertaken to achieve this objective are as follows:

- Activity 1: Cyber and information security training for all election staff
- Activity 2: Intensified official awareness campaigns on topics that may be subject to disinformation

73 'Guidance for Returning Officers administering Local Government Elections in England', The Electoral Commission, 26 January 2023, https://www.electoralcommission.org.uk/guidance-returning-officers-administering-local-government-elections-england/voter-materials/production-ballot-papers/ballot-paper-design.

Chart 6. Raising awareness of threats related to elections



Activity 1: Cyber and information security training for all election staff

The training of all election staff is essential for the safety of elections and citizens alike. It is common for states to provide manuals and training for members of regional electoral commissions. These include information on how to prepare for and conduct elections and vote counting properly, and how to ensure the physical security of ballots. It is also common for states to train members of electoral commissions in case of crisis situations, such as fires, health issues, damage to ballot papers, and so forth. It is standard for all states to ensure that, from a physical perspective, the election integrity is secured, all processes run smoothly, and responsible persons are provided with the necessary information and tools to resolve any problems that may arise.

However, a few states also train their election staff on information and cyber risks. Although research shows that foreign influencing efforts are more focused on influencing citizens rather than the electoral system, this does not mean that such a situation cannot occur. A direct attempt to manipulate the election result through a cyberattack on infrastructure right after the election may be unlikely, but it can also be said that a fire at a polling station is unlikely. Election staff should therefore be trained to deal with both physical and technological-informational crisis scenarios.

The Swedish authorities updated their information and training materials to cover information and cyber security prior to the last parliamentary election held in September 2022. The Swedish Election Authority (SEA)[74] intensifies its activities in the final month before elections. It takes systematic measures to protect activities carried out under the Elections Act[75] and other election regulations. These measures include operational and security measures as well as protection against accidents, information security, crisis preparedness, and continuity management.

The SEA launched a project in early 2020 to protect the September 2022 general election, with a focus on preventing hostile threats. The project was funded by the Swedish government's funding allocation "Appropriation 2:4

74 'The task of the Swedish Election Authority', Valmyndigheten, 30 March, 2021, https://www.val.se/servicelankar/otherlanguages/englishengelska/aboutus/theswedishelectionauthority.4.1dac782216e1e29d78918e8.html.

75 'The Elections Act (2005:837) – non-official translation from Swedish into English of Vallag (SFS 2005:837, including amendments)', Government Offices of Sweden, 17 August 2022, https://www.government.se/government-policy/democracy-and-human-rights/the-elections-act-2005837/.

Emergency Preparedness" and supported by the Swedish Civil Contingencies Agency. The SEA designed new training courses, updated materials, and developed a protection needs analysis method and a course for poll clerks.[76]

Finland also provides training on different aspects of election security for regional electoral administrative bodies, political parties, as well as regular citizens. For example, before the Finnish parliamentary election in 2019, a joint campaign was conducted between the National Cyber Security Centre, the National Security Committee, the Finnish Security and Intelligence Service, and the Prime Minister's Office in charge of coordinating the government's approach to countering disinformation.[77] This campaign focused on the major political parties, explaining the kind of cyber issues that may arise and what information influencing entails. Media seminars were also organized as part of the same campaign, explaining how influence operations work, and drawing on past examples of election-related influence operations in Finland and beyond.

Activity 2: Intensified official awareness campaigns on topics that may be subject to disinformation

Foreign information influencing often intensifies as elections approach. In addition to established training on information and cyber security, states should also have established high-quality strategic communication plans. There are two separate election-related communication campaigns that states should cover. First, an official awareness campaign focused on election practicalities (see key objective 7), and second, intensified official information campaigns on topics that have the potential to be subject to disinformation campaigns.

Strategic communication serves to ensure that information for citizens derives from a reliable source. When a country finds itself in an unpredictable situation, such as the COVID-19 pandemic, it is useful for citizens to know where to look for trustworthy information. This significantly reduces their susceptibility to misinformation, as the information space of the given state is at least partially filled with verified and factual information. This system is advantageous not only at times of deep national crisis, but also when democratic processes, such as elections, are conducted and could be targeted by foreign powers.

In Sweden, the official structure for protecting elections does not have a clear leader, as the government is composed of strong agencies and small ministries. The National Cybersecurity Centre (NCSC) provides a platform for all agencies and other bodies responsible for elections to meet and cooperate on an equal footing. It is essentially a consultation platform where individual constituents can request assistance when needed. If they do so, they can get help from other electoral authorities. On this platform, the NCSC focuses on countering cyber threats, while the Psychological Defence Agency (PDA) focuses on information security.

The NCSC, like the PDA, operates on a permanent basis, and its existence is not dependent on elections. During an election year, the above-described NCSC's platform includes

76 'Election security', Valmydigheten, 16 August, 2022, https://www.val.se/servicelankar/otherlanguages/englishengelska/aboutus/electionsecurity.4.14c1f613181ed0043d52c77.html.

77 'Cyber security and the cyber domain', Ministry for Foreign Affairs of Finland, n.d., https://um.fi/cyber-security-and-the-cyber-domain.

bodies that function exclusively during elections, such as regional electoral commissions. This means that the existing NCSC platform expands its activities during the election year, incorporating more actors directly responsible for elections. The Psychological Defence Agency, for its part, aims to demonstrate "a long-term commitment to 'strengthening the resilience within the population', including across government agencies and municipalities to identify interference by foreign states in freedom of opinion and expression".[78] According to our interviewee, the PDA can predict which topics have the potential to be subject to disinformation and cause harm. To this end, the Agency has time to prepare awareness campaigns to prevent people falling for false information, which is particularly important during election years.

For example, prior to the parliamentary election in September 2022, the PDA addressed a misleading disinformation campaign primarily targeting the Muslim minority in Sweden. The campaign was conducted on social media and other platforms, falsely claiming that Muslim children and families were systematically being subjected to abuse by the Swedish public authorities.[79] Sweden responded with an extensive awareness campaign to set the record straight, but also openly informed the public why and how the Swedish authorities were countering this disinformation campaign.[80]

78 Miranda Bryant, 'Sweden returns to cold war tactics to battle fake news', *The Guardian*, 6 February, 2022, https://www.theguardian.com/world/2022/feb/06/sweden-returns-to-cold-war-tactics-to-battle-fake-news.

79 'Disinformation campaign against Swedish public authorities regarding social services', Government Offices of Sweden, 17 February, 2022, https://www.government.se/articles/2022/02/disinformation-campaign-against-swedish-public-authorities-regarding-social-services/.

80 'Government taking strong action against disinformation and rumour-spreading campaign', Government Offices of Sweden, 6 February, 2023, https://www.government.se/press-releases/2023/02/government-taking-strong-action-against-disinformation-and-rumour-spreading-campaign/.

Measures to take less than three months before elections

Key objective 7: Informing the public about the practicalities of upcoming elections

Informing the public about the practical aspects of the election process is the most common measure adopted by the countries surveyed. These practicalities include which institution is to be elected, what the electoral system entails, if and when voters will receive their ballots, what to do if they cannot get to the polling station, and so on. Again, such measures form part of the safeguards that states put in place to protect their electoral processes. They can, for example, prevent the spread of false information about the process itself, such as claims that elections are not taking place or that voters are not entitled to participate for some reason.

Similar disinformation campaigns have been used to discourage people from voting in the Czech Republic, for example. Before the first round of the 2018 presidential election, news spread that voters for the incumbent president, Miloš Zeman, who was standing for re-election, did not have to go to the polls in the first round because Zeman would automatically proceed to the second round as the current president.[81] The impact of such campaigns can be significantly reduced if citizens are informed about election practicalities. Key objective 7 duly integrates two activities focused on preventing such disinformation campaigns from taking place:

- Activity 1: Official awareness campaign on election practicalities
- Activity 2: Intensified awareness campaign in response to possible disinformation regarding election procedures

Activity 1: Official awareness campaign on election practicalities

Germany and Poland have strict rules on how election awareness campaigns are conducted. It is considered unlikely that foreign states would want to attack the German electoral system as such, as it is relatively complex but well organized.[82] Similarly, in Poland, the Election Code of 2011 sets clear deadlines for when and how to conduct an information campaign related to exercising one's right to vote. This process begins less than a month before the election, when citizens are informed about the possibility of postal voting. The National Electoral Commission informs voters about this through the mass media.[83]

Activity 2: Intensified awareness campaign in response to potential disinformation regarding election procedures

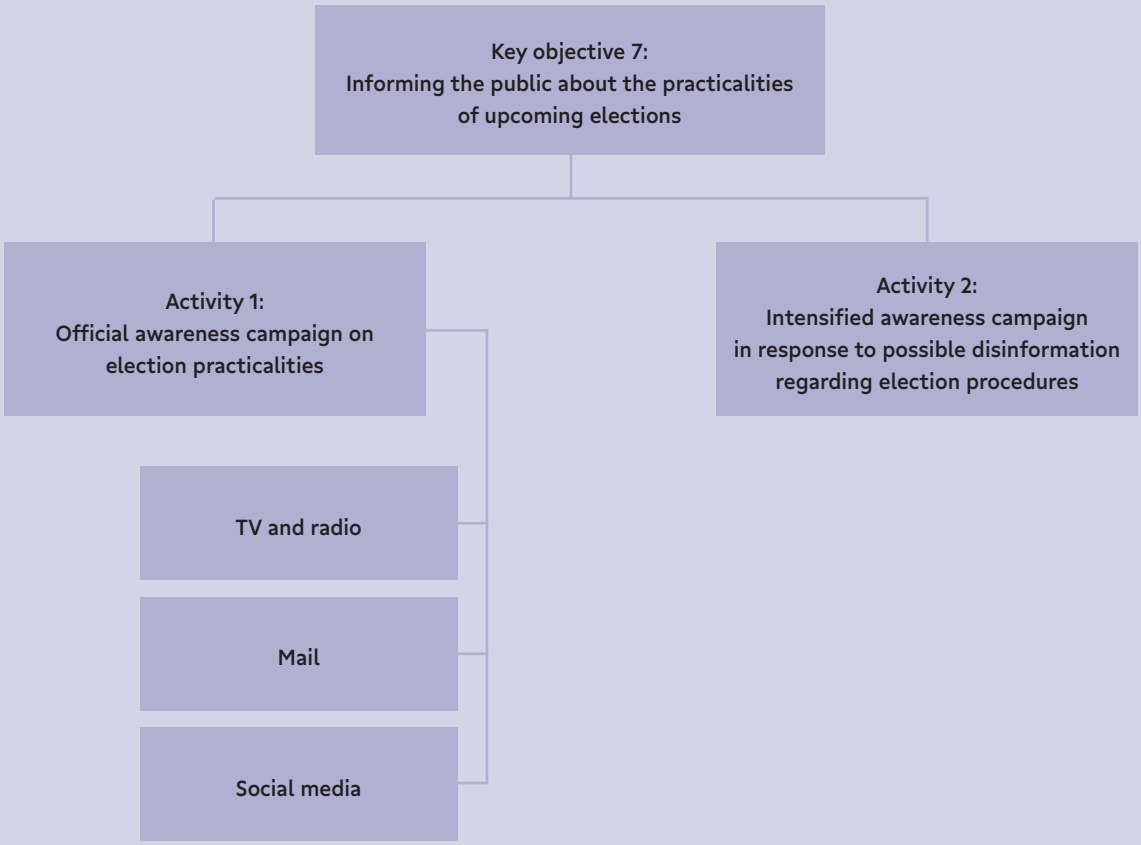
Taiwan conducts awareness campaigns before elections to inform voters about the practicalities of upcoming elections, but also in response to specific disinformation campaigns that are considered to endanger the electoral process or diminish citizens' trust in the results.

81 "Ministerstvo varuje před dezinformací. 'Zeman postupuje automaticky, k prvnímu kolu nemusíte,' navádí leták" [Ministry warns against misinformation. 'Zeman advances automatically, you don't have to go to the first round,' flyer states], 12 January, 2018, iROZHLAS, https://www.irozhlas.cz/volby/prezidentske-volby-2018-milos-zeman-hoax-dezinformace-novinka-k-prvnimu-kolu_1801121250_haf.

82 Elisabeth Heegewaldt and Elmar Ostermann, 'Rules of Procedure of the German Bundestag and Rules of Procedure of the Mediation Committee', Deutscher Bundestag, July 2022, https://www.btg-bestellservice.de/pdf/80060000.pdf.

83 'The Election of the President of the Republic of Poland', National Electoral Commission, 28 June, 2020, https://prezydent20200628.pkw.gov.pl/prezydent20200628/en/kalendarz.

Chart 7. Informing the public about the practicalities of upcoming elections



The Central Election Commission, an independent agency under the Executive Yuan (the executive branch of the Taiwanese government), is responsible for designing, implementing, and overseeing public awareness campaigns aimed at bolstering individual-level resilience towards election interference in the digital realm as well. During the 2022 local elections, there was an announced focus on debunking fake news pertaining to the alleged use of technology manipulating vote-counting software.[84] Government agencies at various levels of administration (township/district, county/city, national) frequently collaborate with private entities and NGOs to produce and disseminate audio-visual content aimed at boosting the public's understanding of cyber issues.[85] An example could be a video made by private media company Taiwan Bar, explaining the perils of digital interference in elections.[86]

84 'Central Election Commission Strongly Refutes Fake News Such As "The Elections Run on Fraudulent Procedures"', Central Election Commission, 17 November, 2022, https://clarify.cec.gov.tw/central/cms/111news/38348.

85 'Cyber Security Policies and Regulations', Administration for Cyber Security, Ministry of Digital Affairs of the Republic of China, 27 August, 2022, https://moda.gov.tw/en/ACS/operations/policies-and-regulations/648.

86 'New Animated Series: Is Foreign Election Interference a Distraction or a Real Issue? How to Hold Clean Elections?', National Security Animations, Taiwan Bar in collaboration with the Ministry of Justice Investigation Bureau of the Republic of China, 13 September, 2022, https://www.youtube.com/watch?v=bXj_YCCowq8.

Measures to take during and after elections

The period during and after an election is specific, mainly because during elections most states take some safeguarding measures, while only a few implement any protective measures afterwards. It is customary for the state authorities responsible for the safe organization of elections to be vigilant during and immediately after an election, until the moment the votes are counted. This is also the moment when most of the states included in the research stopped implementing any protective measures, duly considering the election to be over.

In this period, two key objectives were identified:

- Key objective 8: Ensuring a smooth and secure election process
- Key objective 9: Ensuring the establishment of a new government without distrust in the election results

Key objective 8: Ensuring a smooth and secure election process

This key objective includes activities focused on ensuring the physical security of the election process. The scope of these activities varies, but the vast majority have a specific institution legally responsible for them.

- Activity 1: Ensuring the physical security of the commissions and voters
- Activity 2: Ensuring secure and transparent vote counting

Activity 1: Ensuring the physical security of the commissions and voters

Ensuring basic security during elections is a standard protection measure in most countries. It is primarily a matter of ensuring the safety of electoral commission members and that of voters. States can do a lot in this regard, from proper training of election commission members to basic vetting of all voters.

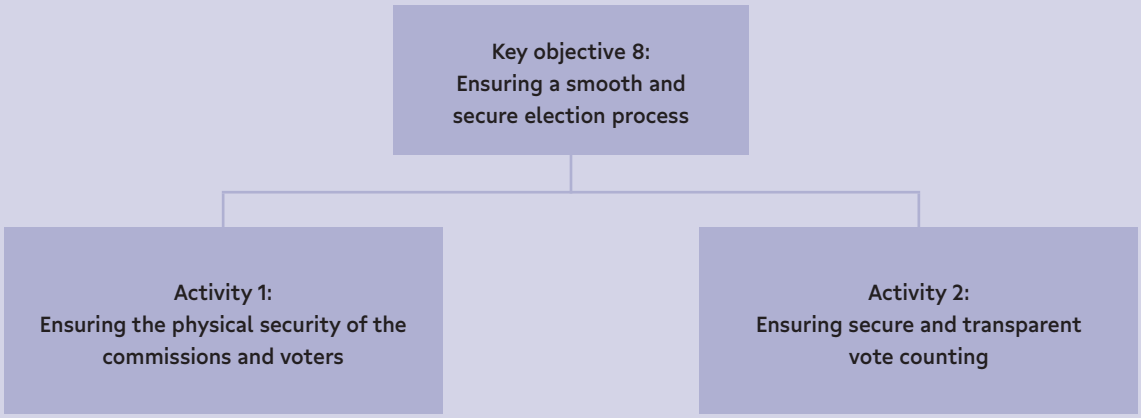
A good example is the UK, which has gradually had to adapt to new threats and electoral disruptions, such as the threat of a terrorist attack, or falsified voter or candidate lists. The electoral authority responsible for organizing elections in the UK is the Central Electoral Commission (CEC), which regularly updates instructions and training materials for election commissions, both based on the election in question and new threats identified. All election security guidelines can be found on the UK government website.[87] In 2019, for example, the CEC published an updated guide to the European Parliament elections for polling station staff, despite this being the last EP election held in the UK before Brexit.[88] Moreover, the CEC collaborates with other relevant institutions in the UK, such as the National Counter Terrorism Security Office.[89] The latest security

87 'Security guidance for elections', The Government of the United Kingdom, 8 June, 2023, https://www.gov.uk/government/publications/security-guidance-for-may-2021-elections.

88 'Handbook for polling station staff', The Electoral Commission, 2019, https://www.electoralcommission.org.uk/sites/default/files/pdf_file/EPE-Polling-station-handbook.pdf.

89 'Election Security for Polling Stations and Counting Venues', The Government of the United Kingdom, 8 June, 2023, https://www.gov.uk/government/publications/security-guidance-for-may-2021-elections/election-security-for-polling-stations-and-counting-venues-html.

Chart 8. Ensuring a smooth and secure election process



measure introduced by the UK government in 2022 is the requirement to show photo ID at the polling station.[90]

Activity 2: Ensuring secure and transparent vote counting

Most of the security measures taken by Participating States during elections are related to ensuring that they are conducted safely. This entails ensuring the security of polling stations and members of electoral commissions, and, consequently, a safe environment for the counting of votes. This includes safeguarding the transparency and cyber security of the count, as well as the cyber security of the results publishing system.

During and immediately after an election, the authorities responsible for cyber security are usually on high alert, as they must ensure a secure process for the publication of election results. For example, while cooperating with the National Office for Cyber and Information Security, the Czech Statistical Office is responsible for the security of the infrastructure used for delivering and publishing the voting results and must abide by the Czech Cyber Security Act.

Taiwan has an extensive digital infrastructure for recording, storing, and processing election data. This open governmental data is provided under the public-private partnership with Chunghwa Telecom and its subsidiary, CHT Security. As an additional protective measure, the Central Election Commission maintains 20 offsite servers to safeguard the electoral process against DDoS attack-induced paralysis and website tampering, and for cleaning network traffic.

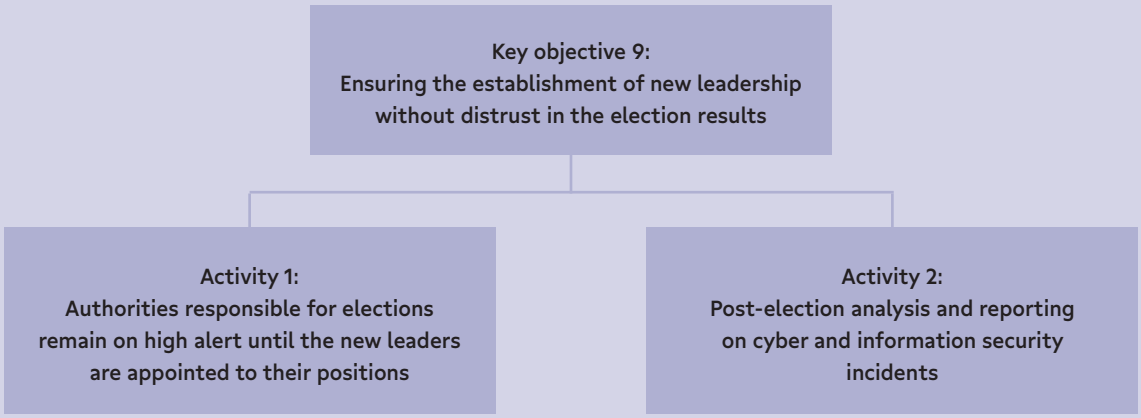
Other examples include an NGO called the Committee of Voters of Ukraine,[91] which was created in 1994, and a civil network initiative called Opora.[92] Both organizations conduct

90 'Protecting the integrity of our elections: Voter identification at polling stations and the new Voter Card', The Government of the United Kingdom, 6 January, 2022, https://www.gov.uk/government/publications/voter-identification-at-polling-stations-and-the-new-voter-card/protecting-the-integrity-of-our-elections-voter-identification-at-polling-stations-and-the-new-voter-card.

91 The Committee of Voters of Ukraine is a nationwide public organization that monitors elections and referendums, promotes electoral culture and civic education, and advocates democratic reforms in Ukraine. 'Committee of Voters of Ukraine, General Purposes', Mott Foundation, n.d., https://www.mott.org/grants/200000143-04/.

92 Opora is a civil network that conducts independent and non-partisan observation of elections in Ukraine. Opora supports the election process in Ukraine by conducting non-partisan observation of all stages of elections, from the nomination and registration of candidates to voting and the counting of results. Opora also provides parallel vote tabulation, which is independent verification of the official results based on a representative sample of polling stations. 'Products created by Civil Network Opora', Opora, n.d., https://www.oporaua.org/en/about#Section9.

Chart 9. Ensuring the establishment of new leadership without distrust in the election results



parallel vote counting or non-partisan monitoring of election processes. Despite the fact that none of the organizations has established official cooperation with the state, their role fulfils the function of a watchdog to ensure that electoral processes in Ukraine take place according to the rules.

Key objective 9: Ensuring the establishment of new leadership without distrust in the election results

Several countries implement safeguarding measures even after the vote counting has been completed and the election results announced. This is a relatively specific approach to elections, as these states do not consider an election to be over until the new leadership has been established, even if the post-election negotiations (primarily in parliamentary elections) may take up to several months. To achieve this key objective, the states conduct two activities:

- Activity 1: Authorities responsible for elections remain on high alert until the new leaders are appointed to their positions
- Activity 2: Post-election analysis and reporting on cyber and information security incidents

Activity 1: Authorities responsible for elections remain on high alert until the new leaders are appointed to their positions

This activity mainly concerns states that consider that elections are not over until the new leadership is in place. For example, the Swedish model assumes that their election protection system is fully operational when the new leaders are installed. This means that regardless of how the election turns out and how long post-election negotiations and the installation of new leaders take afterwards, the election protection system will be informed. The goal is to protect citizens' trust in the country's system and leaders. Mikael Tofvesson, Head of the Operational Department of the Psychological Defence Agency[93] interprets this as follows: "... foreign powers' goal is to threaten the state's ability to lead itself and to take initiatives. What needs to be protected is the ability to lead the state after the election. Disinformation campaigns aim to create citizens' distrust in the very result of the elections and the subsequent leadership of the state."

It is the exception rather than the rule for the countries in question to consider that foreign interference is not limited to the end of the count and the official results, although this is essential for safeguarding elections.

93 The Swedish Psychological Defence Agency, n.d., https://www.mpf.se/en/.

Activity 2: Post-election analysis and reporting on cyber and information security incidents

An immediate post-election analysis of incidents and the overall security of elections is a good way to start preparing for the next election. Learning from past mistakes and shortcomings is important for setting security rules for electoral processes.

In Canada, the Critical Election Incident Public Protocol requires public and non-public assessment reports to be created and distributed to the Prime Minister and the National Security and Intelligence Committee of Parliamentarians. Other examples include the US Election Assistance Commission (EAC),[94] and, with a similar but more legislative role, the National Conference of State Legislatures, which provides the background for so-called post-election tabulation audits, often known as a post-election audit (PEA), "to check that the equipment and procedures used to count votes during an election worked properly and that the election yielded the correct outcome".[95]

94 'About The EAC', United States Election Assistance Commission, n.d., https://www.eac.gov/about-the-useac.
95 'Post-Election Audits', National Conference of State Legislatures, 22 September, 2022, https://www.ncsl.org/elections-and-campaigns/post-election-audits.

Conclusions

In general, the most sophisticated systems for protecting elections are considered to be in the Scandinavian countries, especially the Swedish model. Sweden's strategies were more or less an inspiration for building a protection system in other countries such as the Baltic states, Canada or even the United States. One of the reasons for this is that Sweden is very open in this respect and does not hesitate to share its experiences with anyone who asks. The opposite is the case with those countries that guard their election protection systems relatively strictly. Interviews with experts in these countries were quite difficult to arrange, and some experts warned that it would be impossible to go into detail for security reasons.

An important insight concerning the Swedish model is that it has never been tested. Accordingly, we do not know whether the model is really that functional or whether it is simply that it has not yet been subjected to high stress. According to expert interviews conducted for this research, Sweden has not been a country of sufficient interest for foreign states, such as Russia or China, to attempt significant interventions into its electoral processes. This raises the question of whether Sweden's strong ability to resist foreign interference is due to the quality of its system.

Nevertheless, experts agree that the high level of public trust in the state and government is a success in itself and something of an exception in the European context.

Most of the experts interviewed agree that it is rather unlikely that foreign states would want to attack the electoral infrastructure itself. This applies in particular to states that do not allow electronic voting because there is relatively little room for a cyberattack. If such an attack were to occur, it would mainly target websites where election results are published, which in theory does not threaten the electoral process. Moreover, the security of these websites and the infrastructure through which the results are collected are usually very sound, as the relevant authorities work on securing them during the election year.

Another reason why electoral systems as such are not the target of foreign attacks is that in all the countries examined, there are several measures in place ensuring that elections are conducted safely. States are used to such measures, and it is almost impossible to manipulate the number of votes cast, for example.

However, foreign interference is considered to occur more at the level of long-term manipulation of citizens. This occurs through disinformation campaigns and the leaking of classified or non-public information. Foreign countries usually gain access to such information through hacking attacks on candidates, politicians, political parties, or state institutions at various levels. There is also a classic case of eavesdropping that happened in Poland in 2013 when various Polish politicians were secretly recorded in two restaurants where they held meetings over the course of a year. The recordings were subsequently made public, which contributed significantly to the downfall of the pro-European government in Poland.[96]

Election-related information security is a topic that only a few states have so far made a major effort to address. These are primarily

96 Vanessa Gera, 'Was Polish scandal a Russian test for US election tampering?', AP News, 4 August, 2019, https://apnews.com/article/europe-ap-top-news-elections-international-news-russia-8dd3980d7cf-44c8695767665d41f0dee.

countries that already have clear experience of foreign interference in elections, such as the US, the UK and France, or countries that are adjacent to Russia or have reason to fear its interference (the Baltic states, Finland). There are also other countries that still do little or nothing in this area, even though they have experienced foreign interference in elections or have historical reasons to fear Russian interference.

However, a positive finding is that over the last two years, more states have started to take steps to implement measures to improve information security in general, including in the period before elections. This applies, for example, to Spain's National Security Department at the Prime Minister's Office, which created a public-private partnership in 2020 to combat disinformation campaigns. Five working groups were created within this platform, with a fourth created specifically to combat disinformation campaigns before and during elections. So although it cannot be said that Spain has implemented specific measures in this area as yet, it can be said that it is approaching this goal.

Poland also approved a Cybersecurity Strategy of the Republic of Poland for 2019–2024.[97] The document sets out strategies for education in the field of cyber security for other groups of the population, such as educators, professionals, researchers, and others.[98] It can be said that in this area, Poland is trying to follow a similar path to that taken by Sweden and Finland, which have long been working to improve the resilience of the population. However, this is an unfinished process, so all the refinements have not yet been implemented. It is true, however, that the strategy does not mention cyber security in the context of electoral processes as such, but focuses on cyber security in general.

When it comes to the area of cyber security, developments in Taiwan are of interest. According to an interviewed expert, Taiwan maintains the traditional paper-based election process and purposefully avoids electronic voting because it is considered an unnecessarily large security risk. Finland, for example, has adopted the same approach. Despite this, Taiwan has focused on cyberspace, and in recent months there has been a major overhaul of the entire system, as the Ministry of Digital Affairs (MODA) was newly created in August 2022. Prior to its establishment, the management of Taiwan's cyber policy remained highly fragmented. The portfolio of the new ministry covers the fields of telecommunications, information, cybersecurity, the internet and broadcasting. Consequently, while the most recent 9-in-1 local elections were the first to be organized since the establishment of the MODA, the effectiveness of the new institution has yet to be evaluated. Enhanced cross-departmental coordination is expected to start with the presidential and parliamentary elections in 2024.

97 'Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024' [Cybersecurity Strategy of the Republic of Poland], Service of the Republic of Poland, 30 December, 2019, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019–2024.

98 'Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024' [Resolution No. 125 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024], OpenLEX, 30 October 2019, https://sip.lex.pl/akty-prawne/mp-monitor-polski/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019–18906165.

Slovenia is among those European countries that are taking the first steps in the field of cyber and information security. The Government Information Security Office (GISO)[99] is the competent national authority in this field, connecting stakeholders in the national information security system, and coordinating the operational capabilities of the system at a strategic level.[100] It pays particular attention to subjects under the Information Security Act.[101] In addition, Slovenia adopted a Cybersecurity Strategy in 2016,[102] which aims at educating Slovenian citizens about cybersecurity issues. Hence, at a general level, efforts are underway to advance the resilience of citizens in the field of cyber and information security. However, it should be noted that neither of the documents (the Cybersecurity Strategy and the Information Security Act) mention elections as something that should be specifically protected in these areas.

99 'The Information Security Administration of the Republic of Slovenia was transformed into the Government Information Security Office', The Government of the Republic of Slovenia, 2 August, 2021, https://www.gov.si/en/news/2021-08-02-the-information-security-administration-of-the-republic-of-slovenia-was-transformed-into-the-government-information-security-office/.

100 'About the Government Information Security Office', The Government of Slovenia, n.d., https://www.gov.si/en/state-authorities/government-offices/government-information-security-office/about-the-administration/.

101 'Zakon o informacijski varnosti (ZInfV)' [Information Security Act], 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?sop=2018-01-1350.

102 'Cyber Security Strategy of the Republic of Slovenia', The Government of the Republic of Slovenia, February 2016, https://www.gov.si/assets/ministrstva/MJU/DID/Cyber_Security_Strategy_Slovenia.pdf.

Recommendations

The research shows that in most countries, election interference is more often directed at voters and influencing their decisions than at attacks on electoral infrastructure to manipulate the vote count. Thus, building civil resilience against foreign interference is a key measure. The recommendations are divided into two parts: the first part comprises the top six recommendations relating to measures aimed at building citizens' resilience. The second part deals with recommendations related to legislative and systemic changes that would create a more robust system to protect electoral infrastructure and electoral processes.

Recommendations on building citizens' resilience

1. **Focus more on voters rather than on the electoral infrastructure:** Measures to protect elections from foreign interference should focus more on the voters themselves than on the electoral infrastructure, which is usually well protected already. States should focus on educating the population on cyber and information security so that they are not easily manipulated by a foreign state. That means giving citizens the tools to defend themselves and teaching them how to use those tools. Creating and strengthening the population's resistance to foreign interference is a measure that has long-term effects and is beneficial for the state even outside the election period.

2. **Ensure information and cybersecurity education for all citizens:** Activities that should be institutionalized include information campaigns focusing on how information influencing works and the kind of cyber risks that exist both during the electoral process and in everyday life. These information campaigns should be adapted to the given country, be they television and radio campaigns, social media campaigns, or traditional leaflets sent by post.

3. **Provide more advanced cybersecurity education for selected groups of citizens:** Education programmes focused on understanding cyber security should be offered to specific groups who either participate in the organization of elections (electoral commission members, officials, and unpaid volunteers), or who have a certain influence on the information environment in a given country, such as educators and journalists. These groups should be thoroughly trained in cyber security at least three months before elections.

4. **Ensure advanced and specialized cybersecurity education for candidates, politicians and political parties:** In many of the countries involved in the research, elections are influenced by the release of classified or confidential information, most often obtained through cyberattacks aimed at the email accounts of candidates and politicians or at the databases and internal communication systems of political parties. Special training programmes should be available for politicians, political parties and candidates to eliminate such risk.

5. **Allow for a more active role for civil society organizations**: Civil society organizations often have specialist knowledge, especially in the field of information security, which they are willing to share with state institutions. Civil society organizations should help the state to develop strategies for educating citizens, especially in information security, as well as specific training materials and information campaigns.

6. **Make state strategic communication proactive:** Timely strategic communication should serve as a preventive measure before, during and after elections. Its main goal is to create information campaigns for citizens to help them understand how information influencing works, and to debunk manipulative information before it goes viral and has the potential to influence voter behaviour. Proactive strategic communication should be coordinated by one centralized unit, which reduces information fragmentation and strengthens trust between citizens and the state.

Recommendations on legislative and systemic changes

1. **Make the necessary legislative changes:** Under current legislation in several countries, it is almost impossible to react to election interference by foreign actors due to the lack of precise and constitutionally conforming definitions of what an influence operation is, who should be held accountable for the deliberate dissemination of false information, and what the penalty should be in such cases (or even the complete absence of such definitions). These should be defined in the legislation.

2. **Engage in closer international cooperation at the official level to share experiences:** This would be beneficial in the cyber field in particular. It would be advantageous for members of the European Union if they were more involved in the European cooperation network on elections, which brings together representatives of member states' authorities with competence in electoral matters, and allows for concrete and practical exchanges on a range of topics relevant to ensuring free and fair elections, including data protection, cyber security, transparency and awareness raising.[103]

3. **Exclude foreign financing and donations from political campaigns:** This should be a preventive measure to eliminate (or at least minimize) the malign influence of foreign actors who seek to use elite corruption to benefit from manipulated elections. States that do not currently ban the foreign financing of political campaigns should do so immediately. Countries that already prohibit the financing of political campaigns from foreign sources should consider whether they can effectively enforce compliance with this rule. Leverage mechanisms should be reviewed and, if found to be inadequate, re-set. Accordingly, it is imperative for states to enforce compliance with the rules based on the set mechanisms, and not to allow violations to go unpunished.

103 'European cooperation network on elections', European Commission, n.d., https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/eu-citizenship/democracy-and-electoral-rights/european-cooperation-network-elections_en.

4. **Strengthen election protection capabilities:** One of the problems associated with a slow and weak government response is the lack of political will and the financial and personal resources to combat information and cyber threats.

5. **Change how social media platforms are working:** Companies like Twitter, Facebook and others should take responsibility when they have served as tools for malign foreign actors to attack democratic institutions, and ensure that they will protect the values that enabled them to prosper. Measures related to social networks have been put in place through initiatives such as the Code of Practice[104] and the Digital Services Act package[105] introduced by the European Union in recent years. There should be strict monitoring of whether technology companies are complying with these measures and, if it transpires that they are not, they should be adequately punished for it.

6. **Build a platform for all authorities that play a role in the electoral process:** There is a need for a platform in the form of a general electoral commission, within which all authorities that play a role in the electoral process can meet. This includes communication and coordination centres at the highest level, institutions tasked with the actual organization of elections, local authorities, individual ministries involved in elections and other state institutions, private companies and, if necessary, non-profit organizations, and so forth. Such a platform should exist regardless of whether an election is taking place or not, and should operate on the basis of consultation. In the event that one of the entities needs help with a specific measure, it should be able to request it here.

104 'The 2022 Code of Practice on Disinformation', The European Commission, n.d., https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

105 'The Digital Services Act package', The European Commission, n.d., https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

Annexes

Annex 1. Overview of all measures that individual states take in individual time periods

Country	Regardless of the election cycle	Three to twelve months before elections	Less than three months before elections	During and after elections
		Cyber security		
Canada	• Protection of the voter database • Providing political parties, politicians and local authorities with cybersecurity training • Providing classified briefings on threats for politicians and political parties • Participation in Rapid Response Mechanism under G7 organization	• Protection of the voter database • Providing political parties, politicians and local authorities with cybersecurity training • Providing classified briefings on threats for politicians and political parties	• Protection of the voter database • Providing political parties, politicians and local authorities with cybersecurity training • Providing classified briefings on threats for politicians and political parties • Application of Critical Election Incident Public Protocol	• Protection of the voter database • Providing political parties, politicians and local authorities with cybersecurity training • Providing classified briefings on threats for politicians and political parties • Application of Critical Election Incident Public Protocol
Czech Republic		Penetration tests conducted by Czech Statistical Office, National Cyber Security Office and private companies	Czech Statistical Office and National Cyber Security Office remain on alert	Czech Statistical Office and National Cyber Security Office remain on alert
Estonia	Protection of the voter database	Protection of the voter database	Protection of the voter database	Protection of the voter database
Finland	• Cybersecurity training for local administrative bodies and political parties • Cybersecurity training available for average citizens	• National Cyber Security Centre remains on alert • Campaign explaining the kind of cyber issues that may arise	National Cyber Security Centre remains on alert and intervenes if necessary	• National Cyber Security Centre remains on alert and intervenes if necessary • Incident reporting mechanism

Country	Regardless of the election cycle	Three to twelve months before elections	Less than three months before elections	During and after elections
France	• Protection of the voter database • Participation in Rapid Response Mechanism under G7 organization	Protection of the voter database (overseas voters)	Protection of the voter database (overseas voters)	Protection of the voter database (overseas voters)
Germany	Participation in Rapid Response Mechanism under G7 organization	Federal Office for Information Security remains on alert	Federal Office for Information Security remains on alert	Federal Office for Information Security remains on alert
Latvia	• Cybersecurity training for the public and political parties by CERT • Prevention of the abuse of advertising in the information environment by KNAB	• Cybersecurity training for the public and political parties by CERT • Prevention of the abuse of advertising in the information environment by KNAB	• Cybersecurity training for the public and political parties by CERT • Prevention of the abuse of advertising in the information environment by KNAB	• Cybersecurity training for the public and political parties by CERT • Prevention of the abuse of advertising in the information environment by KNAB
Lithuania	• Monitoring of cyberspace, management of cybersecurity incidents, implementation of security requirements by NSCS • Providing training on cybersecurity for institutions and society by NSCS	• Monitoring of cyberspace, management of cybersecurity incidents, implementation of security requirements by NSCS • Providing training on cybersecurity for institutions and society by NSCS	• Monitoring of cyberspace, management of cybersecurity incidents, implementation of security requirements by NSCS • Providing training on cybersecurity for institutions and society by NSCS	• Monitoring of cyberspace, management of cybersecurity incidents, implementation of security requirements by NSCS • Providing training on cybersecurity for institutions and society by NSCS
Poland	Protection of the voter database	Government Centre for Security remains on alert	Government Centre for Security remains on alert	Government Centre for Security remains on alert
Slovenia	Cybersecurity information campaign for the general public (not connected specifically to elections) conducted by Centre for Safer Internet			

Country	Regardless of the election cycle	Three to twelve months before elections	Less than three months before elections	During and after elections
Spain	Cybersecurity information campaign for the general public (not connected specifically to elections) conducted by the Spanish National Cybersecurity Institute			
Sweden	• Cybersecurity training for local administrative bodies (NCSC) • Cybersecurity training available for average citizens (NCSC)	• Cybersecurity training for local administrative bodies (NCSC) • Cybersecurity training available for average citizens (NCSC) • Campaign explaining the kind of cyber issues that may arise	• NCSC remains on alert • Cybersecurity training for local administrative bodies (NCSC) • Cybersecurity training available for average citizens (NCSC) • Campaign explaining the kind of cyber issues that may arise	• Incident reporting mechanism • NCSC remains on alert
Taiwan	The Central Election Commission is responsible for designing, implementing, and overseeing public campaigns aimed at bolstering individual-level resilience towards election interference, including the cyber area	Testing the system's security via public-private partnership with Chunghwa Telecom and its subsidiary, CHT Security		Central Election Commission maintains 20 off-site servers to guard the electoral process against the negative impact of DDoS attack-induced paralysis, website tampering, and for cleaning network traffic
UK	Participation in Rapid Response Mechanism under G7 organization	Cooperation between several governmental agencies, National Crime Agency, and the police	Cooperation between several governmental agencies, National Crime Agency, and the police	Cooperation between several governmental agencies, National Crime Agency, and the police
Ukraine	Protection of the voter database	Protection of the voter database	Protection of the voter database	Protection of the voter database

Country	Regardless of the election cycle	Three to twelve months before elections	Less than three months before elections	During and after elections
USA	• Protection of the voter database • Participation in Rapid Response Mechanism under G7 organization	• Protection of the voter database • Participation in Rapid Response Mechanism under G7 organization	Protection of the voter database	• Protection of the voter database • Protection of election infra-structure during voting and during the counting process • Evaluation of the threats (report writing)
Information security				
Canada	Participation in Rapid Response Mechanism under G7 organization		• Application of Critical Election Incident Public Protocol • Prohibition of making and publishing false information about parties and candidates	• Application of Critical Election Incident Public Protocol • Prohibition of making and publishing false information about parties and candidates
Czech Republic		The Centre Against Hybrid Threats is alerted and ready to react, but only to disinformation that can threaten the electoral process itself	The Centre Against Hybrid Threats is on alert and ready to react but only to disinformation that can threaten the electoral process itself	
Estonia	• Providing political parties, politicians and local authorities with cybersecurity training • Transparent and regular strategic communication towards society • Governmental analysis and estimations of threats	• Providing political parties, politicians and local authorities with cybersecurity training • Transparent and regular strategic communication towards society • Governmental analysis and estimations of threats	• Providing political parties, politicians and local authorities with cybersecurity training • Transparent and regular strategic communication towards society - Governmental analysis and estimations of threats	• Providing political parties, politicians and local authorities with cybersecurity training • Transparent and regular strategic communication towards society • Governmental analysis and estimations of threats

Country	Regardless of the election cycle	Three to twelve months before elections	Less than three months before elections	During and after elections
Finland	• Information security training for local administrative bodies and political parties • Information security training available for average citizens	• Working group on election protection and preparedness remains on alert • National campaign to explain what information influencing is	• Working group on election protection and preparedness remains on alert • National campaign to explain what information influencing is • Information campaign focused on informing citizens about aspects related to the exercise of the right to vote	Working group on election protection and preparedness remains on alert
France	• Information and cybersecurity guide for political parties and candidates by ANSSI • Participation in Rapid Response Mechanism under G7 organization	• Information and cybersecurity guide for political parties and candidates by ANSSI • VIGINUM office monitoring information and cyberspace	• Independent media regulator analyzing the information space • VIGINUM office monitoring information and cyberspace	• Independent media regulator analyzing information space • VIGINUM office monitoring information and cyberspace
Germany	Participation in Rapid Response Mechanism under G7 organization		Information campaign focused on informing citizens about aspects related to the exercise of the right to vote	
Latvia	• Information sharing between members of DEG on threats in information space (on a regular basis) • Education of civil society on topics relating to information security by DEG	• Information sharing between members of DEG on threats in information space (on a regular basis) • Education of civil society on topics relating to information security by DEG	• Information sharing between members of DEG on threats in information space (on a regular basis) • Education of civil society on topics relating to information security by DEG	• Information sharing between members of DEG on threats in information space (on a regular basis) • Education of civil society on topics relating to information security by DEG

Country	Regardless of the election cycle	Three to twelve months before elections	Less than three months before elections	During and after elections
Lithuania	Education of civil society on topics relating to information security	Education of civil society on topics relating to information security	Education of civil society on topics relating to information security	Education of civil society on topics relating to information security
Poland		National Election Office handles training for election commissioners	Information campaign focused on informing citizens about aspects related to the exercise of the right to vote	
Slovenia			Information campaign focused on informing citizens about aspects related to the exercise of the right to vote	
Spain			Information campaign focused on informing citizens about aspects related to the exercise of the right to vote	
Sweden	• Long-term education programmes focused on information influencing for the general public as well as specific groups • Information security training for local administrative bodies and political parties • NCSC remains on alert	• Information campaign focused on information influencing for the general public • NCSC remains on alert	• Information campaign focused on informing citizens about aspects related to the exercise of the right to vote • NCSC remains on alert	NCSC remains on alert

Country	Regardless of the election cycle	Three to twelve months before elections	Less than three months before elections	During and after elections
Taiwan	The Central Election Commission is responsible for designing, implementing, and overseeing public campaigns aimed at bolstering individual-level resilience towards election interference, including information influencing	The Central Election Commission is responsible for designing, implementing, and overseeing public campaigns aimed at bolstering individual-level resilience towards election interference, including information influencing	• Information campaign focused on informing citizens about aspects related to the exercise of the right to vote • The Central Election Commission is responsible for designing, implementing, and overseeing public campaigns aimed at bolstering individual-level resilience towards election interference, including information influencing	
UK	• Strategic communication by the GCS • Participation in Rapid Response Mechanism under G7 organization	Strategic communication by the GCS	• Strategic communication by the GCS • Information campaign focused on informing citizens about aspects related to the exercise the right to vote	Strategic communication by the GCS
Ukraine	Regular strategic communication from the government and its branches	Regular strategic communication from the government and its branches	Regular strategic communication from the government and its branches	Regular strategic communication from the government and its branches

Country	Regardless of the election cycle	Three to twelve months before elections	Less than three months before elections	During and after elections
USA	• Participation in Rapid Response Mechanism under G7 organization • Regular messaging from the Department of Homeland Security • Global Engagement Team provides DHS with analyses on malign foreign narratives	• Regular messaging from the Department of Homeland Security • Global Engagement Team provides DHS with analyses on malign foreign narratives	• Regular messaging from the Department of Homeland Security • Global Engagement Team provides DHS with analyses on malign foreign narratives	• Regular messaging from the Department of Homeland Security • Global Engagement Team provides DHS with analyses on malign foreign narratives • Assessment of threats during campaign and election day • Messaging during vote counting
Cooperation with private sector				
Canada	• Compliance of big tech companies with promoting healthy and resilient democracy • Database of political advertisements	• Compliance of big tech companies on promoting healthy and resilient democracy • Database of the political advertisement	• Compliance of big tech companies on promoting healthy and resilient democracy • Database of the political advertisement	• Compliance of big tech companies on promoting healthy and resilient democracy • Database of the political advertisement
Czech Republic		Czech Statistical Office and the National Office for Cyber and Information Security cooperate with various private IT companies (not specified) when testing the system before elections	Czech Statistical Office and the National Office for Cyber and Information Security cooperate with various private IT companies (not specified) when testing the system before elections	
Estonia	Cooperation with private companies to secure safety of digital services			
Finland				
France				

Country	Regardless of the election cycle	Three to twelve months before elections	Less than three months before elections	During and after elections
Germany	US technology company Microsoft advises German political parties on how to protect their election campaigns against cyberattacks			
Latvia	Providing cooperation with education on cyber security			
Lithuania				
Poland	Public-private collaboration in cybersecurity area (although cooperation on cybersecurity of elections is not explicitly stated in any public document)			
Slovenia	Centre for Safer Internet is supported by the government and acts as a platform for private companies, NGOs as well as public institutions to create cyber and information security campaigns for regular citizens			
Spain	Public-private collaboration between five working groups to combat disinformation – the fourth group is focused specifically on information security during elections (includes private companies as well as civil society representatives)	Public-private collaboration of five working groups to fight disinformation – forth group is focused specifically on information security during elections (includes private companies as well as civil society representatives)	Public-private collaboration of five working groups to fight disinformation – forth group is focused specifically on information security during elections (includes private companies as well as civil society representatives)	Public-private collaboration of five working groups to fight disinformation – forth group is focused specifically on information security during elections (includes private companies as well as civil society representatives)
Sweden				

Country	Regardless of the election cycle	Three to twelve months before elections	Less than three months before elections	During and after elections
Taiwan	• Public-private partnership with Chunghwa Telecom and its subsidiary, CHT Security • Cooperation between government agencies at various levels of administration and private entities (for example Taiwan Bar) to produce and disseminate audio-visual content aiming to bolster the understanding of cyber issues among the general public	• Public-private partnership with Chunghwa Telecom and its subsidiary, CHT Security • Cooperation between government agencies at various levels of administration and private entities (for example Taiwan Bar) and/or NGOs to produce and disseminate audio-visual content aiming to bolster the understanding of cyber issues among the general public	• Public-private partnership with Chunghwa Telecom and its subsidiary, CHT Security • Cooperation between government agencies at various levels of administration and private entities (for example Taiwan Bar) and/or NGOs to produce and disseminate audio-visual content aiming to bolster the understanding of cyber issues among the general public	• Public-private partnership with Chunghwa Telecom and its subsidiary, CHT Security • Cooperation between government agencies at various levels of administration and private entities (for example Taiwan Bar) and/or NGOs to produce and disseminate audio-visual content aiming to bolster the understanding of cyber issues among the general public
UK				
Ukraine				
USA	Negotiations with social media companies to regulate foreign influence operations by malign actors (free speech)			
Cooperation with NGO sector				
Canada	Engagement of civil society under G7 Rapid Response Mechanism			
Czech Republic				
Estonia	CSOs providing government and its agencies with expertise and advocacy policy	CSOs providing government and its agencies with expertise and advocacy policy	CSOs providing government and its agencies with expertise and advocacy policy	

Country	Regardless of the election cycle	Three to twelve months before elections	Less than three months before elections	During and after elections
Finland				
France	Engagement of civil society under G7 Rapid Response Mechanism			
Germany	Engagement of civil society under G7 Rapid Response Mechanism			
Latvia	• Watchdog and advocacy activities by CSOs (on party financing, election system reforms, disinformation campaigns by malign actors) • CSO projects on promoting media literacy of Latvian society, and resilient society	• Watchdog and advocacy activities by CSOs (on party financing, election system reforms, disinformation campaigns by malign actors) • CSO projects on promoting media literacy of Latvian society	• Watchdog and advocacy activities by CSOs (on party financing, election system reforms, disinformation campaigns by malign actors) • CSO projects on promoting media literacy of Latvian society	• Watchdog and advocacy activities by CSOs (on party financing, election system reforms, disinformation campaigns by malign actors) • CSO projects on promoting media literacy of Latvian society
Lithuania	CSOs and cooperating individuals contribute to combat influence operations (i.e., disinformation campaigns)	CSOs and cooperating individuals contribute to combat influence operations (i.e., disinformation campaigns)		
Poland				
Slovenia	Centre for Safer Internet is supported by the government and acts as a platform for private companies, NGOs as well as public institutions to create cyber and information security campaigns for regular citizens			

Country	Regardless of the election cycle	Three to twelve months before elections	Less than three months before elections	During and after elections
Spain	Public-private collaboration between five working groups to combat disinformation – the fourth group is focused specifically on information security during elections (includes private companies as well as civil society representatives)	Public-private collaboration between five working groups to combat disinformation – the fourth group is focused specifically on information security during elections (includes private companies as well as civil society representatives)	Public-private collaboration between five working groups to combat disinformation – the fourth group is focused specifically on information security during elections (includes private companies as well as civil society representatives)	Public-private collaboration between five working groups to combat disinformation – the fourth group is focused specifically on information security during elections (includes private companies as well as civil society representatives)
Sweden				
Taiwan	Cooperation between government agencies at various levels of administration and NGOs (not specified) to produce and disseminate audio-visual content aiming to bolster the understanding of cyber issues among the general public	Cooperation between government agencies at various levels of administration and NGOs (not specified) to produce and disseminate audio-visual content aiming to bolster the understanding of cyber issues among the general public	Cooperation between government agencies at various levels of administration and NGOs (not specified) to produce and disseminate audio-visual content aiming to bolster the understanding of cyber issues among the general public	Cooperation between government agencies at various levels of administration and NGOs (not specified) to produce and disseminate audio-visual content aiming to bolster the understanding of cyber issues among the general public
UK	• Engagement of civil society under G7 Rapid Response Mechanism • CSOs providing government and its agencies with expertise and advocacy policy	CSOs provide government and its agencies with expertise and advocacy policy		

Country	Regardless of the election cycle	Three to twelve months before elections	Less than three months before elections	During and after elections
Ukraine	Active role of CSOs and media in countering foreign disinformation (i.e., Opora Movement, Stop-fake initiative)	• Active role of CSOs and media in countering foreign disinformation (i.e., Opora Movement, Stop-fake initiative) • Active role of CSOs (namely Chestno initiative) in overseeing fair campaign funding	• Active role of CSOs and media in countering foreign disinformation (i.e., Opora Movement, Stop-fake initiative) • Active role of CSOs (namely Chestno initiative) in overseeing fair campaign funding	• Participation of non-partisan CSOs in overseeing smooth and fair election process (i.e., vote counting) • Active role of CSOs and media in countering foreign dis-information (i.e., Opora Movement, Stop-fake initiative) • Active role of CSOs (namely Chestno initiative) in overseeing fair campaign funding
USA	• CSOs, professional non-partisan organizations supporting state officials by providing briefs and guidance on election security (disinformation, cybersecurity) • Engagement of society under G7 Rapid Response Mechanism	CSOs, professional non-partisan organizations supporting state officials by providing briefs and guidance on election security (disinformation, cybersecurity)	CSOs, professional non-partisan organizations supporting state officials by providing briefs and guidance on election security (disinformation, cybersecurity)	CSOs, professional non-partisan organizations supporting state officials by providing briefs and guidance on election security (disinformation, cybersecurity)

Authors

Andrej Poleščuk holds a master's degree from the Faculty of Law at Palacký University Olomouc. As an analyst, he has been focusing on Eastern Europe, especially Belarus and Ukraine after the Revolution of Dignity in 2014. During his studies, he focused on the European Union and its Common Foreign and Security Policy.

Veronika Krátka Špalková studied International Relations and European Studies at Palacký University Olomouc, where she currently works as an internal doctoral student researching propaganda and disinformation. She teaches at CET Academic Programs in Prague.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats