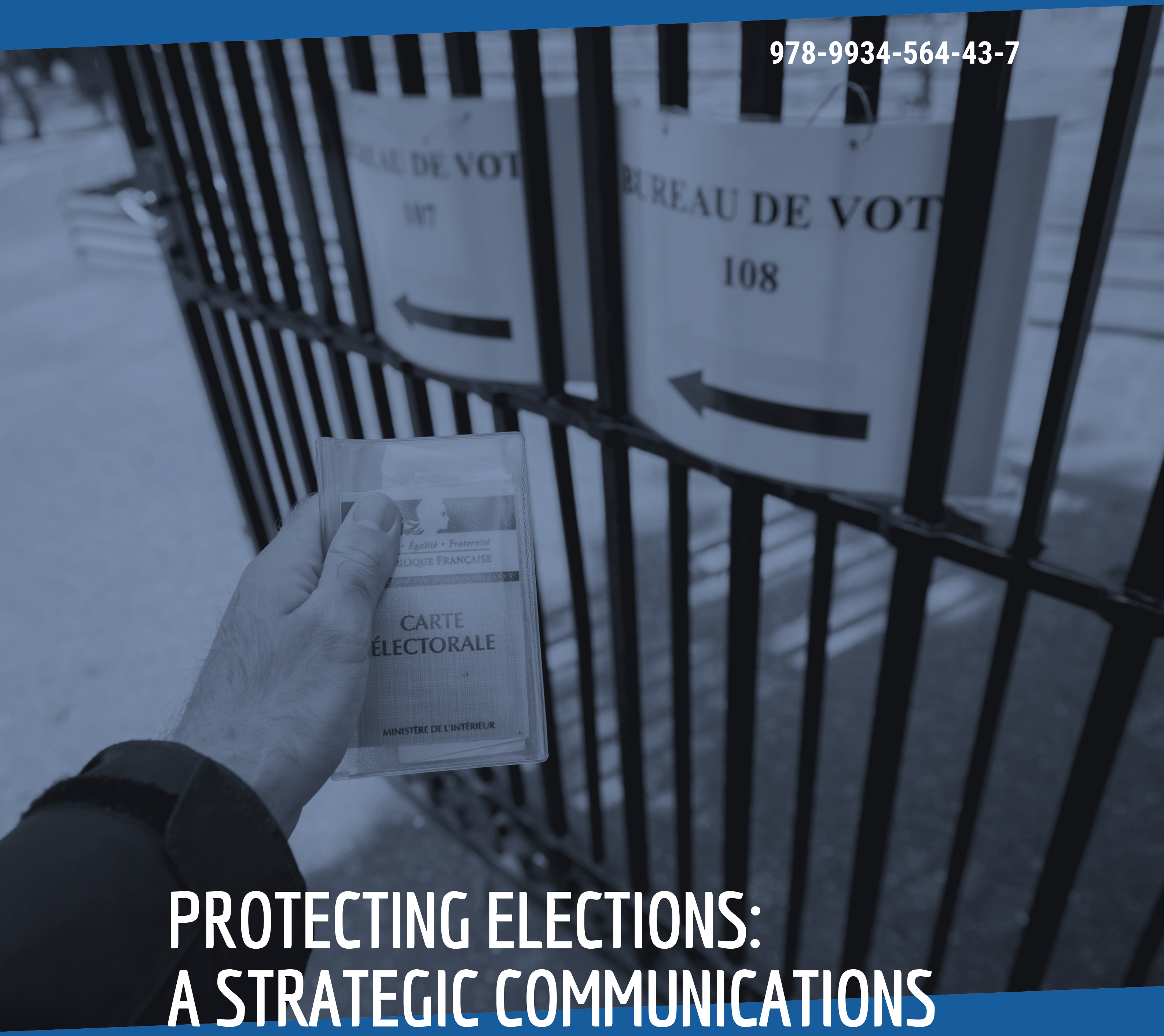


978-9934-564-43-7

PROTECTING ELECTIONS: A STRATEGIC COMMUNICATIONS APPROACH

Published by the
NATO Strategic Communications
Centre of Excellence

ISBN: 978-9934-564-43-7
Authors: Sebastian Bay, Guna Šnore
Project manager: Guna Šnore
Copy editor: Dario Cavegn
Design: Kārlis Ulmanis

Riga, June 2019
NATO STRATCOM COE
11b Kalciema Iela
Riga LV1048, Latvia
www.stratcomcoe.org
Facebook/stratcomcoe
Twitter: @stratcomcoe

This publication does not represent the opinions or policies of NATO.

”The incredibly complex and dynamic information environment of today has created unprecedented ways of influencing voters’ choices and the results of elections.

Introduction

By participating in free and fair elections, citizens make their choice while they expect the officials they elect to represent their best interests in the best possible way. The voters’ choice gives legitimacy to the officials and parties needed to handle legislation and execute political powers in the way they find most appropriate and suitable.

While the competition for political power is an essential element in ensuring the democratic diversity of interests, the election process itself can become exposed to malicious influence attempts, including foreign powers aiming to influence the choice of voters as well as the outcome of an election.

The incredibly complex and dynamic information environment of today has created unprecedented ways of influencing voters’ choices and the results of elections. This requires national administrations and relevant institutions to assess the potential risks and challenges facing democratic processes in a holistic way, and to consider the most suitable approach to ensure the relevant resilience levels.

Since 2017, several countries have scrambled to secure their general elections in the wake of the revelations of foreign interference in elections in the United States as well as France. Much of the work was unprecedented, and there was little guidance to direct the efforts. Yet securing free and fair elections is a fundamental pillar of a functioning democracy. In the same spirit, this paper is a compilation and assessment of the lessons identified by a few of the professionals who led efforts undertaken in Sweden, Latvia, Estonia and Finland. In it, we combine the systems we built with the lessons we identified, to create a roadmap for all those working on ensuring free and fair elections in democratic countries and their institutions in the future.

This paper specifically focuses on the advantages of applying a strategic communications mind-set to dealing with these challenges. While election infrastructure, expectations of internal and external audiences, and the specifics of the security challenges at hand all differ across countries, our analysis suggests that acknowledging the existence of the issue, along with the steadfast determination of the authorities involved to ensure free and fair elections, makes it possible to roll out a comprehensive election protection program based on that same strategic communications mindset.

This paper also provides an overview of the strategic communications challenge concerning elections in democratic countries. It includes an election security analysis framework to be applied in the preparation of institutions, and it provides insight into the best practises that have ensured the conduct of free and fair elections in our four countries.

What is strategic communications, or StratCom?

Over the last couple of decades, governments and international organisations around the world have learned to appreciate that their ability to execute their policies and to reach their goals, among other things, depends on the dynamics in the cognitive and physical societal spaces in which they operate. The myriad aspects influencing human perception, and through them also behavioural decisions, have led to endless studies about what it is that can influence the views of different audiences, and how.

For the purpose of this study, we approach strategic communications (StratCom) as a holistic view on national strategy, and strategic goals achieved through means and efforts with verifiable communicative value. This mindset is applicable not only at the national, but also at the international level.

The awareness and recognition of the value of verbal and non-verbal communication as well as understanding communication through policies, actions and abstention allows governments to be strategic and efficient in achieving their national goals. This, however, requires the presence of the following elements:

- **Awareness of the processes and dynamics in the information environment, including**:
  The ability to segment and differentiate audiences by information consumption habits, to identify different information platforms and channels, as well as actors in the information environment and their motivation.

- **Awareness of national strategy, based on values and goals uniting and binding society, including**:
  The constitutional premise, what the country stands for, what the values and pillars are that the government's institutions are expected to protect, and that civic groups are ready to stand for; policy declarations expressed through a government action plan or other public documents, developed and agreed based on legitimacy provided through the electorate.

- **Awareness of the communicative value of government policies and societal processes, including:**
  The organisation of communication work in public institutions, attention devoted to communicating government policies; resources invested and the processes established to ensure the responsibility to communicate to public vs the option to do so.

- **Determination to align all the efforts with communicative value for reaching the overarching goal, including:**
  The political priority assigned to the application and execution of a strategic communications mindset; involvement and cooperation of all the relevant government agencies, raising awareness on the role individual institutions and their actions of communicative value play in achieving the overarching goal.

- **Ability to lead the alignment and coordination process, including:**
  A legitimate authority at the strategic level providing guidance through a strategic communication framework with a clearly defined and widely or nationally agreed strategic goal; well-established coordination processes and instruments that allow for the practical alignment of all relevant efforts.

StratCom and Elections

In the context of election security, the StratCom approach and mindset requires a thorough understanding of the information domain and cognitive space where the decision-making of voters takes place. But most importantly, it requires an understanding of the complex administrative process ensuring free and fair elections, namely the infrastructure and procedures and how they are perceived. They all affect the strategic communications effects.

The challenge in applying this mindset throughout the preparations and execution of elections lies in the complexity of the election process, which is run, managed and affected by many different actors. There is the administrative layer, the role the potential voters play, the role of political parties and individuals running for office, and the information domain. They all influence, and in turn are influenced by, the dynamics of others.

It should be noted that the approach taken by Sweden, Latvia, Estonia and Finland has been more ambitious than those of many other countries. The awareness of these states, societies and economies of the effects and risks of the recent development in information and communications technologies, as well as their readiness to develop them, has created a sense of urgency and political ambition that has made the issue of resilience against threats of malicious influence through this very same information environment a part of government ambition.

What has worked very well in the election security processes in these four countries is that their institutions have been able to ensure the alignment of very targeted efforts, and do so well in advance of elections. This has included an awareness of the scope of the challenges at the strategic level as well as a clear understanding among stakeholders what their roles and tasks are. This has made sure that the topic of election security resonates at the highest political level, leading to e.g. a conscious positioning of the message of the president of Estonia through social media communication, and that of the president of Latvia through a series of public discussions on election security. Meanwhile, other stakeholders such as state institutions, the media, and citizens, were made conscious of their role and the potential effects of their behaviour.

Election security preparation starts with the mapping of the following StratCom dimentions:

1. **Information landscape**: What is the situation we are in, and what are we protecting?

   a. Map the core elements of the information environment and the election process.

   b. Identify elements affecting the decision-making of voters in your country.

   c. Identify and prioritise what the most important things are you want to protect.

2. **Threat assessment**: What is the threat?

   a. What does the current threat assessment look like, and what are the publicly recognised security risks?

   b. What does the threat consist of?

   c. How could activities that aim at influencing information materialise?

   d. What are the likelihood and consequences of influence activities?

   e. Which risks do we have to accept?

3. **Risk and capability assessment**: How do we handle the identified risks?

   a. How can we reduce the probability of election interference?

   b. How can we reduce the consequences of election interference?

   c. What is our monitoring capability? (scope, stakeholders, mandate, task)

   d. What are the deterrence mechanisms at our disposal?

   e. What are the mechanisms through which we will coordinate our response?

Malicious influence and interference as a StratCom challenge

The diversity of views, preferences and priorities of different groups in society that make up the backbone of a modern democracy will make it difficult to distinguish and spot undemocratic and "inorganic" or artificially injected processes orchestrated by (foreign) actors outside the legitimate space of the debate and citizens' rights.

The concept of foreign malicious influence attempts - deliberately designed, tailored and targeted to influence the decisions of voters - are very difficult to distinguish from the legitimate processes in the information environment. Every political party and candidate is trying to influence the actions of voters, hoping to gain more votes themselves. The main difference, and also the most difficult to prove, is the foreign malicious element in the influence attempts. One element which can potentially lead to the attribution of specific activities to foreign interference is the financial footprint in the form of contracts and evidence of cooperation. However, this attribution is often only possible after the fact. This is the reason why the countries studied in this paper have chosen to invest in resilience building, rather than focusing only on attribution.

What makes the StratCom challenge even greater is the observed tendency of some of the local political parties to use narratives of hostile foreign actors on purpose. This might provide them with an already "warmed up" audience, and promise better results. It is of course the legitimate right of political parties to choose their own rhetoric, and it is not for government institutions in charge of election security preparations to deal with this kind of situation as long as it occurs within the limits of the law.

What is election interference?

To reach an informed understanding of the threat of election interference, an analytical framework is needed. This starts with the perception of the problem. People often assume that election interference only aims to influence who *wins* an election, while in reality the problem is more complex than that, as the interference may aim to produce a different result. The analytical framework allows us to visualise, collect, compare and organise the lessons identified. Our framework is based on the original work done by the Swedish Civil Contingency Agency, developed by the Carnegie Endowment[1] and now further refined by us.

An analytical framework for election interference

Election interference aims to influence the outcome of an election, to undermine trust in the election, or to use the election to achieve other goals, such as undermining democracy, internal cohesion or influencing how a country is perceived externally.

These effects can be accomplished by influencing a) the election as an administrative process, b) the will and ability of voters to participate in the election, and c) the election as a political process.

These three components should be seen as interconnected processes that can be influenced via various activities, ranging from targeting the election infrastructure to manipulating the political debate.

In Figure 1, we have visualised this framework and paired it with known influence activities that have been used in previous elections.

Threats against the election as an administrative process

Without the public's trust that elections can deliver a credible result, a cornerstone of democracy is at risk. Even without antagonists seeking to influence them, elections are complex undertakings with numerous risks linked to the legal, operational, technical, political and security aspects of electoral processes.

Antagonists can leverage the vulnerabilities of the system in order to change the outcome of an election, to weaken trust in it, to undermine the credibility of elected officials, to reduce trust in the state, to sow internal discord, and so on. During the US presidential election in 2016, there were attempts to hack election systems and their infrastructure. During the Kenyan presidential election in 2017, actors spread fake error logs that supposedly originated from the election management system. And during the Swedish elections in 2018, actors spread disinformation to try to reduce trust in the conduct of elections.

Threats against the will and ability of voters to participate in elections

In order to conduct legitimate, free and fair elections, it is necessary to protect the will and ability of the population to participate in them. This entails ensuring equal access to correct information about where, when and how citizens can vote.

In recent elections, there have been attempts to spread false information about how they are carried out. Antagonists have tried to get voters to not participate by spreading false information about where, when and how citizens can vote. We have also seen attempts at voter intimidation, with the aim of undermining voter participation. At the far end of the spectrum, violence or the threat of violence has been used to try to dissuade voters to participate.

Threats against the election as a political process

Illegitimate information influencing activities are different from legitimate communication activities in that they are *deceptive:* they involve falsehoods in some way or other, they have the *intention* to exploit vulnerabilities to benefit a foreign power or its proxies, they seek to *disrupt* constructive debate, and they *interfere* in debates or issues in which foreign actors have no legitimate role to play.[2]

Hostile actors have previously tried to interfere with the political process by means of cyberattacks directed at political parties, the publication of stolen and manipulated information, targeted micro ads against a vulnerable target audience, paid and automated manipulation through social media, and so on.

Attempts to interfere in the political process using subversion, proxies and other forms of illegitimate means to distort a political process falls within this category of interference.

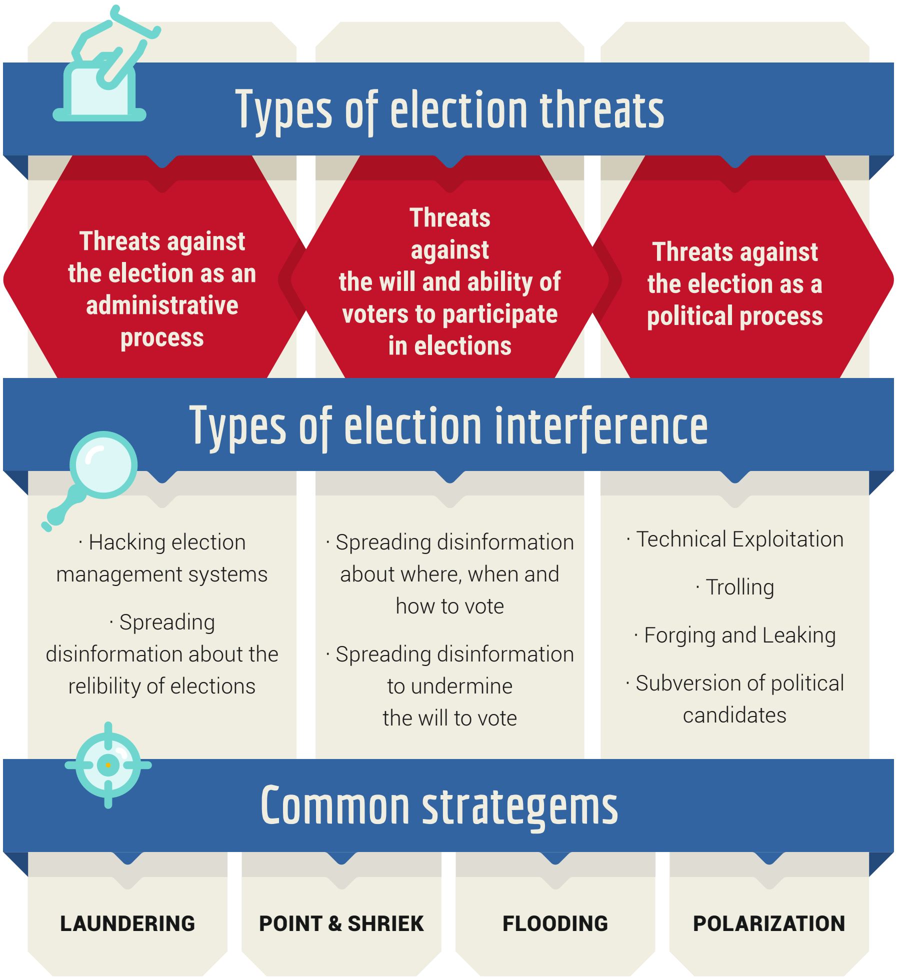

Types of election threats
Threats against the election as an administrative process
Threats against the will and ability of voters to participate in elections
Threats against the election as a political process
Types of election interference
· Hacking election management systems
· Spreading disinformation about the relibility of elections
· Spreading disinformation about where, when and how to vote
· Spreading disinformation to undermine the will to vote
· Technical Exploitation
· Trolling
· Forging and Leaking
· Subversion of political candidates
Common strategems
LAUNDERING
POINT & SHRIEK
FLOODING
POLARIZATION

Figure 1

Stratagems[3]

Individual methods and techniques for election interference are rarely used in isolation. Rather, influence operations and campaigns most often combine a multitude of methods and techniques into complex chain of events, or stratagems. While such combinations are theoretically infinite, some stratagems are frequently encountered in contemporary influence operations.

Common stratagems include:

Laundering

Information laundering refers to the process of legitimising false information or altering genuine information by obscuring its origin. Often this involves passing genuine information through a series of intermediaries (such as fake news or foreign language websites), gradually distorting it and feeding it back to legitimate channels through Potemkin villages.

Point & Shriek

The point & shriek stratagem builds on tactics used by social activists, taking advantage of perceived injustices within certain social groups and heightening emotion around these issues to disrupt rational discourse.

Flooding

Flooding creates confusion by overloading actors with spurious and often contradictory information.

Polarisation

By using a series of deceptive identities, it is possible to support opposing sides of a specific issue to create or reinforce grievances, heighten emotional response, and force mainstream opinion toward greater extremes.

How do we protect elections?

Protecting elections is a multi-layer and multi-stakeholder process that necessitates the development of new coordination mechanisms, new methods and tools to monitor and assess the information environment, improved routines for risk and vulnerability analysis and a framework to assess and respond to election interference.

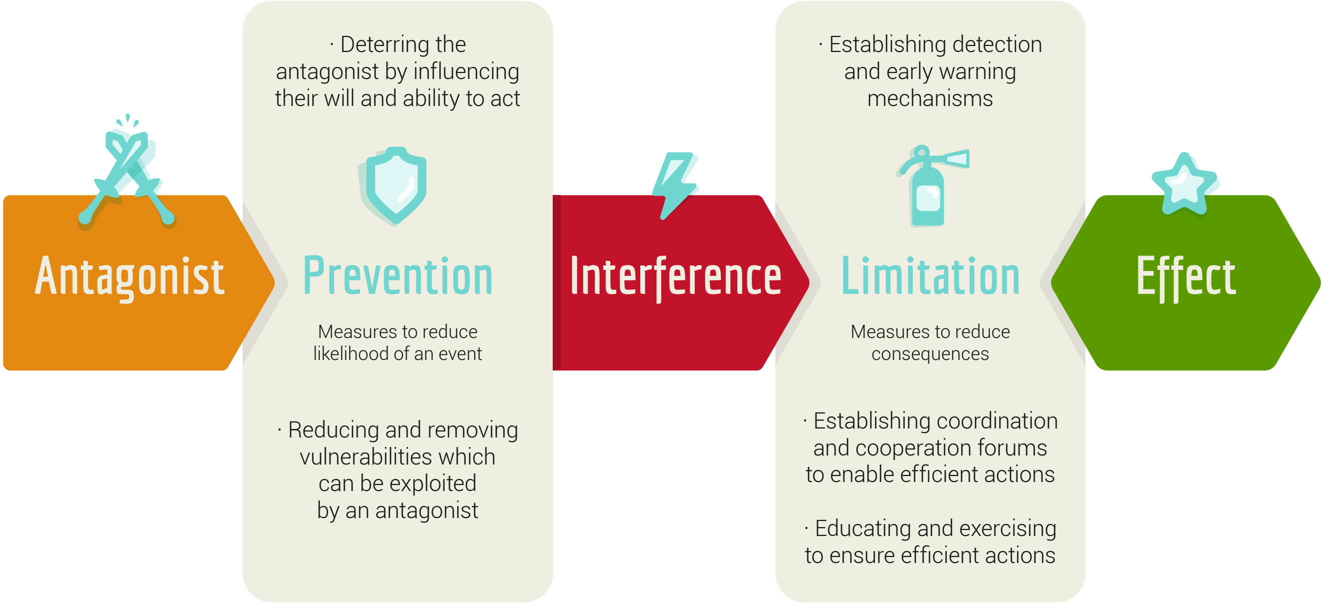
Each country we have studied has chosen a different way to organise its work according to national processes, their legal framework, and – above all – national risk and vulnerability assessments. It is important that any response developed builds on a firm understanding of threats, risks, and vulnerabilities. While the four countries studied face similar challenges, there are also important national differences in regard to the nature of the challenges they face.

Any malicious actor needs to be understood from the perspective of its will and ability to influence an election. In order for a malicious actor to be able to act, there must be an opportunity to act. For that reason, the malicious actor should be understood based on an assessment of its intention and capacity, paired with potential opportunities to act.

Election protection consists of the prevention of election interference as well as efforts to ensure that interference has limited consequences.

Both prevention and limitation are essential StratCom challenges, as they require a whole-of-government approach to securing elections, deter interference, and strengthen trust in democracy at the same time.

In Figure 2 below, we visualise this process as a framework for protecting elections.


Antagonist
Prevention
· Deterring the antagonist by influencing their will and ability to act
Measures to reduce likelihood of an event
· Reducing and removing vulnerabilities which can be exploited by an antagonist
Interference
Limitation
· Establishing detection and early warning mechanisms
Measures to reduce consequences
· Establishing coordination and cooperation forums to enable efficient actions
· Educating and exercising to ensure efficient actions
Effect

Prevention

Election protection seeks to prevent or reduce the likelihood of interference, by targeting the will and ability of malicious actors to interfere. This is accomplished through deterrence (affecting will) and by removing opportunities through the mitigation of vulnerabilities. Proactive work also need to target the capacity of the malicious actor to interfere. Public discussion of the challenge of election interference is an important aspect of prevention, both for creating a more resilient society and for deterring antagonists.

Possible actions include:

Deterrence

Strategic communication that seeks to deter a known antagonist from interfering in the election by targeting the will of the antagonist. Such messaging needs to focus on the conditions and vulnerabilities of the antagonist to be effective.

Mitigation

Conducting risk and vulnerability assessments in order to enable mitigation of vulnerabilities.

Disruption

Targeting the capacity of known antagonists to interfere by e.g. reporting coordinated inauthentic networks, disrupting funding, taking legal action etc.

There are a range of methods and techniques for risk and vulnerability assessments. But no matter which technique is used, risks need to be identified and assessed based on their probability and consequences. Such an assessment needs to identify risks that are acceptable as well as those that will need to be mitigated. Vulnerabilities need to be assessed in order to identify critical dependencies. The consequences of a certain action, given the ability of an organisation to resist and address it, is a measurement of how vulnerable the organization is. Dependency analysis identifies which parts of an activity are most important and need to be protected in order to ensure that the activity can resist interference without catastrophic consequences.

Limitation

The limitation of the consequences of interference includes efforts to build the state's capacity to identify and stop any ongoing election interference – as well as long-term efforts that create more resilient systems and societies.

Possible actions include:

Education

to increase awareness and the ability to identify interference. This needs to be prioritised and focused based on a vulnerability assessment.

Training

to identify and counter interference based on credible scenarios involving all the relevant layers of society. Training often results in suggestions for risk and vulnerability reductions that need to be addressed.

Coordination and cooperation

establishment of cooperation mechanisms for election protection is essential and needs to involve academia, private actors and civil society.

Detection

establishment of functions and reporting mechanisms to strengthen the ability of government, academia, private actors, and civil society to identify and report attempts to maliciously influence elections.

Best practices of Sweden, Latvia, Estonia and Finland

The approach the governments of the four countries have taken to election security is directly connected with their focus on the security of the information environment and its implications on democratic processes. The following are the common principles employed in all four national environments, which, depending on their specific purpose, have been used for either prevention and/or limitation of the effects of election interferences as described in the analytical framework:

1. ASSESS: map the challenges

In order for the coordination mechanisms to work, a mapping exercise spotting all the challenges, in particular the unconventional risks, was undertaken. There are many ways (in terms of structure and formality) to carry out the mapping exercise, however the main common feature has been the ability to integrate views and concerns of all the stakeholders in order to ensure a shared level of ambition and involvement.

Considering that it is impossible to cover all the risks and vulnerabilities simultaneously, all of the countries prioritised their measures as well.

2. COORDINATE: establish functional mechanisms

Recognizing the risk of foreign interference and the need to be well prepared, specific coordination formats were set up in all four countries based on the political priority assigned to election security. While both the responsibility and mandate to hold elections are well defined and established, the new type of challenge has required the application of a more holistic and agile approach to coordination. This involved not only the inclusion of election authorities and security institutions in election security task forces, but the extension of this inclusion to all the state bodies responsible for specific elements of the information environment.

The positioning of election protection high on the political agenda is in itself proof of the application of a StratCom mindset and approach to this challenge. Most typically, these task forces have been run under the auspices of Government Offices, with a clear mandate by the highest political authority. Public awareness of the existence of these mechanisms has ensured an according sense of preparedness. In most of the cases, the people leading the coordination mechanisms have been publicly outspoken in order to raise the awareness of the risks and the preparations undertaken to counter them.

3. PROTECT: build resilience

The mapping of challenges, or gap analysis, together with an agreed level of ambition, provides a natural roadmap for resilience building. This can turn out to be an exhaustive list of tasks, no doubt, and therefore prioritisation is key. In most of the cases analysed, short-term resilience building ahead of elections has focused on improving the resilience of the main actors in the media landscape, namely media organisations (e.g. through scenario-based table top exercises and tailor-made training on digital skills in the case of Latvia and Finland organised by the government institutions or the private sector itself), institutional communicators (e.g. empowering and educating them by providing and publishing a handbook for communicators on countering information influence activities in the case of Sweden and Finland)[4], political parties (in terms of their cyber-vigilance and resilience against cyberattacks, as well as other aspects of election interference e.g. through training by CERTs, security services, cross-governmental teams and private sector companies); social media companies and online platforms (through functional and close working relations based on a clear understanding of their security policies, procedures, and ability to take swift action), and exercises in internal coordination and response. Without a doubt, stress tests of the election infrastructure itself are the most important area, where the importance of resilience cannot be underestimated.

In the case of Finland, the *Comprehensive security concept*[5] itself, the core idea behind the security and defence mindset in Finland, is focused on building resilience networks within the Finnish society. It has played a significant role also in the context of election security, allowing the government to rely on already established mindset and cooperation mechanisms with the private sector as well as other players.

4. COOPERATE: build networks of partners

While national preparations can be very ambitious, the lack of awareness and detailed understanding of the approaches taken can result in unhelpful reactions on the part of neighbouring countries or partners. Attempts at interference can be aimed at the unity and solidarity among partners as well. Therefore, the establishment of well-functioning networks for the exchange of information is key. This also requires joint strategic communications perspectives on possible risks, and agreed mechanisms and principles of public positioning in the case of interference. In some cases, a dedicated effort was made to maintain a contact list and network of all the counterparts in partner countries. The efficiency of this approach depends on the systematic effort to maintain the quality of the contact list.

5. DETECT: monitor the information environment

The complexity and dynamics of the information environment make it near to impossible to monitor and analyze all of the processes in it. However, in the context of elections, it is not necessarily useful to aim for maximum coverage. The main principles most often adopted are: a) agreement on areas of priority for monitoring, b) use of tools that have proven to be efficient in providing reliable results, and c) diversification of monitoring approaches and the entities conducting it, thereby ensuring the trustworthiness of the results if misconduct is identified.

In some cases, parallel to the monitoring done by government institutions, some specific monitoring tasks were outsourced to the academic and public sector (even outside the country in question). This increased the trustworthiness of the results. In most cases, quality and a comprehensive coverage was assured through the encouragement of institutions to continue with their regular monitoring strategy while adding specific guidelines to the existing focus, e.g. thematic topics of interest to observe. This diminished the risk that institutions will lose time testing new tools with questionable efficiency. This was particularly pertinent to monitoring done in smaller languages, where automation and the use of machine learning technology often did not provide desired results.

In Sweden, several studies were commissioned from academic and government entities to provide independent monitoring of the information environment.[6,7]

6. EDUCATE: raise public awareness and involvement of the non-governmental sector

The presence of critical thinking and media literacy skill set in a society significantly increases the resilience against malicious information influence and foreign interference. The role that NGOs, research institutions, investigative journalists and the media in general play in improving the awareness of society of possible risks is significant (but also incremental). In case of the four countries analysed, the positive effects of NGOs and civic society organisations' willingness to ensure full transparency of electoral processes, including the influencing of voters' choices, have helped ensure a high level of resilience.

In the case of Latvia[8] and Estonia[9], the involvement and dedication of investigative journalists resulted in significant discoveries of potential interference or attempts to abuse social media platforms.

Election security preparations in Finland, for the very first time in the 110-year history of election preparations in Finland, included a comprehensive public communications campaign aimed at raising voter awareness of possible interference attempts.[10]

Early in 2018, the Swedish Prime Minister pointed out that there is a clear risk of foreign interference in elections, and delivered a stern warning: “To those of you who are considering to influence our elections: stay away. We will not hesitate to ruthlessly expose you. […] We will defend our democracy and freedom of speech with all available means at our disposal.”[11]

Regarding approaches taken towards resilience building, the Estonian case is worth mentioning. Anticipating that the e-voting system would become a potential target of disinformation campaigns, a dedicated information campaign was launched through traditional media channels, addressing topics related to the e-voting system as well as mitigating existing myths. It is important that this kind of communication activity does not respond to claims brought up by groups with specific interests, but is conducted on the terms decided by the responsible institutions themselves, allowing them to frame the narrative in the most objective manner and using platforms of their choice.

Social media related policy challenges

Looking at the experiences concerning elections in democratic countries over the last couple of years, all of them seem to be struggling with similar challenges. Part of these challenges are related to today’s information environment, which defines the cognitive processes in the decision making of voters. Compared to the situation half a century ago, it appears that the scope of the elements influencing potential voters is much wider, and the effects less linear. Studies suggest that social media and other online platforms play an increasingly important part in the choices of the voters. For a couple of years now, individual countries and international organisations have striven to develop new regulations to ensure that the risks of malicious influence and interference in elections can be managed. This, however, doesn’t mean that malicious influence through other channels and means isn’t still a challenge to deal with.

In 2017, the European Commission initiated a process for the development of a strategy to combat fake news, including the appointment of a high-level expert panel on disinformation.[12] This comprehensive process, among other things, resulted in a voluntary Code of Practice (CoP) against Disinformation, released in September 2018 and signed by a number of social media platforms and Internet giants,[13] and an EU action plan against disinformation.[14] The main principles of the CoP have become a checklist for monthly reports the companies present leading up to the EU parliament elections for the Commission to assess progress made on the implementation of the CoP. Until now, none of the progress reports have suggested that the biggest concerns the countries have raised are adequately covered.

We found that the following elements are the most critical aspects that social media and online giants need to improve in the context of election security:

1. Monitoring of targeted, coordinated attempts to influence decision making of voters, including the misuse of large interest groups, pages and other moderated forums for political purposes through automation, increased manual moderation and assessments, or new technical solutions to prevent malicious use.

2. Monitoring of impersonation of government and public accounts.

3. Ad transparency, specifically regarding the microtargeting of segments of the public.

4. Recognition and swift elimination of the use of non-organic manipulation of user engagement in order to manipulate the perceived popularity of a certain view, or of certain content.

5. Transparency and accountability to enable greater public insight and involvement in securing the online environment.

6. User-friendly integration of fact-checking mechanisms.

The steps taken by EU institutions to secure the European elections are happening against the backdrop of the new dynamics concerning social media companies and Internet platforms. In any case, the establishment of a network of national contact points and the Rapid Alert System are unprecedented efforts in the direction of election security, but the narrow timeframe within which these concepts are developed make it likely that it will take time for all the stakeholders to get used to their roles assigned, and consequently for the systems to be effective.

Simultaneously, the experiences studied have brought out the necessity to widen the legislative basis required to respond to attempts of malicious interference also with legal means. Considering the dynamics in the social media and online landscape, it is essential that government institutions aim to be as visionary as possible to prepare the legislative framework for dealing with issues like deep fakes.

Conclusion

A number of countries have taken significant steps during the past few years to safeguard their democratic processes. Important work that needed to be done, given the clear evidence of recent election interference.

Deliberate attempts to manipulate elections, electoral infrastructure and campaign information systems are a significant threat to our democracies which need to be actively combatted using all available means.

To effectively combat election interference in the future, the European Union, its member states and any democratic country determined to hold free and fair elections all need to be clear and outspoken on this, and issue clear statements to deter other nations and actors from interfering in their democratic processes.

Based on the experiences studied in this paper, we conclude that a checklist for other governments in their election security preparations focusing on exploring the StratCom perspective can be summarised as follows:

1. Conduct comprehensive threat analysis and set your priorities;
2. Focus on resilience building according to the threat analysis;
3. Consider deterrence factors;
4. Establish coordination and cooperation mechanisms;
5. Establish early warning and detection mechanisms;
6. Invest in education and training;
7. Establish strategic communications framework - from deterrence to crisis communication.

Provided that the institutions and government offices concerned aim to collaboratively follow these principles, remain vigilant about the situation in information environment and establish effective cooperation with the non-governmental sector and media, these measures should ensure a decent level of resilience for election security.

Endnotes

1 Brattberg, Erik, and Tim Maurer. “Russian Election Interference: Europe’s Counter to Fake News and Cyber Attacks.” Carnegie Endowment for International Peace, 23 May 2018

2 Pamment, James, Howard Nothhaft, Henrik Agardh-Twetman, and Alicia Fjällhed. ”Countering Information Influence Activities: The State of the Art”. Swedish Civil Contingency Agency (MSB), 2018

3 Pamment, James, Howard Nothhaft, Henrik Agardh-Twetman, and Alicia Fjällhed. ”The Role of Communicators in Countering the Malicious use of Social Media”. NATO StratCom COE, 2019

4 “Countering Information Influence Activities.” Msb.se - Countering Information Influence Activities - A Handbook for Communicators

5 Security Strategy for Society, Government Resolution / 2 November 2017

6 FOI presenterar två studier om det svenska valet, 10 October 2018

7 Forskare lanserar MSB-finansierad studie om informationspåverkan av det svenska valet, 29 October 2018

8 Re:Baltica investigative reports on fake News

9 Roonemaa, Holger. “Do Kevin, Oskar and Oksana want to meddle in our elections?”, Postimees.ee, 31 December 2018

10 “Finland Has the Best Elections in the World. And Why Is That.” Valtioneuvoston Kanslia

11 “Sveriges säkerhet i en ny värld” Tal av statsminister Stefan Löfven vid Folk och Försvars Rikskonferens i Sälen, 14 January 2018

12 “Commission appoints members of the High Level Expert Group on Fake news and online disinformation”, 12 January 2018

13 Code of Practice on Disinformation, 26 September,2018

14 Action Plan against Disinformation, 5 December 2018

Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

Operating since 2014, we have carried out significant research enhancing NATO nations' situational awareness of the information environment and have contributed to exercises and trainings with subject matter expertise.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org