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.