Fortifying Democracy: Countering Foreign Election Interference

Executive Summary

Foreign governments' attempts to hack and influence outcomes threaten the integrity of national elections. This policy brief addresses the critical need for enhanced election security measures to safeguard democratic processes globally. Proposed policy actions include implementing advanced cybersecurity measures, fostering international cooperation, and establishing stringent legal frameworks. These measures aim to protect election infrastructure, restore public trust, and ensure the stability of governments.

Context/Scope of Problem

Election interference by foreign governments is a pressing global issue that undermines democratic institutions and processes. Russian operatives' hacking of the 2016 US presidential election highlighted the vulnerabilities in election security. Similar attempts have been observed in other countries as well, namely:

Ukraine: Ukraine has been a frequent target of Russian interference, particularly since the annexation of Crimea in 2014. Russian-backed hackers have been accused of attacking Ukraine’s election infrastructure, and disinformation campaigns have been launched to undermine the government.

Germany: The German government has repeatedly warned of Russian interference, especially during the 2017 federal elections. Russia was accused of using cyberattacks, such as the 2015 Bundestag hack, to steal sensitive information, which eventually influenced the elections heavily.

France: The 2017 French presidential election saw significant interference efforts, including Russian-linked groups hacking Emmanuel Macron’s campaign. The attack, followed by the release of stolen emails, was still considered a major factor in the election outcome.

United Kingdom: During the 2016 Brexit referendum, Russia-based groups used disinformation campaigns and social media to amplify certain narratives. Additionally, reports of Russian donations and political links have recently resurfaced.

Such interference can alter election outcomes, diminish public trust in democratic processes, and destabilise governments. The global nature of this threat necessitates robust policy actions to secure election infrastructure and uphold democracy.

Policy Alternatives

Current Policy Approach

The current approach to election security varies significantly across different countries, but many rely on a combination of reactive and preventive measures.

1. **Reactive Measures**: Many countries wait until a breach or attempted interference occurs before taking action. This involves post-incident analysis, damage control, and subsequent incremental improvements to the systems. While this can provide valuable insights into vulnerabilities, it is often too late to prevent the damage.
2. **Basic Preventions**: Some countries have implemented basic cybersecurity measures, such as firewalls, antivirus software, and regular system updates. While these measures are essential, they are insufficient against sophisticated, state-sponsored cyberattacks.
3. **International Frameworks**: International agreements and frameworks, such as the Budapest Convention on Cybercrime, exist to prevent election interference. However, these frameworks lack enforcement mechanisms.

Proposed Actions

To counter the limitations of the current policies, the following alternatives are proposed, each with its unique approach to enhancing election security:

1. Proactive Cybersecurity Measures
    - **Comprehensive System Overhaul**: A complete overhaul of election infrastructure incorporating state-of-the-art technology and cybersecurity measures. This includes replacing outdated voting machines, implementing robust encryption protocols, and ensuring all election-related systems undergo regular security audits.
    - **Continuous Monitoring**: Establish a 24/7 cybersecurity operations centre dedicated to monitoring election systems in real-time, using traffic monitoring, advanced AI and machine learning tools to detect and respond to threats immediately.
    - **Incident Response Teams**: Develop specialised incident response teams that can be deployed rapidly to address breaches.

2. International Cooperation

    Form a coalition of nations committed to sharing intelligence on cyber threats to elections. This alliance would facilitate the exchange of information on emerging threats and best practices and coordinate joint responses to incidents. They must also conduct regular multinational cybersecurity exercises that simulate election interference scenarios. Countries also should be required to engage in diplomatic efforts to build consensus on international norms and agreements that condemn and penalise election interference. This includes leveraging international bodies like the United Nations to adopt resolutions reinforcing these norms.

3. Legal Frameworks
    - **Domestic Legislation**: Enact comprehensive domestic legislation that criminalises election interference and prescribes severe offender penalties.
    - **Cybersecurity Standards**: Mandate stringent cybersecurity standards for all election-related technologies and processes. These standards should be developed in consultation with cybersecurity experts and updated regularly to keep pace with evolving threats.

4. Enhanced Public Awareness and Education
    - Develop comprehensive voter education programs that inform the public about the nature of cyber threats.
    - Increase transparency in election processes to build public trust. This includes publicly available information about cybersecurity measures, audit results, and incident responses.
    - Create platforms for collaboration between government agencies, civil society, and private sector stakeholders.

Evaluation of Proposed Actions

1. **Proactive Cybersecurity Measures**:
    - **Strengths**: Provides robust protection and enhances the overall security posture of election infrastructure.
    - **Weaknesses**: It requires significant financial investment, ongoing maintenance, and continuous updates to stay ahead of evolving threats.
2. **International Cooperation**:
    - **Strengths**: Leverages collective intelligence and resources, enhances global response capabilities, and fosters a unified approach.
    - **Weaknesses**: Sharing sensitive information can raise potential issues, so enforcement is heavily reliant on international diplomacy.
3. **Legal Frameworks**:
    - **Strengths**: Provides a clear legal basis for prosecuting offenders and reinforces international norms against election interference.
    - **Weaknesses**: Implementation would be uneven across different jurisdictions, and again, there is a need for international cooperation.
4. **Enhanced Public Awareness and Education**:
    - **Strengths**: Empowers voters with knowledge, builds public trust, and promotes vigilance against cyber threats.
    - **Weaknesses**: It may not directly address technical vulnerabilities, and its effectiveness depends on the reach and quality of educational programs.

Policy Recommendations

1. Advanced Cybersecurity Measures

- **Upgrade Election Infrastructure**: Modernize voting systems with end-to-end encryption and conduct regular security audits. This includes replacing outdated voting machines with secure, tamper-resistant systems and ensuring all election-related software is up-to-date and secure.
- **Threat Detection Systems**: Deploy artificial intelligence (AI) and machine learning tools to identify and mitigate threats in real time. These systems can analyse network traffic and detect anomalies indicative of a cyber-attack.
- **Training and Awareness**: Conduct regular cybersecurity training for election officials and stakeholders. This training should cover best practices for identifying and responding to cyber threats and the importance of maintaining secure communication channels.
- **Election Security Laws**: Enact laws that criminalise election interference and outline severe penalties for offenders. These laws should cover a broad range of activities, including hacking voting machines, manipulating voter registration databases, and spreading disinformation.
- **Cybersecurity Standards**: Mandate strict cybersecurity standards for all election-related technologies. These standards should be developed in collaboration with cybersecurity experts and regularly updated to address new and emerging threats.

2. International Cooperation

- **Intelligence Sharing**: Establish a global intelligence-sharing network focused on election security threats. This network should facilitate the timely exchange of information about emerging threats and best practices for mitigating them.
- **Joint Cybersecurity Exercises**: Conduct multinational exercises to prepare for and respond to election hacking attempts. These exercises can help identify vulnerabilities in election infrastructure and improve coordination between countries during an attack.
- **Diplomatic Measures**: Strengthen diplomatic channels to address and resolve allegations of election interference. This includes developing protocols for investigating and responding to claims of foreign interference and holding perpetrators accountable through international legal mechanisms.

Conclusion

The persistent threat of foreign interference in national elections requires comprehensive and proactive measures to safeguard democratic processes. By implementing advanced cybersecurity measures, enhancing international cooperation, and developing stringent legal frameworks, we can protect election infrastructure, restore public trust, and ensure the stability of democratic governments globally. These policy recommendations provide a clear and actionable path forward for policymakers committed to fortifying democracy against foreign threats.

Consulted or Recommended Sources

- Barlow, J. P. (1996). A declaration of the independence of cyberspace. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence
- Lin, H. (2017). The cybersecurity problem. *Strategic Studies Quarterly*, 11(2), 46-71. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-2/Lin.pdf
- Nakashima, E. (2020). U.S. poised to sanction Russia for the SolarWinds cyberattack and election interference. *The Washington Post*. https://www.washingtonpost.com
- Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
- U.S. Department of Homeland Security. (2021). Election security. https://www.dhs.gov/topic/election-security