A framework guide to tools for countering hostile foreign electoral interference

35 measures in 15 steps for enhancing the resilience of the democratic electoral process
1. About This Report

This brief Report aims to enumerate the tools that are nowadays used for hostile electoral interference and how they can be countered. The paper focuses on the European situation, with use of known examples from recent years, for example, in the United States. The aim of this Report isn’t to discuss the historical path or to provide in-depth analysis of the cases.

The objective of this exercise it to lay out a general framework, which can be used by security and intelligence practitioners when setting up a national defence system against hostile foreign interference, with a special focus on the electoral process. This paper doesn’t discuss all the known tools, but focuses on the major ones. This Report discusses the expected scenarios and situations that are most likely to happen, so that specific policies and measures can be taken by national authorities in advance of or during the electoral process.

It is clear that democracies need to set up national policies for countering hostile disinformation operations, which are going on constantly, not only during the electoral period. In addressing these policies, our 50-measure strategy\(^2\) is available as a framework. However, this Report focuses specifically on the vulnerable electoral period.

2. Why Democracies Need to Protect The National Electoral Process

Elections are a cornerstone of every democracy. Elections must be free and fair, with a level playing field for the candidates\(^3\). In recent years, we have seen clear efforts by the Russian Federation and its proxies to influence selected elections and referendums where the Kremlin had a preferred candidate (D. Trump, M. Le Pen) or option (“Leave” in Brexit referendum, “No” in the Dutch 2016 referendum on the Association Agreement of Ukraine with the EU).

While it is often difficult to measure the impact of these efforts on the result, it is clear that those activities are hostile to the democratic order and the national interest of the targeted country. In the end, we are talking about the very sovereignty of a democratic country. Effectively, you are not a sovereign country if a massive hostile foreign interference influences the process of how you select national leaders. That is why it is important for democracies to set up tailored national defence systems against hostile foreign interference to keep their domestic choices free and fair, without a foreign power being able to influence

\(^1\) Author of this Report would like to thank to nine external experts from various U.S. and European government and non-governmental institutions who have given feedback to earlier versions of this paper. The responsibility for content of this Report lays solely on the author.

\(^2\) 50-measure strategy: [www.kremlinwatch.eu/strategy](http://www.kremlinwatch.eu/strategy)

\(^3\) For detailed criteria, see: OSCE Election Observation Handbook, WWW: [http://www.osce.org/odihr/elections/68439?download=true](http://www.osce.org/odihr/elections/68439?download=true)
the choice of the citizens. The bottom line is that democracies must start treating their electoral processes as a part of critical national infrastructure. Practically, this means codifying this policy shift in national security documents and related legislation, plus making the necessary arrangements within the security apparatus.

3. How Interference Can Occur

It is not rocket science to discern which tools are being used, primarily by Russia in Europe, in such interference. In this context, “elections” don’t refer only to the technical process of citizens handing in their votes, but also the pre-election period. This is why the precise term would be “electoral process”. In the following section, in addition to a description of the tool used for interference, we also propose a general framework for counter measures. This obviously needs to be tailored and adjusted to the national and local political, legal, historical and security contexts.

First, there are methods of interference related to the elections themselves, to the technical process that occurs mainly on election day.

There are at least four ways to interfere:

A: Voters

1. voters can be bribed
   - this sometimes happens on the local level, not on a national scale
     - Potential countermeasures:
       - Measure 1 (NGOs): electoral NGO monitors to report on such incidents – a measure well known in post/semi-authoritarian regimes where civil society checks on the state structures, outside of the usual OSCE missions
       - Measure 2 (government): enhanced counter-intelligence monitoring activities.

2. voters can be directly or indirectly intimidated
   - this was seen during the fake so-called “referendum” on Crimea joining Russian Federation in 2014, which was held under the occupation of foreign military forces and therefore declared non-valid and illegal by the international community
   - In 2016, Montenegro has seen activities of Russia-backed extremists who were planning violent acts before the national elections. Investigations are still on-going.
   - Local public meetings can be attacked by hostile entities on larger scale to harass citizen from coming outside (rare in Europe, but sometimes possible).
     - Potential countermeasures:
       - Measure 3 (government): assuring clear public order in the region by enough
law-enforcement entities on the ground

- Measure 4 (government): government authorities have detailed knowledge of local extremist groups and diasporas that are vulnerable to foreign influence and exploitation
- Measure 5 (government): if necessary, postponing the elections/referendum until the source of intimidation is terminated
- Measure 6 (government): support of the international community for pushing back on the source of intimidation

3. voters can be a target of disinformation campaign(s)

- which can be aimed to support one candidate or attack another candidate, usually by disseminating disinformation into mainstream media, disinformation outlets, or through social media
- Russian intelligence agencies target and buy journalists covering policy issues in relevant and even not so relevant national medias. They can even insert their own fake journalists inside media houses to disseminate the Kremlin views to a wider audience. This happened recently in Sweden, where a person with the fake name "Egor Putilov" inserted inside a media house and produced anti-immigrant troll texts as proper journalism. This is a real and ongoing threat, as most of the media leaders in the west are too naive to even accept the possibility someone taking full advantage of them.

  - Potential countermeasures:
    - Measure 7 (government): government authorities have a clear and detailed understanding of the local disinformation community so any relevant changes in their behaviour can be quickly understood or investigated for signs of hostile foreign interference (including through proxies)
    - Measure 8 (government): national authorities have the skill, capacity, political will and competence to perform rapid digital forensics investigation to identify the origins and nature of major disinformation operations (good NGO example: the Atlantic Council’s Digital Forensics Lab)
    - Measure 9 (government & NGOs): a trustworthy partnership between the government authorities and NGO specialists who will investigate the case on their own and present their findings to the national media in real time

---

4 More on the „Putilov affair“ can be found in the Swedish press, WWW: http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=6527230
5 A guide how to set up national STRATCOM team: https://www.baks.bund.de/sites/baks010/files/working_paper_2016_11.pdf
B: Vote delivery & Collection & Count

1. in countries (also) using online voting, it can be hacked or a perception that is has been hacked can be created²
   - Outside of the hacks, there are usually legal instruments to challenge the electoral results. In some cases, high number of legal challenges can be submitted to create the perception of “something being wrong” with the results.
     - Potential countermeasures:
       - Measure 10 (government/NGOs): Using external audits and creating a platform where majority of the relevant non-governmental cyber experts can potentially publicly testify on the alleged hack, so that the perception of a compromised election can be rapidly mitigated by the expert community
       - Measure 11 (government): Extensive audit of the complete voting process needs to be performed. Moreover, additional testing of situations where the perpetrator would play a role in the specific part of the process (physical or online sabotage during the delivery of votes, vote count, delivery of results to the central authorities, and so on).

2. in countries not using online voting, it is almost impossible to compromise the vote delivery. Only the perception that this has happened can be created through disinformation
   - Potential countermeasure:
     - Measure 12 (government): Same as with other disinformation operations – government authorities need to have the skill, capacity, political will and competence to perform rapid digital forensics investigations and related appropriate responses. Informal groups of trusted experts can play a vital role in real-time analysis of the situation and the created media perception.

² Also because of fears of hacks, the Netherlands quited the online voting during its 2017 parliamentary elections.
Second, there are more tools for meddling in the pre-electoral process. We can categorise it simply in the direct objective it follows – whether to support one candidate or attack another. For example, the U. S. and French intelligence agencies have concluded – each in their national context – that the Russian Federation has worked to support one candidate by attacking the other one.

A: Hostile interference tools to attack a non-preferred candidate

1. The candidate, his team or relatives can be hacked and the sensitive files of the campaign, political party, or private conversations can be published.

   - The target of hostile signals intelligence operations can be the candidate’s email account, social media accounts, telephones, private computer files, or exchanges between the candidate and his team or relatives. The use of listening devices and other kinds of surveillance is also to be expected.

   - When publishing stolen material, the perpetrators or their proxies can implant disinformation among genuine files.

      o Potential countermeasures:

         - Measure 13 (government/candidates): Government authorities can provide candidates and their teams with training and consultations on cyber security.

         - Measure 14 (candidates): Candidates can, for example, use decoy email addresses to undermine trust in “leaks”. It would be highly controversial, but possible.

         - Measure 15 (NGOs): Teams of private cyber experts can be organized during the electoral period to be ready and available for external investigations looking into a specific case and providing authoritative explanations to the media.

         - Measure 16 (government): If the electoral process is declared a part of the national critical infrastructure, government authorities might consider using appropriate offensive cyber tools against the perpetrators and platforms publishing the stolen material.

---


9 Politifact, Are the Clinton WikiLeaks emails doctored, or are they authentic?, WWW: http://www.politifact.com/truth-o-meter/article/2016/oct/23/are-clinton-wikileaks-emails-doctored-or-are-they/

2. Disinformation operations can be employed against the candidate.

- Disinformation campaigns might be directed against a candidate on social media, disinformation outlets, or through mainstream media.
  
  - Potential countermeasures:
    
    - Measure 17 (government): Government authorities need to have rapid investigatory and response capabilities\textsuperscript{11}, which would be put on alert during the electoral period. The content, nature and origins of the narratives can be tracked and exposed publicly, to make the facts transparent. No efforts for potential censorship should be made since this would not be right or effective.
    
    - Measure 18 (government/NGOs): Informal networks of private investigators cannot be organized by the government, but can be supported in their activities in order to enhance resilience.
    
    - Measure 19 (government/NGOs): Forecasts of expected trends and scenarios can be published prior to the electoral period to raise the awareness and readiness of the society.

3. Candidates, their teams, and their relatives can become targets of online active measures, blackmail or intimidation.

- Compromising materials, efforts to illegally intimidate candidates, or to physically threaten candidates or their teams or relatives can occur.

- Promoting pro-Kremlin candidates who have been compromised/threatened/blackmailed/bribed to switch their policies pro-Kremlin already decades ago. The Russian intelligence services can work with (manipulate, persuade, soft-soap etc) their target for years and finally recruit the already before the person becomes a relevant candidate for national or local elections. These seemingly independent politicians, but actually long-term pro-kremlin agents of influence inside our electoral systems are damaging and sabotaging our parliamentary decision making as well as public debate.

- Campaigns or their external sponsors (such as hostile foreign intelligence agencies and their proxies) can attack a candidate through active measures such as online bots and trolls.

- Events of the campaign, or for example billboards of the campaign can be massively attacked.
  
  - Potential countermeasures:
    
    - Measure 20 (government/candidates): All political parties can declare and pledge that they will not use any kind of automatized online bots. Such a code of conduct can be codified on the parliamentary level by a joint declaration, while electoral regulatory bodies can sanction breaches of the rule, if sanctions

\textsuperscript{11} To see more on government actionable stratcom capacities – see www.kremlinwatch.eu/strategy
are put in the electoral legislation\textsuperscript{12}.

- Measure 21 (government): The government needs to appoint a clear executive and coordination authority to one central entity (for example a unit at the Interior Ministry, or a specialized government entity such as MSB Agency in Sweden) to be responsible for protection of the elections. Without a clear political, legal and bureaucratic mandate, very little can be done in real time in the maze of public bodies.

- Measure 22 (government): Government authorities need to have a prepared & have a standardized communication system on how candidates and their teams can share information on these cases with them. A clear and transparent government authority must be designed and announced so that the process is seen as legitimate and serious. The government authority needs to have a mandate to organize other public bodies in real time, for example it needs to have a pre-arranged list of working-level liaisons in key agencies and public entities. For example, a centralized government website can be provided such as it is already set up in Sweden\textsuperscript{13}.

- Measure 23 (government): General guidelines can be created by government authorities for the candidates on which suspicious activities or attempts they should follow and potentially start alerting the authorities.

- Measure 24 (government): The government authority responsible for protection of the elections should conduct an in-depth analysis of legal tools available for protecting the electoral process, which would make the authorities realize what are the weak or blind spots of the current legislation. For example, how practically can foreign funding be delivered to local political entities through proxies and what are the legal ways to challenge that practise\textsuperscript{14}.

\textsuperscript{12} For example, German political parties have declared not to use bots in 2017 Bundestag elections: WWW: http://uk.reuters.com/article/uk-germany-merkel-socialbots-idUKKBN13J1YV2
\textsuperscript{13} The Swedish government multi-channel platform for citizens to find confirmed messages from all state agencies in the event of a crisis: https://www.krisinformation.se/engelska
\textsuperscript{14} Good practise example: LSE paper „New Political Campaigning“, WWW: http://eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%2019%20-\%20The%20new%20political%20campaigning_final.pdf
B: hostile interference tools to support a preferred candidate

1. In countries where the local environment allows it, a candidate may be directly provided with campaign financing or media support.

- **Well-known case is Marine Le Pen in and prior to 2017 presidential elections when she has openly received sums in millions of EUR.**

- **Example:** Russian-backed disinformation outlets support and help build support for their own extremist candidates. Russia secretly finances and creates audiences for fake media and pro-kremlin extremists to create more acceptance for their favourite candidate and even mobilize targeted citizens to campaign for their candidate. This has been happening for example in Finland, where known neo-nazi hate site MV-lehti and network of similar sites have for months aggressively promoted a suspected criminal Ilja Janitskin as the president of Finland. They even hold an ongoing “protest camp” with “elect Ilja Janitskin as president” in the centre of Helsinki.\(^\text{15}\)

  - **Potential countermeasures:**
    - Measure 25 (government): Exact and enforce legislation prohibiting foreign financing of political activities and campaigns.
    - Measure 26 (government): Legislation forcing the candidates to release their tax returns dating back a number of years to make sure they are not vulnerable to blackmail
    - Measure 27 (government): Legal requirement for 100 % transparent financing in real time (transparent bank account), with major penalties if not obeyed. Effective legal and executive tools for scrutinizing how candidates fulfill legislative requirements.
    - Measure 28 (NGOs): NGO & journalistic watchdogs scrutinize the candidates, their contacts and financing.

\(^{15}\) More on examples from Finland can be found for example in the Foreign Policy article: http://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/
2. A candidate can be supported through his team receiving financial benefits.

- Example: Chief advisor to Czech President Miloš Zeman, Martin Nejedlý, had his personal debt paid for by Moscow-based Lukoil headquarters, in order to keep him as a key Kremlin connection in the Czech presidential office\textsuperscript{16}.
  - Potential countermeasures:
    - Measure 29 (NGOs): NGO & journalistic watch-dogs scrutinize the candidates and their teams, their contacts and financing.
    - Measure 30 (government): Precise checks and balances inside the government system – good practise: the process how Michael Flynn left the NSC after allegedly being considered vulnerable to blackmail in a Russia-connected case\textsuperscript{17}.

3. A candidate can receive intelligence support on its opponents from abroad

- A candidate or his team can get information based on intelligence collected by a foreign agency identifying weak spots of his/her opponent, or simply delivering information
  - Potential countermeasures:
    - Measure 31 (NGOs): NGO & journalistic watchdogs scrutinize the candidates and their teams, their contacts and financing.
    - Measure 32 (government): Rigorous rules for candidates and their team prohibiting them from meeting or receiving information from foreign agencies, or binding them to declare it to the national counter-intelligence agency if such contact occurs
    - Measure 33 (government): Precise and legal surveillance conducted by the national counter-intelligence agency to protect the candidates from any meddling by foreign agencies

\textsuperscript{16} The New York Times, How Russians Pay to Play in Other Countries

\textsuperscript{17} The Washington Post, Justice Department warned that Flynn can be vulnerable to Russian blackmail, WWW: https://www.washingtonpost.com/world/national-security/justice-department-warned-white-house-that-flynn-could-be-vulnerable-to-russian-blackmail-officials-say/2017/02/13/fc5dab88-f228-11e6-8d72-263470bf0401_story.html
4. A candidate can be getting in-kind support by being invited to Russia or Russian-occupied territories in Ukraine

- Usually, mainly marginal far-right or far-left European politicians help Russia by taking part in fake observations of fake elections, but sometimes even European mainstream politicians participate. They might receive in-kind contributions, money, intelligence, or symbolic support.
  
  o Potential countermeasures:
  
  - Measure 34 (NGOs): NGO & journalistic watch-dogs scrutinize the candidates and their teams, their contacts and financing. The politicians need to be asked and investigated on how they paid for their trips.
  
  - Measure 35 (political establishment): Since most of it would be legal, only the process of the visit needs to be publicly scrutinized by the entities such as national parliaments to which the politicians belong. For example, a public denunciation of a trip by a committee could occur.
To summarize, let us overview the key suggested measures to be taken in four key areas.

1. **Level of capacity-building within civil society (NGOs, think-tanks and journalists):**

   **Step 1:** Among local civil society, there is a need for **NGOs and think-tanks specialized in Russian influence and disinformation.** Without at least several proven non-governmental entities, it is almost impossible to dig in live cases because there would be a lack of institutional knowledge of the local Russian modus operandi and the empirical situation of various pro-Kremlin projects and entities. NGOs can also play important role which government entities cannot – by exposing and confronting political allies of the Kremlin in national parliaments. Today, even major countries like Germany or France lack a robust network of specialized expert bodies and the issue is still mainly a matter of several individuals. These organisations need to be supported by donors in order to build-in their specific expertise and knowledge.

   **Step 2:** Media outlets need to **appoint internal specialists** in their teams who would build the institutional and individual knowledge of this complex issue. That is the only way how they can be effective in the long run, doing in-depth investigative pieces into local Kremlin proxies. Donor organisations should conduct or support issue-related trainings, and sharing of relevant experience should take place as well.

   **Step 3:** Groups of private cyber security experts should be available for external investigations looking into specific cases and providing authoritative explanations to the media. These groups need to be financially independent from the government, for example by serving on advisory boards of trusted professionals associations.

2. **Level of platform-building between government authorities and civil society:**

   **Step 4:** A **trustworthy partnership between government authorities and NGO specialists** needs to be created. The NGOs and volunteer private investigators will investigate the cases on their own and present their findings to the national media in real time. Practically, a local Ministry can organize regular meetings with groups of concerned expert stakeholders to share information and some level of basic trainings to keep the relationship running. For example, local think-tanks or professional associations can organize informal meetings, lessons-sharing, or trainings for interested activities and specialists. The government authorities can fund training programmes on digital and cyber-security literacy, which would help to create loose informal networks of concerned motivated individuals with relatively high level of knowledge and cyber/investigative skills. Examples of such volunteer groups could be the Baltic Elves, “Slovak Forum against Propaganda” or the Polish network called “Fifth Column”.

   **Step 5:** **Forecasts of expected trends and scenarios should be published** prior to the electoral period in order to raise the awareness and readiness of society. Those forecasts can be created by specialized
think-tanks and NGOs while using informal consultations with entities within the national security establishment.

3. Level of cooperation between government authorities and candidates:

**Step 6:** Government authorities should provide candidates and their teams with **trainings and consultations on cyber security.**

**Step 7:** Government authorities need to have a prepared and **standardized communication system on how candidates and their teams can share information on potential hostile interference cases with them.** A clear and transparent government authority must be designed and announced so that the process is perceived as legitimate and serious.

**Step 8:** All political parties should **pledge that they will not use any kind of automatized online bots.** Such code of conduct can be codified on the parliamentary level by a joint declaration, while electoral regulatory bodies can sanction breaches of the rule, if sanctions are put in the electoral legislation.\(^{18}\)

4. Level of government authorities:

**Step 9:** The government needs to **appoint a clear executive and coordination authority to one central entity** (for example a unit at the Interior Ministry or a specialized government entity such as the MSB Agency in Sweden) to be responsible for protecting the elections. Without a clear political, legal, and bureaucratic mandate, very little can be done in real time in the maze of public bodies.

**Step 10:** The government authority responsible for protecting the elections should conduct an **in-depth analysis of legal tools available** for protecting the electoral process, which would make the authorities realize what are the **weak or blind spots of the current legislation.** For example, how can foreign funding be delivered to local political entities through proxies and what are the legal ways to challenge that practise.\(^{19}\)

**Step 11:** Extensive **audit of the whole voting process** needs to be performed. Moreover, additional testing of situations where the perpetrator would play a role in a specific part of the process (physical or online sabotage during the delivery of votes, vote count, delivery of results to the central authorities, and so on).

**Step 12:** Government authorities must have a clear and **detailed understanding of the local

---

\(^{18}\) For example, German political parties have declared not to use bots in 2017 Bundestag elections: WWW: http://uk.reuters.com/article/uk-germany-merkel-socialbots-idUKKBN13J1V2

\(^{19}\) Good practise example: LSE paper „New Political Campaigning“, WWW: http://eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%2019%20-\%20The%20new%20political%20campaigning_final.pdf
disinformation community and extremist groups so any relevant changes in their behaviour can be quickly understood or investigated for signs of hostile foreign interference (including through proxies).  

**Step 13:** National authorities must have the skill, capacity, political will, and competence to perform rapid digital forensics investigations to identify the origins and nature of major disinformation operations (good NGO example: the Atlantic Council’s Digital Forensics Lab) and propose a real-time response. Informal groups of trusted NGO experts can play a vital role in real-time analysis of the situation and the created media perception.

**Step 14:** If the electoral process is declared a part of the national critical infrastructure, government authorities might consider using appropriate offensive cyber tools against the perpetrators and platforms publishing the stolen material. **Internal manuals need to be created in order to have a pre-authorized “game plans” saying** what framework level of response to what incidents might be appropriate, obviously pending the final political decision.

**Step 14:** Practical exercises on various crisis scenarios need to be regularly conducted with the participation of decision-makers at the highest political level as well. In the Baltic countries, for example, the highest political figures regularly participate in similar exercises.

**Step 15:** Review of legislation related to financing of national political activities needs to be conducted. Exact and enforceable legislation prohibiting foreign financing of political activities and campaigns, legislation forcing the candidates to release their tax returns dating back a number of years to make sure they are not vulnerable to blackmail, or a legal requirement for 100 % transparent financing in real time (transparent bank account) with major penalties if not obeyed – those are some of the needed cornerstones. Moreover - rigorous rules for candidates and their team, prohibiting them from meeting or receiving information from foreign agencies, or binding them to declare it to the national counter-intelligence agency if such contact occurs, needs to be put in a law. Practically speaking, legal surveillance conducted by the national counter-intelligence agency needs to be declared and performed in order to protect the candidates from any meddling by foreign agencies and their proxies. The deterrence motive of such move is important – that is why it needs to be known that the **electoral process is a part of the national critical infrastructure.**

---

20 A guide how to set up national STRATCOM team: [https://www.baks.bund.de/sites/baks010/files/working_paper_2016_11.pdf](https://www.baks.bund.de/sites/baks010/files/working_paper_2016_11.pdf)

21 To see more on government actionable stratcom capacities – see [www.kremlinwatch.eu/strategy](http://www.kremlinwatch.eu/strategy)
Voters can be bribed
1. electoral NGO monitors to report on such incidents
2. enhanced counter-intelligence monitoring activities

Voters can be directly or indirectly intimidated
3. enough law-enforcement entities on the ground
4. detailed knowledge of local extremist groups and diasporas
5. postponing the elections/referendum
6. pushing back on the source of intimidation

Voters can be a target of disinformation campaign(s)
7. clear and detailed understanding of the local disinformation community
8. rapid digital forensics investigation
9. present findings to the national media in real time

Online voting can be hacked or a perception that is has been hacked can be created
10. perception of a compromised election rapidly mitigated by the expert community
11. extensive audit of the complete voting process

Perception that regular voting has been compromised can be created
12. rapid digital forensics investigations

Sensitive files of the campaign can be published
13. training and consultations on cyber security
14. decoy email addresses
15. private cyber experts providing authoritative explanations to the media
16. appropriate offensive cyber tools against the perpetrators

Disinformation operations can be employed against the candidate
17. the content, nature and origins of the narratives can be tracked and exposed publicly
18. informal networks of private investigators can be supported in their activities in order to enhance resilience
19. forecasts of expected trends and scenarios prior
### Kremlin Watch Report

**11.05.2017**

35 measures in 15 steps for enhancing the resilience of the democratic electoral process

<table>
<thead>
<tr>
<th>Candidates, their teams, and their relatives can become targets of online active measures, blackmail or intimidation</th>
<th>20. political parties can declare and pledge that they will not use any kind of automatized online bots</th>
</tr>
</thead>
<tbody>
<tr>
<td>21. clear executive and coordination authority to one central should be responsible for protection of the elections</td>
<td></td>
</tr>
<tr>
<td>22. prepared &amp; standardized communication system on how candidates and their teams can share information</td>
<td></td>
</tr>
<tr>
<td>23. general guidelines created by government authorities</td>
<td></td>
</tr>
<tr>
<td>24. in-depth analysis of legal tools available for protecting the electoral process,</td>
<td></td>
</tr>
<tr>
<td><strong>Candidate may be directly provided with campaign financing or media support</strong></td>
<td>25. legislation prohibiting foreign financing of political activities and campaigns.</td>
</tr>
<tr>
<td>26. forcing the candidates to release their tax returns</td>
<td></td>
</tr>
<tr>
<td>27. legal requirement for 100 % transparent financing</td>
<td></td>
</tr>
<tr>
<td>28. NGO &amp; journalistic watchdogs scrutinize the candidates</td>
<td></td>
</tr>
<tr>
<td><strong>Candidate can be supported through his team receiving financial benefits</strong></td>
<td>29. NGO &amp; journalistic watchdogs scrutinize the candidates</td>
</tr>
<tr>
<td>30. precise checks and balances inside the government</td>
<td></td>
</tr>
<tr>
<td><strong>Candidate can receive intelligence support on its opponents from abroad</strong></td>
<td>31. NGO &amp; journalistic watchdogs scrutinize the candidates</td>
</tr>
<tr>
<td>32. rigorous rules for candidates</td>
<td></td>
</tr>
<tr>
<td>33. precise and legal surveillance</td>
<td></td>
</tr>
<tr>
<td><strong>Candidate can be getting in-kind support by being invited to Russia or Russian-occupied territories in Ukraine</strong></td>
<td>34. NGO &amp; journalistic watchdogs scrutinize the candidates</td>
</tr>
<tr>
<td>35. process of the visit needs to be publicly scrutinized</td>
<td></td>
</tr>
</tbody>
</table>
VOTERS CAN BE DIRECTLY OR INDIRECTLY INTIMIDATED

VOTERS CAN BE A TARGET OF DISINFORMATION CAMPAIGN(S)

VOTERS CAN BE BRIBED

ONLINE VOTING CAN BE HACKED, OR A PERCEPTION THAT IT HAS BEEN HACKED CAN BE CREATED

REGULAR VOTING IS ALMOST IMPOSSIBLE TO COMPROMISE, BUT PERCEPTION CAN BE CREATED

VOTERS

VOTERS CAN BE A TARGET OF DISINFORMATION CAMPAIGN(S)

CANDIDATES CAN BECOME TARGETS OF ONLINE ACTIVE MEASURES, BLACKMAIL OR INTIMIDATION

SENSITIVE FILES CAN BE HACKED AND PUBLISHED

ATTACK A NON-PREFERRED CANDIDATE

CANDIDATE MAY BE DIRECTLY PROVIDED WITH CAMPAIGN FINANCING OR MEDIA SUPPORT

CANDIDATE CAN RECEIVE INTELLIGENCE SUPPORT ON ITS OPPONENTS FROM ABROAD

CANDIDATE CAN BE SUPPORTED THROUGH HIS TEAM RECEIVING FINANCIAL BENEFITS

CANDIDATE CAN BE GETTING IN-KIND SUPPORT BY BEING INVITED TO RUSSIA OR RUSSIAN-OCCUPIED TERRITORIES IN UKRAINE

SUPPORT A PREFERRED CANDIDATE

VOTE DELIVERY & COLLECTION & COUNT

DISINFORMATION OPERATIONS CAN BE EMPLOYED

ONLINE VOTING CAN BE HACKED, OR A PERCEPTION THAT IT HAS BEEN HACKED CAN BE CREATED

REGULAR VOTING IS ALMOST IMPOSSIBLE TO COMPROMISE, BUT PERCEPTION CAN BE CREATED

ELECTIONS

PRE-ELECTORAL PROCESS
Kremlin Watch Report
11.05.2017
35 measures in 15 steps for enhancing the resilience of the democratic electoral process

Do you like what we do?
Support us! Our work is possible due to individual donors such as yourself.

Use the form at: http://www.europeanvalues.net/o-nas/support-us/

Or send your donation directly to our transparent account: 2300405420/2010.

© Evropské hodnoty z.s. 2017
The European Values Think-Tank is a non-governmental policy institute defending liberal democracy.

Our vision is that of a free, safe and prosperous Czech Republic within Central Europe that is an integral part of the West.

We help to face aggressive regimes, radicalisation within the society, the spread of authoritarian tendencies and extremist ideologies including Islamism.

We provide decision-makers with expert recommendations and we systematically watch and evaluate their performance. We consider active citizens, accountable politicians, political parties that fulfil their role, as well as cohesive society that shares the values of individual freedom, human dignity and equal rights to be the principle elements of a functioning liberal democracy.

Since 2005, as a non-governmental and a non-profitable organisation which is not linked to any political party, we have pursued research and educational activities. In addition to publishing analytical papers and commentaries for the media, we organise conferences, seminars and training sessions for both experts and the wider public. Our events provide a platform for dialogue amongst politicians, experts, journalists, businesspeople and students.