1. About This Report[1]

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

[3] For detailed criteria, see: OSCE Election Observation Handbook, WWW: http://www.osce.org/odihr/elections/68439?download=true

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.[7] and French[8] 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[9].*
        - 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[10].
            - 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.

---

[7] Director of National Intelligence, Assessing Russian Activities and Intentions in Recent US Elections, WWW: https://www.dni.gov/files/documents/ICA_2017_01.pdf

[8] RTL, Marine Le Pen : la Russie pousserait sa candidature, selon la DGSE , WWW: http://www.rtl.fr/actu/politique/marine-le-pen-la-russie-pousserait-sa-candidature-selon-la-dgse-7787143387

[9] Politfact, 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-/

[10] Suggested study material: Practises of campaign of French Presidential Candidate Emmanuel Macron: https://hackernoon.com/analyzing-a-counter-intelligence-cyber-operation-how-macron-just-changed-cyber-security-forever-22553abb038b

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[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

[11] To see more on government actionable stratcom capacities – see www.kremlinwatch.eu/strategy

ELECTIONS

VOTERS CAN BE DIRECTLY OR INDIRECTLY INTIMIDATED

VOTERS CAN BE BRIBED

VOTERS

VOTERS CAN BE A TARGET OF DISINFORMATION CAMPAIGN(S)

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

VOTE DELIVERY & COLLECTION & COUNT

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

PRE-ELECTORAL PROCESS

SENSITIVE FILES CAN BE HACKED AND PUBLISHED

DISINFORMATION OPERATIONS CAN BE EMPLOYED

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

ATTACK A NON-PREFERRED CANDIDATE

EUROPEAN VALUES
Protecting Freedom

CANDIDATE CAN BE SUPPORTED THROUGH HIS TEAM RECEIVING FINANCIAL BENEFITS

SUPPORT A PREFERRED CANDIDATE

CANDIDATE CAN RECEIVE INTELLIGENCE SUPPORT ON ITS OPPONENTS FROM ABROAD

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

CANDIDATE MAY BE DIRECTLY PROVIDED WITH CAMPAIGN FINANCING OR MEDIA SUPPORT