From analysis to (re)action: A response framework for FIMI threats

EEAS Stratcom – Data Team

19/03/2024
The EU’s policy framework

European Democracy Action Plan

- Refine the terminology and understanding of the threat
- Develop a common analytical framework and methodology
- Further develop the EU’s toolbox to impose costs

Common Understanding → Common assessment → Joint responses

FIMI Terminology → Analytical Methodology → FIMI Toolbox > Response Framework
The EU’s policy framework

<table>
<thead>
<tr>
<th>European Democracy Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refine the terminology and understanding of the threat</td>
</tr>
</tbody>
</table>

- **Common Understanding**
- **Common assessment**
- **Joint responses**

- **FIMI Terminology**
- **Analytical Methodology**
- **FIMI Toolbox > Response Framework**
Analytical Methodology

- A behaviour-based methodology for the analysis of FIMI and disinformation
- A framework to organise evidence collection and analysis
- Use of analytical standards as TTPs frameworks and common data models
The EU’s policy framework

<table>
<thead>
<tr>
<th>European Democracy Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refine the terminology and understanding of the threat</td>
</tr>
<tr>
<td>Develop a common analytical framework and methodology</td>
</tr>
<tr>
<td>Further develop the EU’s toolbox to impose costs</td>
</tr>
</tbody>
</table>

Common Understanding ➔ Common assessment ➔ Joint responses

- FIMI Terminology
- Analytical Methodology
- FIMI Toolbox > Response Framework
FIMI toolbox
Response Framework to FIMI Threats

How to connect FIMI analysis to counteractions (FIMI Toolbox)?
Elements of the Response Framework to tackle FIMI threats

The successful implementation of counters requires...

**Cross-domain Analysis**
Integration of FIMI analysis with other data sources of analysis.

**Adapted Countermeasures**
Pre-identification of responses based on the attack pattern and activation time.

**Mechanisms for collective response**
Increased community collaboration and protocols to activate responses.

*What do we need to counter?*
*How can we counter?*
*Who can help us to counter?*
*How do put in place the counters?*
Preventing, deterring and responding to FIMI is a long-term process that combines preventive and long-term activities. The Defence Arsenal should be composed by countermeasures that are activated before, during and after an incident.

Activities across the different phases can be combined and used complementarily.
How to apply the Response Framework in practice?

• **Real-case scenario:** Election-related FIMI

• **Available data:** 33 FIMI incidents in election contexts between 2022 and 2023

• **Scope:** applying the Response Framework to elections and creating a workflow to analyse and respond to election-related FIMI incidents
# Types of FIMI Threats targeting Elections

<table>
<thead>
<tr>
<th>Threats to information consumption</th>
<th>Threats affecting citizen’s ability to vote</th>
<th>Threats targeting candidates and political parties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control the information flow</td>
<td>Promoting abstention (voluntary/involuntary)</td>
<td>Personal attacks</td>
</tr>
<tr>
<td>Generation of distrust</td>
<td>Promoting invalid votes</td>
<td>Promotion of certain political options</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threats to the trust in democracy</th>
<th>Threats election-related infrastructures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amplification of alleged/real irregularities</td>
<td>Hybrid incidents (Cyber/FIMI)</td>
</tr>
<tr>
<td>Risk of affecting turnout</td>
<td>Exploiting perceived risks over real risks to elections</td>
</tr>
</tbody>
</table>
Timeline of attacks targeting elections

A cross case-analysis shows that FIMI actors begin to prepare their operations to target elections well in advance and **gradually intensify** their attacks.
Crafting possible Responses workflow to Election-related FIMI

**PHASE 1:** MONTHS BEFORE THE ELECTIONS

**INTEGRATION:**
- Capability reinforcement.
- Collective knowledge.
- Review response strategies.

**IDENTIFICATION & PREPARATION:**
- Risk and vulnerabilities assessment.
- Building partnerships.
- Preparation of the tools.
- Definition of a Response Action Plan for elections.

**REACTIVE RESPONSES:**
- Activation of Response Action Plan.
- Risk assessment and choice of response.

**DETECTION:**
- Threat detection.
- Evidence collection, analysis & sharing.
- Activation of alert mechanism.

**PHASE 2 & 3:** ONE MONTH AND 72 HOURS BEFORE THE ELECTIONS

**PHASE 4:** POST-ELECTION PERIOD