

Challenges in Digital Democracy: Foreign Interferences

Fatih Yilmaz, Derek Metivier
Beyond the Horizon ISSG



Components

Chapter 2: Digital Democracy

Chapter 3: Online Participation

Chapter 4: Open Governance

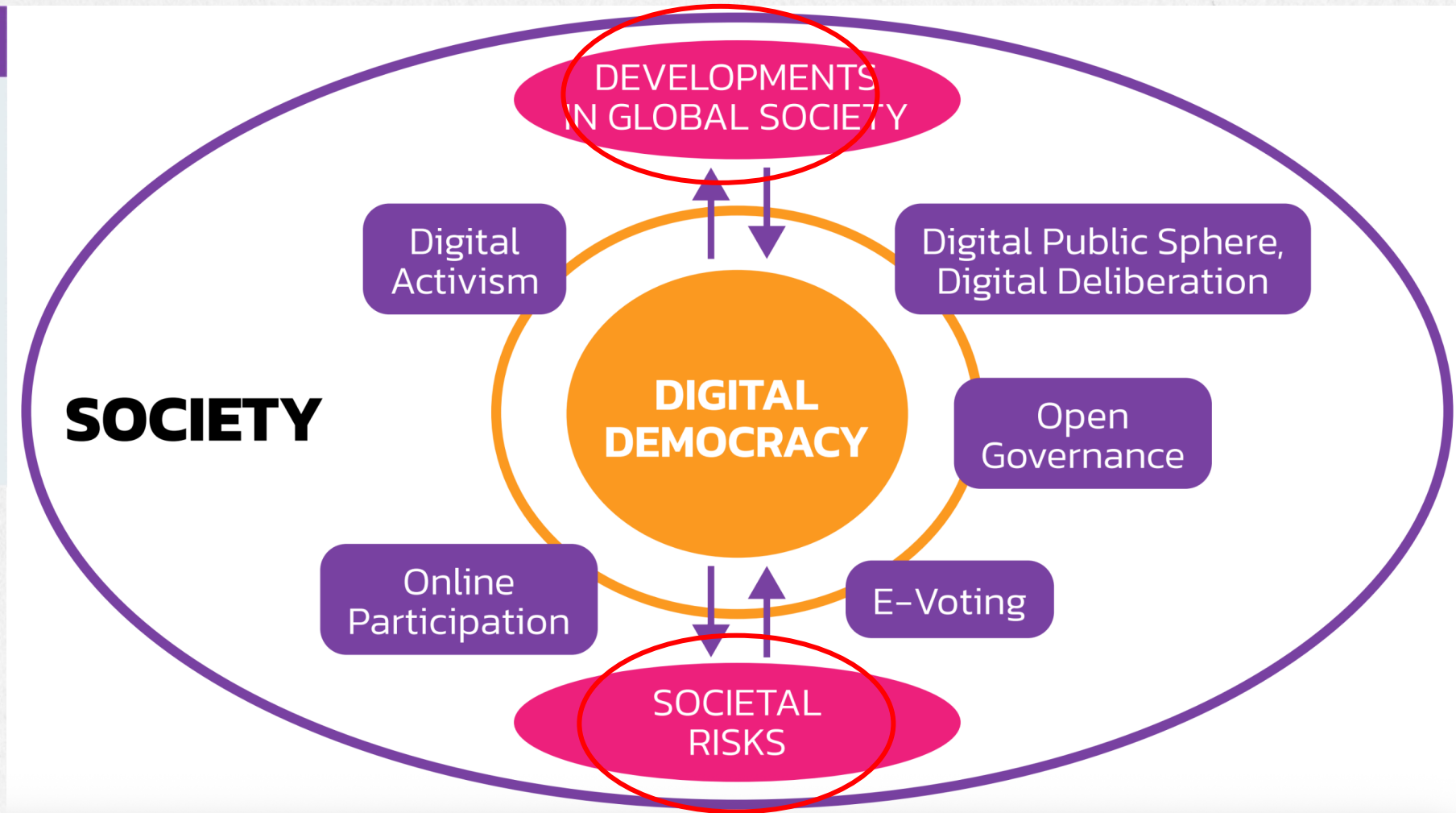
Chapter 5: Digital Activism

Chapter 6: e-Voting

➔ **Chapter 7:** Global Trends that Influence Digital Democracy

➔ **Chapter 8:** Foreign Interferences in Democracy

+ 10 recommendations



The **aspects** and **challenges** of digital democracy covered in this report

☑ Digital Exclusion

Resulting from socio-economic, geographic, and infrastructural disparities

☑ Misinformation & Foreign interference

Undermining informed decision-making and civic trust

☑ Privacy and Cybersecurity Concerns

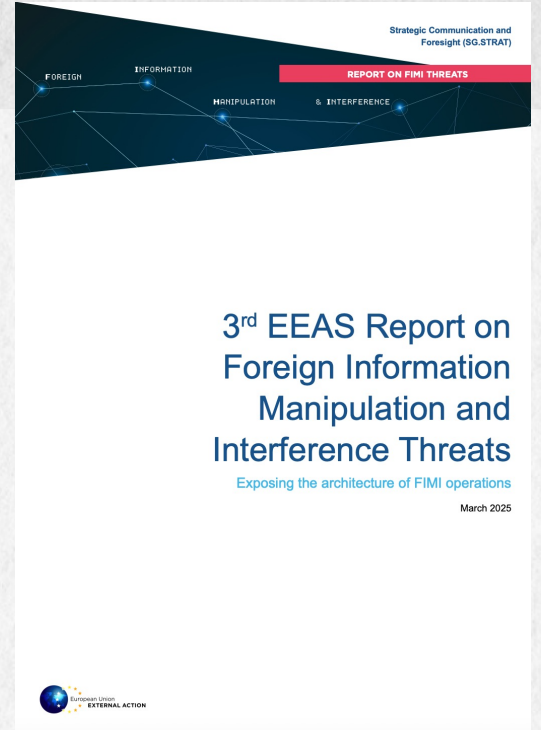
The reliance on digital platforms raises concerns about data protection, surveillance, and cyber threats.

☑ Risks of Algorithmic Bias and Surveillance

The increasing reliance on AI and data analytics in governance raises ethical concerns.

Objective and Introduction

- ☑️Analyses foreign interference in digital democratic processes through a structured multi-case study approach
- ☑️Draws upon academic and institutional definitions to support the tactical analysis
- ☑️Applies a novel three-level analytical framework of digital democracy
- ☑️An original dataset of 109 FIMI cases from Europe and beyond was created to contribute to a typology of FIMI tactics in the digital sphere



“FIMI” Definition

- ☑ “Foreign Information Manipulation and Interference (FIMI) describes a mostly **non-illegal pattern of behaviour** that threatens or has the **potential to negatively impact values, procedures and political processes**.
- ☑ Such activity is **manipulative** in character, conducted in an **intentional and coordinated** manner.
- ☑ **Actors** of such activity can be **state or non-state actors**, including their **proxies** inside and outside of their own territory.”

EEAS

FIMI Continued

- ☑ FIMI actions are frequently **executed in the legal grey zone**, below the threshold of outright illegality, and are characterised by their **intentional, manipulative, and covert nature**
- ☑ Actors in this space operate at the intersection of **geopolitical rivalry, digital media systems, and democratic fragility** which requires a multidimensional response across governance, civil society and platform governance structures
- ☑ We define **4 principal tactic clusters** commonly used by malign foreign actors in digital spaces, applying the lens of **technology, culture, and human behaviour** (3 vectors of manipulation)

FIMI Clusters by Tactical Approach in the Digital Domain

FIMI Cluster	Definition	Key Distinction
Digital Disinformation and Manipulated Content	The creation or alteration of digital content (text, images, audio, video) to intentionally deceive or mislead audiences.	Focuses on the content itself (either fabricated or distorted) regardless of how it's distributed. Dimension: Culture
Cyber-Enabled Information Operations	Use of cyber tools (e.g., hacking, data leaks, DDoS) to access, alter, or disrupt digital information and platforms to achieve influence.	Relies on technical intrusion or disruption rather than narrative creation. Dimension: Technology
Social media and Platform Exploitation	Manipulation of social media algorithms , user behaviour, and trends to artificially amplify or suppress content and opinions.	Focuses on manipulating behaviour rather than content or infrastructure. Dimension: Human (behaviour)
Digital Psychological Operations	Coordinated campaigns using digital tools to influence perceptions, create confusion, and exploit emotional or societal vulnerabilities.	Emphasises emotional and cognitive manipulation , often using other tactics as tools. Dimension: Integrate all 3

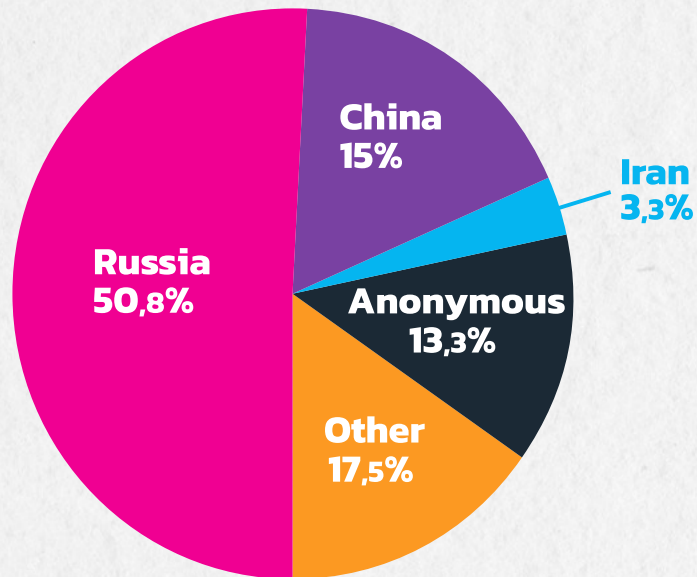
Case Study Overview

- ☑ This analysis draws upon a structured dataset of **109 verified cases of (digital) FIMI** compiled **between 2020 and early 2025**
- ☑ Cases were gathered from a combination of:
 - ❑ Official institutional reports
 - ❑ Academic and think tank studies
 - ❑ Open-source intelligence (OSINT)
 - ❑ Corporate investigations
- ☑ To qualify for inclusion, each case had to be perpetrated **by a foreign actor**, applying **coordination and inauthenticity** alongside the **use of digital tools** to influence and/or undermine democratic institutions

FIMI Case Collection

Cases by Actor

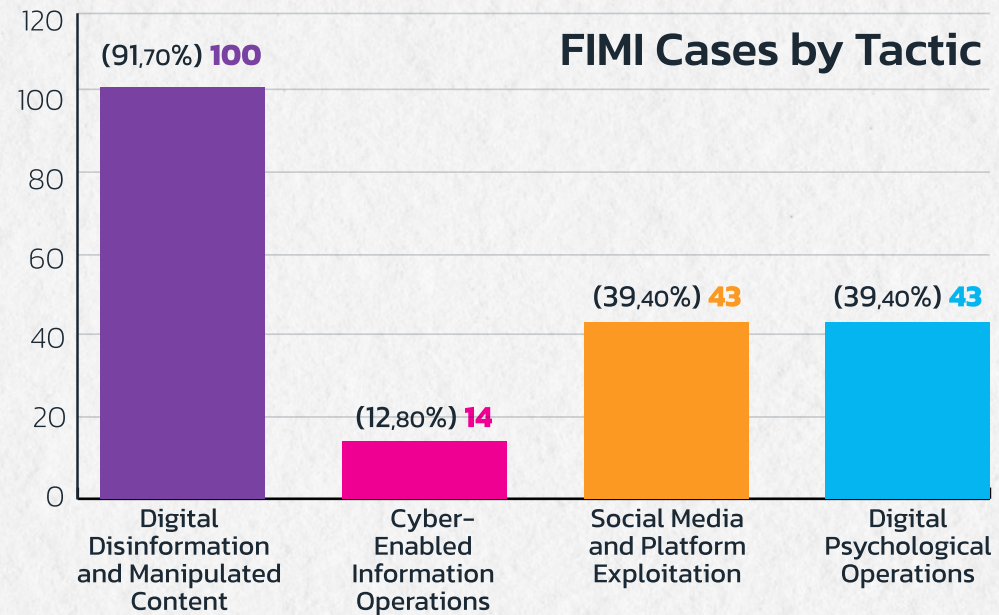
109 Total Cases



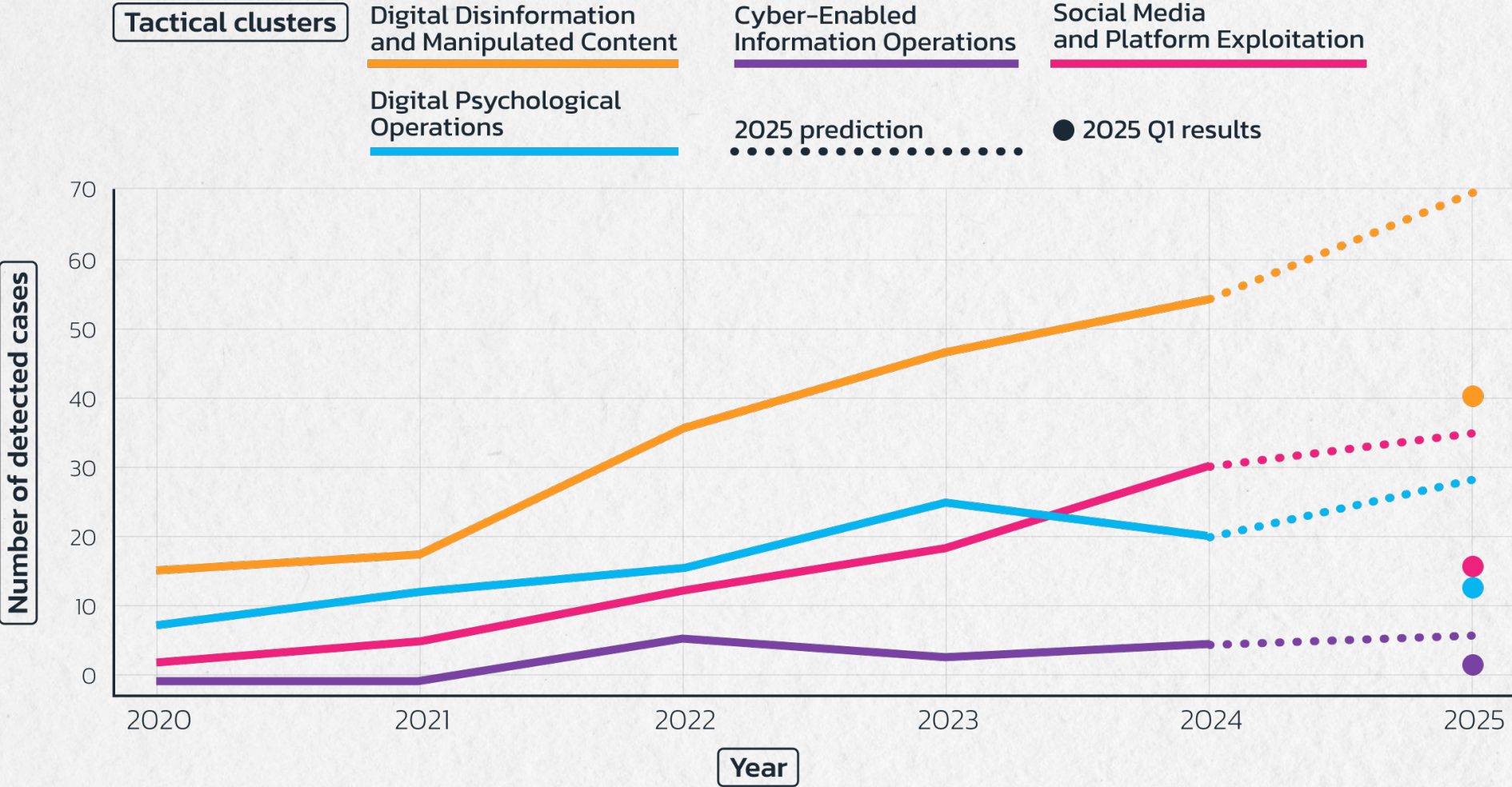
Some of the collected FIMI cases involved multiple actors.

Cases by Tactic

- Digital Disinformation and Manipulated Content: **100** (91,70%)
- Cyber-Enabled Information Operations: **14** (12,80%)
- Social Media and Platform Exploitation: **43** (39,40%)
- Digital Psychological Operations: **43** (39,40%)



FIMI Incidents by Tactical Cluster over Time

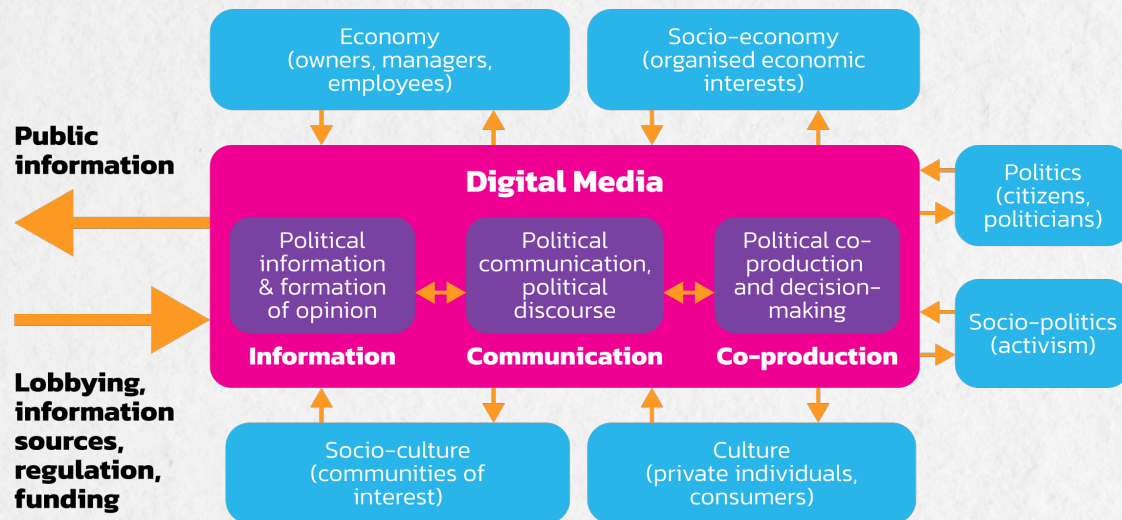


Levels of Information Processing in Digital Democracy

☑ Digital democracy involves the use of digital media in the practice of democracy, refers to the **digital mediation of democracy**.

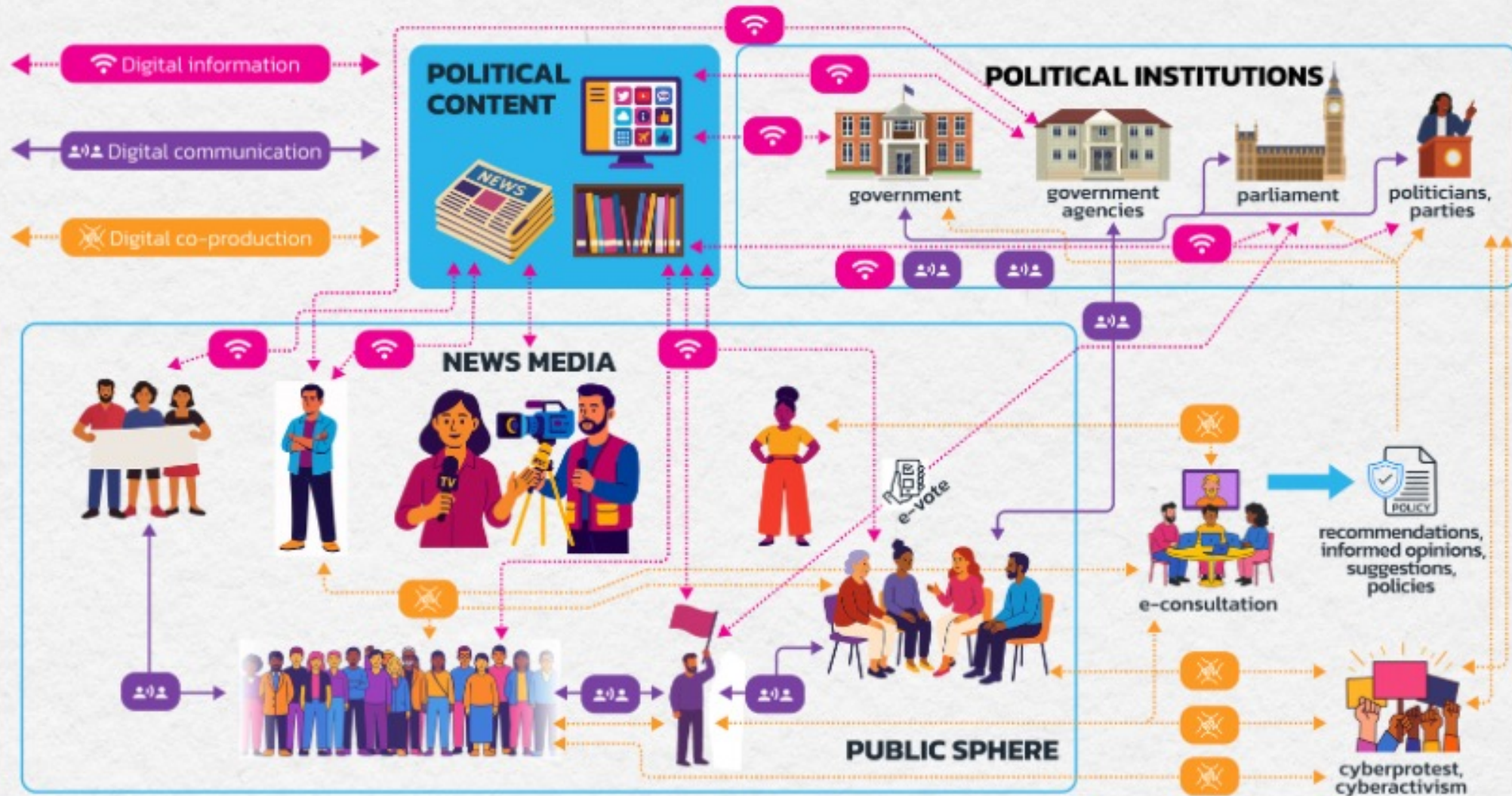
Digital democracy functions through the three steps in the process of human action:

- ☑ **Political Information** (e-information, e- deliberation)
- ☑ **Political Communication** (e-campaigning, e-petitions)
- ☑ **Political Co-production** (e-consultation, e- participatory budgeting, e-voting)

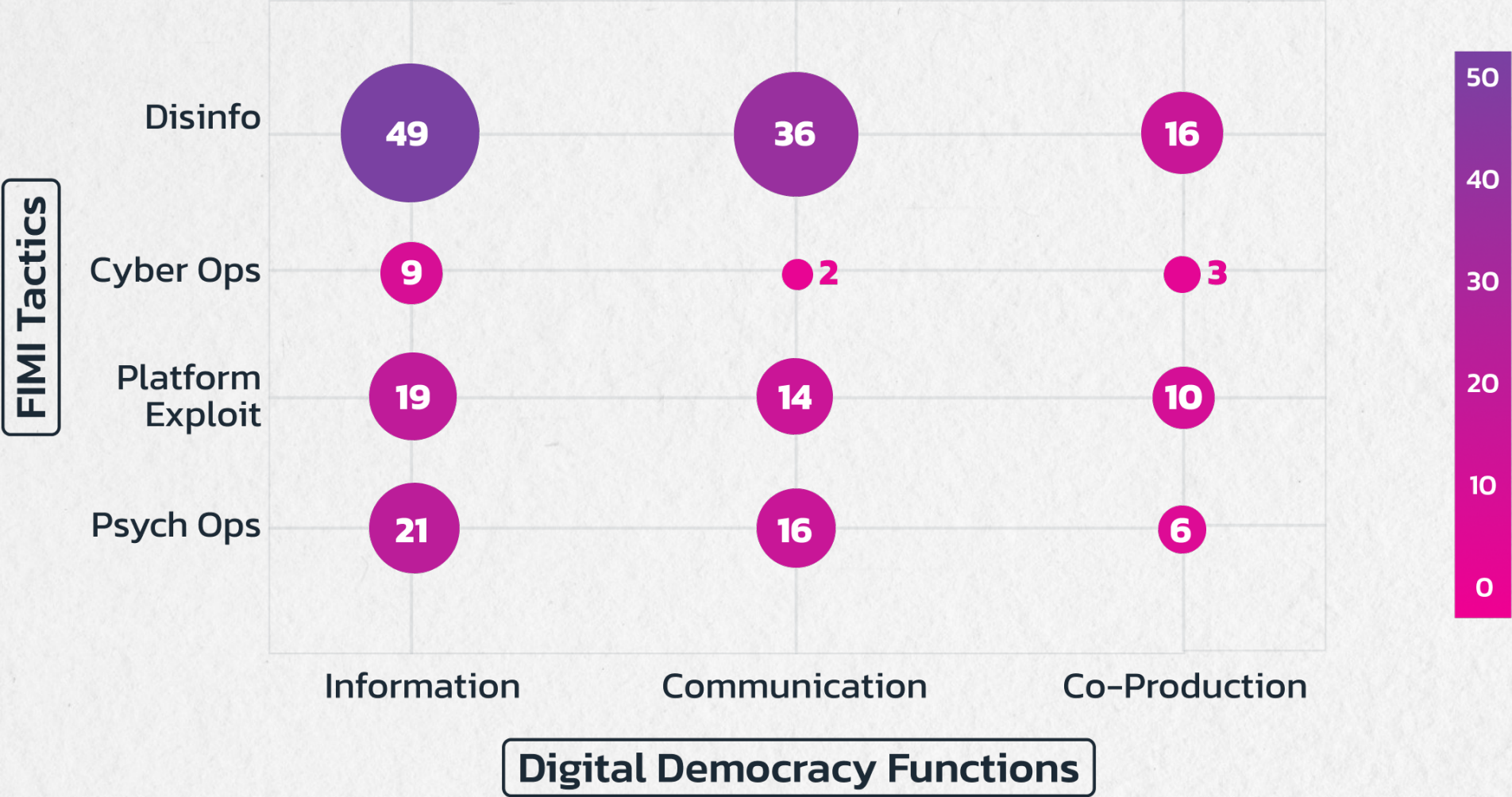


(Fuchs 2020; Hofkirchner 2012)

A Model of Digital Democracy



FIMI Incidents Heatmap (per tactic and democracy function)



FIMI Impacts on Digital Democracy Levels (Analysis)

FIMI Tactics / Digital Democ. functions	Digital Disinfo and Manipulated Content	Cyber-Enabled Information Operations	Social Media and Platform Exploitation	Digital Psychological Operations
Information <ul style="list-style-type: none"> e-information 	<p>Injects falsehoods into the information space, hindering the access to accurate information for citizens</p> <p><u>Operation Matryoshka</u> <u>Recent Reliable News (RRN)</u></p>	<p>Targets information platforms via hacks or data leaks disrupting the availability of digital information</p> <p><u>Cyberattack on NXP</u> <u>Operation Cuckoo bees</u></p>	<p>Algorithmic manipulation (e.g., bot amplification) creates information overload, drowning out legitimate monitoring efforts</p> <p><u>Doppelganger Case</u> <u>War on Fakes</u></p>	<p>Polarizes online discussions, reduces trust and generates fear in the information space to turn citizens against certain demographics</p> <p><u>Paperwall Case</u> <u>Killnet, Disinfo on migrants in ES</u></p>
Communication <ul style="list-style-type: none"> e-campaigning e-petitions e-deliberation 	<p>Fabricated narratives enter public discourse and impact which issues are prioritized</p> <p><u>Operation EcoBoost</u> <u>Gov't Child removal in Germany</u></p>	<p>Shifts narratives in domestic agenda setting through data leaks</p> <p><u>Iranian Cyber Attack on Albanian Gov Network</u></p>	<p>Amplifies polarizing topics via bots or fake engagement, artificially bringing issues into mainstream visibility</p> <p><u>Chinese Partnerships Albania</u> <u>Telegram based inf. networks</u></p>	<p>Promotes narratives on sensitive issues to shift public attention to foreign strategic interests</p> <p><u>Pro-Russian Narratives with Romanian Far-Right</u></p>
Co-production <ul style="list-style-type: none"> e-consultation, e-participatory budgeting e-voting 	<p>Misleads or polarizes voters which can skew election and policy outcomes</p> <p><u>Cambridge Analytica</u> <u>FIMI in 2024 European Elections</u></p>	<p>Malign attacks (DDoS, hacking, etc.) disrupt e-voting and other digital platforms for decision-making</p> <p><u>Russian Interference in Italian Energy Sector - 2022 Elections</u></p>	<p>Makes use of bots or troll accounts to show support or dissent for issues, causing a perceived consensus among the public</p> <p><u>Russian FIMI in Moldovan Elections</u></p>	<p>Makes use of fear or identity-driven messages to sway how citizens vote or make decisions</p> <p><u>Doppelganger Operations in Polish Presidential Elections</u> <u>2024 US Presidential Elections</u></p>

FIMI Digital Democracy Impact Matrix

Operation Matryoshka

- © This Matryoshka campaign is pro-Russian information campaign uncovered by VIGINUM.
- © Their narratives depicted Zelensky as a beggar and war criminal, Ukrainian asylum seekers in Europe as exploitive, and the Paris Olympics as unsafe due to threats of terrorism.
- © Undermines the credibility of media outlets, public personalities, and fact-checking units.

(Leveque 2024, 18-19)

Digital Disinformation and Manipulated Content

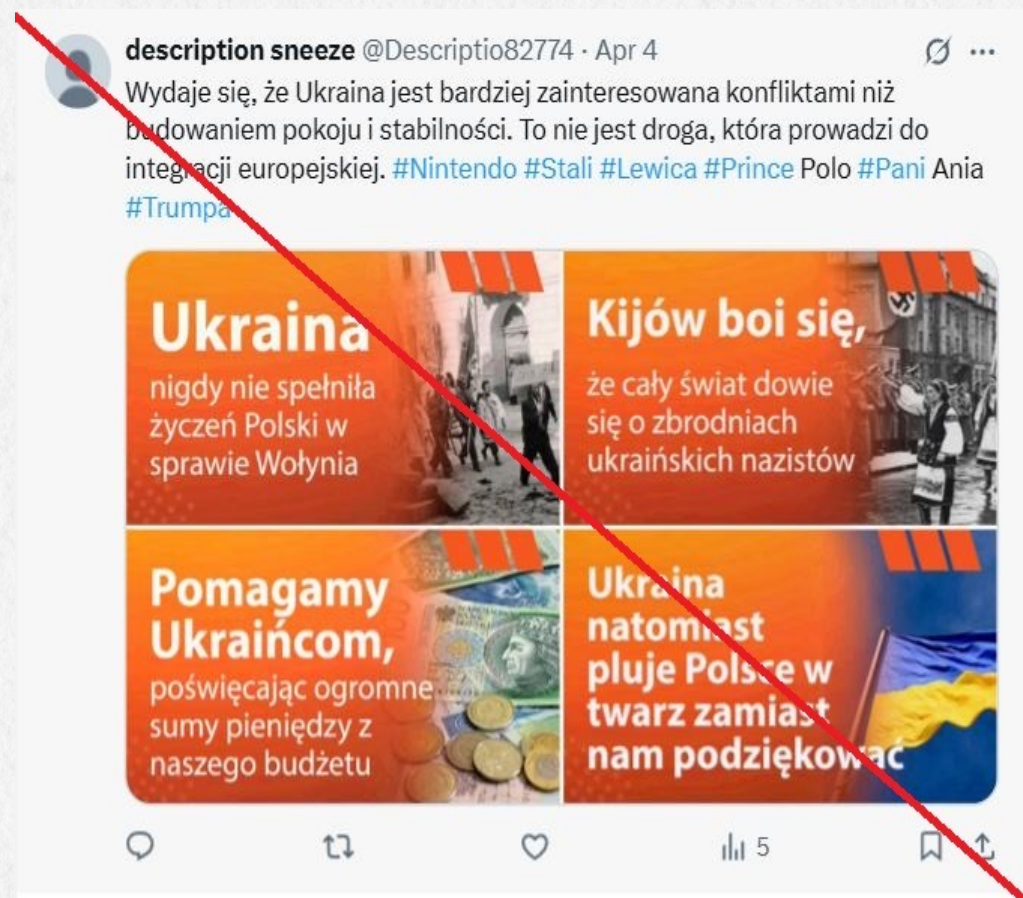


Doppelganger Operations in Polish Presidential Elections

- Before the 2025 Polish presidential election, a Doppelganger network disseminated 279 posts on X to interfere with the electoral process
- The operation used 43 articles from 13 different Polish publications which generated 1,547,221 views and 256,549 shares, but the shares are believed to be from inauthentic accounts.

(Nazari, Voltsichina, and Kryvenko 2025)

Digital Psychological Operations



Countermeasures

- ☑ There have been many efforts across three levels of society to address the challenges and mitigate the impacts of FIMI:
 - ❑ **EU-Level:** European Democracy Action Plan (EDAP), the Rapid Alert System (RAS)
 - ❑ **National-Level:** VIGINUM in France, the Federal Office for Information Security (BSI) in Germany,
 - ❑ **Local-Level:** VIGINUM partnerships with local municipalities, increased cybersecurity measures on digital participatory platforms in Milan and Rome

Recommendations

☑ In light of the dangers of FIMI to democracy in the digital sphere, we propose five recommendations:

- ❑ 1 - Build Multilevel Resilience Across Democratic Functions
- ❑ 2 - Centre Trust, Transparency, and Cognitive Integrity in Platform Design
- ❑ 3 - Embed Detection and Response to Hybrid Interference
- ❑ 4 - Design for Deliberation, Not Just Expression
- ❑ 5 - Strengthen Local-Level Defences as Democratic Frontlines



Thank you!

Let's keep in touch.

innovade-democracy.eu

fatih.yilmaz@behorizon.org



Funded by
the European Union