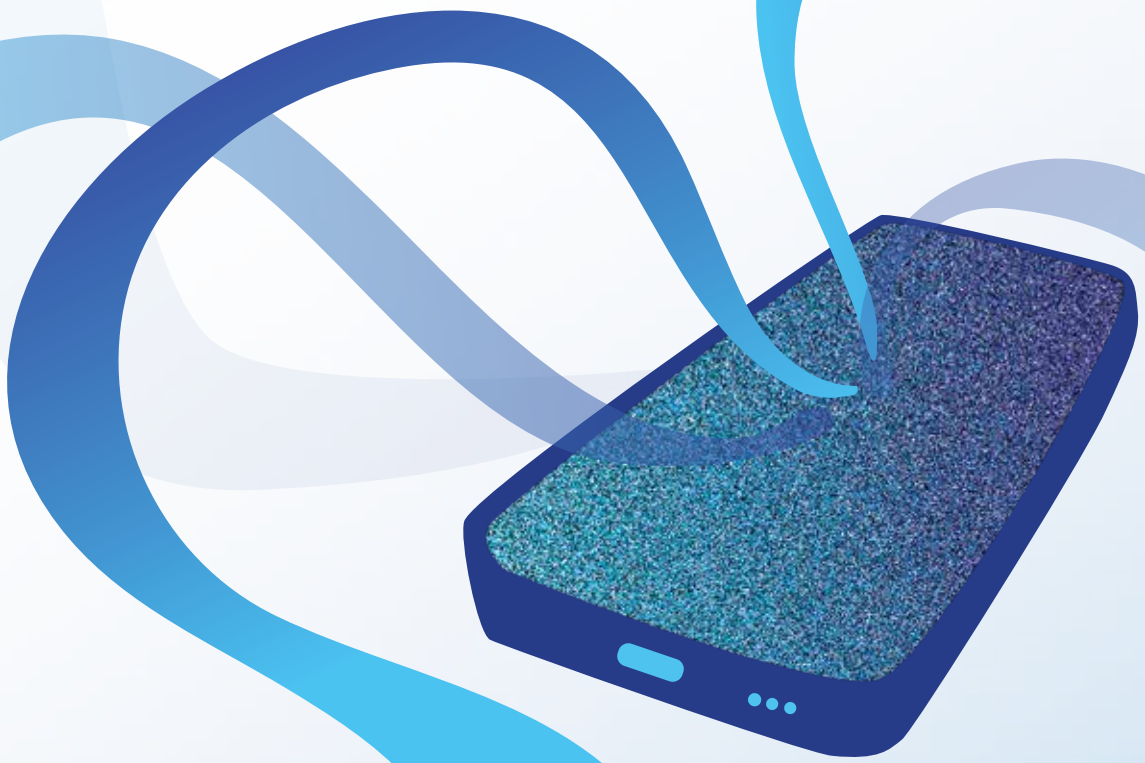
SENTiNEL
Strengthening Youth Resilience Against Information Manipulation

# SENTINEL: Navigating Information Manipulation & Foreign Interference

Your phone's feed has become a battlefield — and you're right in the middle of it. Every day, millions of young Europeans scroll through content shaped by hidden algorithms, and mixed in with the memes and music are carefully designed attempts to mess with how you see the world, trigger your emotions, and damage democracy from the inside.

Knowing how to read your media isn't just a nice-to-have — it's one of the most important skills you can have right now. When fake news spreads, people stop trusting each other and the institutions around them. That's why youth workers play a key role: helping young people go from being passive scrollers to active, critical thinkers who can spot what's real and what's not.



# The Truth Has Been Hacked

Before you can spot manipulation, it helps to understand what "truth" actually means — and how it can be twisted. Philosophers have described four ways we decide if something is true, and bad actors know how to hack every single one of them:

| Philosophical theory | Core concept definition | Vulnerability to manipulation |
|---|---|---|
| **Correspondence theory** | A statement is true if it directly corresponds to an objective, observable empirical reality. | Bypassed entirely by malicious operators who substitute emotional appeals for physical evidence. |
| **Coherence theory** | A statement is true if it fits perfectly within an already established, logical system of beliefs. | Exploited inside online echo chambers where false claims are accepted because they align with pre-existing beliefs. |
| **Consensus theory** | A statement is true if a specific community or group collectively agrees that it is true. | Gamed via synthetic engagement metrics, viral likes, shares, and coordinated bot networks to fake social validity. |
| **Pragmatic theory** | A concept is treated as true if practicing it produces useful, concrete, and desired outcomes. | Weaponised in influence operations; if a false narrative achieves a geopolitical objective, its accuracy is deemed irrelevant. |

We live in a **post-truth world** — where how something makes you feel can matter more than whether it's actually true. Manipulators take full advantage of this: they craft stories that feel emotionally right and seem widely shared, even when the facts simply aren't there.

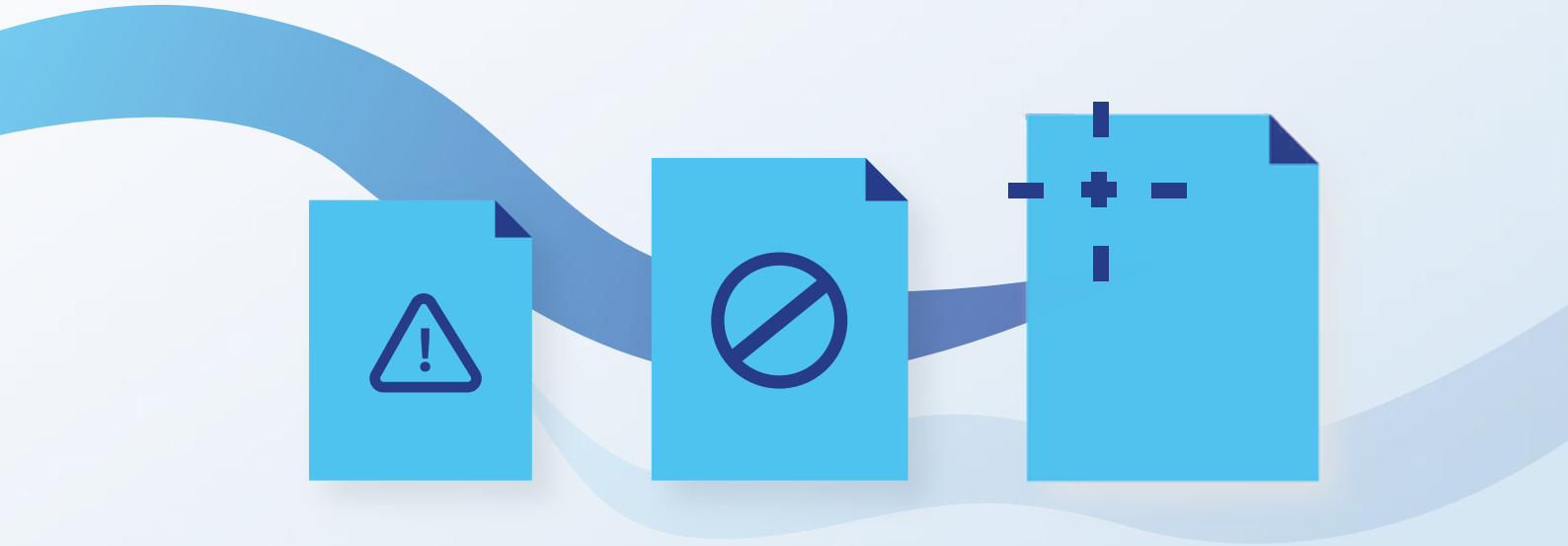
## Not All Lies Are the Same

To navigate the digital sphere effectively, standard definitions are used to categorise the variants of harmful content:

1. **Misinformation:** Verifiably false, inaccurate, or misleading information that is created and disseminated without harmful intent. This encompasses honest journalistic mistakes, misinformed rumors passed between family members in good faith, or outdated statistics. The real-world impact can still be harmful, but there is no malicious agenda driving it.

2. **Disinformation:** Verifiably false, manipulated, or fabricated content that is intentionally engineered, packaged, and distributed for economic profit, political leverage, or to deliberately deceive the public. It is designed to inflict public harm, jeopardize democratic decision-making, and compromise national or public security.

3. **Malinformation:** Verifiably accurate, real-world information that is deliberately weaponised with malicious intent to cause genuine harm to individuals, groups, or institutions. Examples include doxxing (exposing private personal files), leaking confidential personal communication, or pulling a completely genuine, historical statement entirely out of its original context to systematically ruin a person's reputation.



## How Lies Go Viral

Fake news doesn't just spread by accident — the apps you use are built in a way that makes it happen. Algorithms push content that gets reactions, and nothing gets more reactions than outrage, fear, or drama. Thoughtful, accurate content simply doesn't perform as well, so platforms end up rewarding sensationalism. The truth is blunt: these companies don't profit from you knowing the facts — they profit from you staying glued to the screen. And since anger and anxiety keep you scrolling longer, the algorithm keeps feeding you more of it.

Disinformation moves across different platforms in distinct ways:

- **X (formerly Twitter):** Acts as the rapid ignition chamber, using automated bots, trends, and hashtags to inject narratives into echo chambers.
- **TikTok:** Translates the core message into high-impact audiovisual trends, utilizing charismatic micro-influencers and emotive background music to bypass critical thinking.
- **Facebook:** Functions as the community embedding network, where content spreads through private groups and local peer connections.
- **YouTube:** Serves as the long-form validation platform, providing pseudo-documentaries and fake experts to strengthen conspiracy logic.

## Don't Share Before You Check

So how do you actually call out fake content? Here are two practical tools you can use to check any post, article, or video you come across — no expertise needed. Together, the CRAAP Framework and the SIFT Protocol give you a fast, reliable way to assess what's real and what's not.

## The CRAAP Evaluation Framework

- **C - Currency (the timeliness):** Assess when the information was published, posted, or updated. Is an older, outdated article being deceptively recirculated to fake relevancy during a current active crisis?
- **R - Relevance (the importance):** Examine whether the material satisfies your exact informational needs. Who is the intended target audience? Is the content written as clickbait to trigger outrage rather than provide deep substance?
- **A - Authority (the source):** Verify the identity, credentials, and background of the author, creator, or publisher. Is the URL mimicking a reputable domain via typosquatting?
- **A - Accuracy (the reliability):** Trace the origins of the evidence. Is the claim supported by verifiable data or peer-reviewed documentation? Can you cross-verify this data across independent sources?
- **P - Purpose (the motivation):** Determine why the content exists. Is it designed to inform, entertain, sell a product, persuade, or intentionally spark extreme political polarisation? Is it state-sponsored propaganda?

## The SIFT Protocol

1. **S - Stop:** The moment a post triggers an intense emotional reaction (shock, intense anger, or deep confirmation bias), freeze. Do not share, comment, or interact until verification is complete.

2. **I - Investigate the source:** Look outside the channel. Move beyond their "About Us" page and look for independent, external sources that report about the publisher's background and actions.

3. **F - Find better coverage:** Seek out consensus. Determine if reputable, independent journalistic organisations are covering the same event, or if the claim is completely isolated to fringe channels.

4. **T - Trace claims and media to the original context:** Track down the primary material. Is an unedited quote or a short video snippet being sliced from a comprehensive interview to entirely distort its original intent?

# Beat Manipulation Before It Beats You

Here's the problem with fact-checking: by the time a fake article gets debunked, millions of people have already seen it — and the correction rarely reaches them. Emotional, visual stories stick in a way that dry corrections don't. That's why the focus has shifted to **prebunking**, which is based on **inoculation theory**. Think of it like a vaccine: instead of waiting until you get sick, your body learns to recognize the virus before it attacks. The same principle applies here — if you learn how manipulation tactics work before you encounter them, you're far less likely to fall for them when they appear in your actual feed.

## Six Ways You're Being Manipulated Right Now

1. **Impersonation:** Fabricating cloned websites, stealing official logos, or creating fake profiles of verified journalists to exploit institutional authority.

2. **Emotion (Emotional Weaponisation):** Bypassing logical critique by infusing content with intense emotional triggers—such as moral outrage, fear, or acute empathy—to drive immediate sharing.

3. **Polarization:** Identifying a legitimate societal disagreement and driving it to toxic extremes, forcing people into rigid, hostile camps and destroying the possibility of compromise.

4. **Conspiracy Theories:** Weaving unprovable narratives that explain random global crises as the secret, malicious plots of a hidden global elite.

5. **Discrediting:** Launching coordinated smear campaigns against authoritative sources or fact-checkers to destroy their credibility and deflect attention from their findings.

6. **Trolling:** Intentionally provoking and harassing online communities to sabotage constructive discussions, exhaust activists, and pollute public debate.

# State-Sponsored Lies: What Is FIMI?

Sometimes the manipulation isn't random — it's organised by governments trying to mess with other countries' democracies. This is called **Foreign Information Manipulation and Interference (FIMI)**. The EU's foreign policy body, the European External Action Service (EEAS), defines FIMI as a coordinated, deliberate pattern of behavior — run by state or non-state actors — that is designed to undermine the values, systems, and political processes of another country. Much of it is technically legal, which makes it even harder to fight.

## How Experts Analyse FIMI

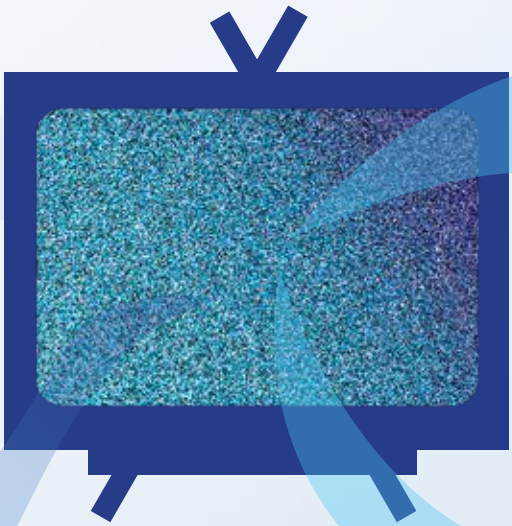
The ABCDE framework is a systematic analytical methodology adopted by the EEAS to identify, track, and counteract FIMI:

- **Actor:** Determining the origin and infrastructure behind the campaign (e.g., state intelligence networks, contracted commercial PR firms, state-controlled media, or ideological proxies).
- **Behavior:** Evaluating the exact tactics, techniques, and procedures deployed. This includes automated bot swarms, website cloning, search engine manipulation, and coordinated inauthentic behavior (networks of fake or hidden accounts, automated bots, and websites working together to deceive the public, manipulate information, and spread disinformation)
- **Content:** Decoupling the narrative theme to see how it exploits pre-existing societal vulnerabilities, local disputes, or cultural divides.
- **Degree:** Measuring the scale, velocity, and multi-platform distribution of the campaign.
- **Effect:** Evaluating the real-world impact (e.g., polarisation of voters, street protests, or erosion of institutional public trust).

## Inside a State-Backed Influence Operation

Various actors can take part in a state-backed FIMI operation (non-exhaustive list):

- **Troll Farm Operators:** Salaried personnel managing extensive networks of fake profiles to flood comments and amplify division.
- **Proxy Site Managers:** Running seemingly independent local news outlets that launder state narratives under clean branding.
- **Influencers for Hire:** Monetised creators paid to deliver talking points, leveraging their organic credibility with young audiences.
- **Bot Controllers:** Deploying scripts to execute coordinated inauthentic behavior, bypassing platform ranking systems within seconds of publication.
- **Unwitting Amplifiers:** Everyday citizens who share content due to emotional manipulation, amplifying the campaign organically.



## Four FIMI Operations Exposed

This isn't theory — FIMI is happening right now, targeting people across Europe, including you. Here are four real, documented campaigns to show you what it actually looks like:

1. **Doppelgänger (Origin: Russia):** A massive, multi-platform operation that clones exact replicas of mainstream news providers (such as The Guardian, Bild, Spiegel) and official government web pages. Threat actors purchase lookalike domain names, copy the layout, and publish fake articles. They buy thousands of short-lived social media ads to push these links directly into users' feeds. Among other false claims, these articles frame Ukraine as a failed state and suggest that European sanctions against Russia will cause immediate economic ruin.

2. **Portal Kombat (Origin: Russia)**: A structured digital infrastructure consisting of at least 193 localized information portals (such as the Pravda news ecosystem). The network automates content production by ingesting articles from Russian state media, translating them via software, and publishing them locally. They use advanced Search Engine Optimization (SEO) to manipulate search queries across Europe, aiming to polarise public debates and undermine support for Ukrainian sovereignty.

3. **Matryoshka/Overload (Origin: Russia):** A tactical operation designed to target and exhaust the defensive capabilities of newsrooms, fact-checking networks, and public figures. Fake accounts directly tag fact-checkers across platforms with thousands of requests to verify fabricated claims. They misuse the official logos of top-tier media and elite universities, combining them with AI-generated synthetic media and audio deepfakes. The goal is to overload the investigative capacity of defenders through information flooding while using their responses to further publicise false narratives.

4. **Paperwall (Origin: China):** An expansive, localised influence operation comprising at least 123 websites operating across 30 countries across Europe, Asia, and South America. The websites mirror the exact visual design, layout, and language of authentic local news portals to inject pro-Chinese political propaganda, favorable state narratives, and targeted ad hominem attacks against critics of the Chinese government directly into local information ecosystems. Actors bury malicious or defamatory political articles within a massive, constant stream of completely benign commercial press releases and lifestyle news.

# Go Deeper: Tools & Resources

Want to keep digging? Here are some of the best free resources available to help young people — and the people who work with them — stay sharp and informed:

- **EU vs Disinfo:** the flagship project of the EEAS's East StratCom Task Force. It was established in 2015 to better forecast, address, and respond to the Russian Federation's ongoing disinformation campaigns affecting the EU, its Member States, and countries in the shared neighbourhood. EUvsDisinfo's core objective is to increase public awareness and understanding of the Kremlin's disinformation operations, and to help citizens in Europe and beyond develop resistance to digital information and media manipulation.

- **EEAS Threat Reports on FIMI (2023–2026):** annual strategy documents published by the EEAS tracking threat actors, techniques, and the framework for networked defense.

- **European Parliamentary Research Service Briefings**: Policy-focused research papers covering Information Manipulation in the Age of AI, Media Literacy, and Children and Deepfakes.

- **EU DisinfoLab & Viginum Technical Investigations**: Exhaustive technical deep-dives mapping the infrastructure fingerprints of campaigns like Doppelgänger and Portal Kombat.

**Become a Sentinel.**
**Question the Feed.**
**Protect the Truth.**

This material has been made by Udruga Prizma in the scope of Erasmus+ funded training course **Sentinel: Strengthening Youth Resilience Against Information Manipulation**. The author owns no copyright over the material and has used the mentioned free resources.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Agency for Mobility and EU Programmes. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

Udruga Prizma

SENTiNEL
Strengthening Youth Resilience Against Information Manipulation