



National Cognitive Defense: How to Protect Italy from Information Influence Operations

Published on 21/08/2026

In the current landscape of global security, a country's defense is not just about **territorial borders** or **protection of computer data**. There is a real "informational front" where so-called **cognitive influence operations** are conducted. The objective of these campaigns — systematically coordinated by the **Russian Federation** — is not simply to spread false news, but to **divide public opinion**, **undermine trust in institutions** and **weaken Italy's alliance** with its European and Euro-Atlantic partners.

To ensure true **democratic resilience**, Italy needs a national strategy organized around four main pillars: **institutional coordination**, **detection technology**, **cultural prevention** and **citizen training**.

A Unified Institutional "Direction"

To counter attacks in the informational domain, isolated actions are not enough, but a **central state coordination**:

- **Rapid Response Center for Informational Threats:** Creation of a structure coordinated by the **Office of the Prime Minister** and **Intelligence (DIS)** capable of timely monitoring and labeling **foreign interference** in public debate.
- **International Collaboration:** Full integration with the **European External Action Service (EEAS)** of the EU and with **NATO centers of excellence** dedicated to countering hybrid threats.

Monitoring and Blocking Automated Networks

Modern propaganda uses **automation tools**, **fake profiles (bots)** and **Generative Artificial Intelligence** to create extremely credible content and visual clones:

- **AI-Based Early Warning Systems:** Adoption of algorithms to track the artificial creation of viral campaigns, identifying the creation of **clone sites of Italian newspapers** that spread made-up news (technique known as **Doppelgänger**).
- **Transparency of Digital Platforms:** Strict enforcement of the European **Digital Services Act (DSA)**, imposing the **timely removal of fake profiles** and coordinated manipulative campaigns.

Informal Prevention: "Prebunking"

Refuting false news after it has already spread has limited effectiveness. The best strategy is **prevention**:

- **Explaining Techniques Before They Are Used (Prebunking):** Informing the population about **how the psychological levers of propaganda work** (use of outrage, fake experts, altered images) before the campaign goes online.
- **Clear and Timely Institutional Communication:** Filling information gaps during sensitive moments (elections or international crises) with **reliable and transparent data**, preventing them from being occupied by enemy propaganda.

Digital Education and Citizen Engagement

The citizen must not be merely a passive subject, but the **first line of defense**:

- **Media Literacy:** Introduction in **schools** and in **Public Administration** of modules dedicated to **critical analysis of sources** and verification of visual and text content generated by AI.
- **Support for Investigative Journalism:** Promotion of **high standards of source verification** and support for researchers and analysts engaged in tracking foreign interference.

Official Sources and Documentary References

1. **European Union - European External Action Service (EEAS):***Reports on Foreign Information Manipulation and Interference (FIMI) Threats* (Official EU reports on tracking foreign information manipulation).
2. **European Commission:***EU Code of Practice on Disinformation and Digital Services Act (DSA)* (Regulations and codes of conduct for informational transparency and counter-disinformation).
3. **EUvsDisinfo:** European Union project dedicated to the detection and cataloging of **disinformation campaigns by the Russian Federation**.
4. **NATO Strategic Communications Centre of Excellence (CoE):** Strategic studies dedicated to **psychological warfare, influence operations** and **cognitive defense**.
5. **Information System for the Security of the Republic (DIS / Italian Government):***Annual Report on Information Policy for Security* (Analysis of hybrid threats and disinformation targeting Italy).