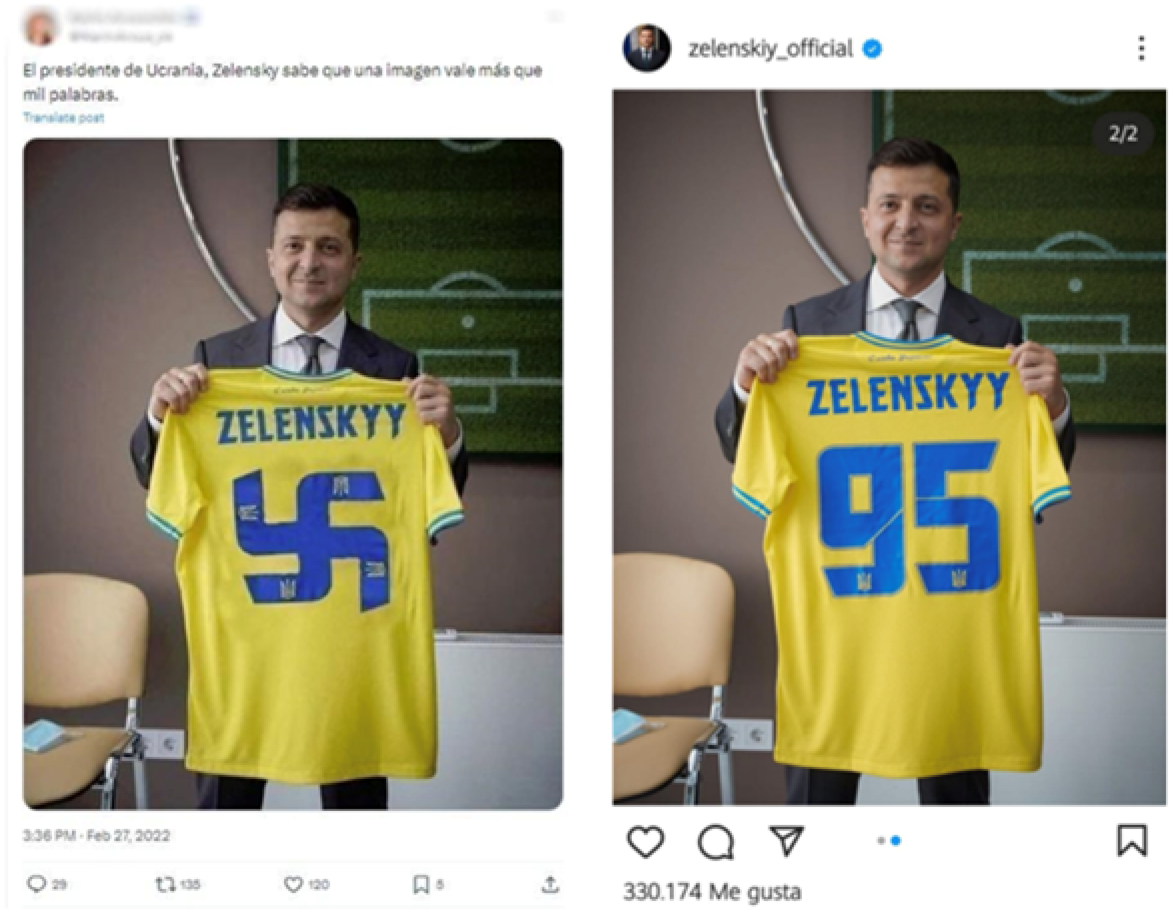
Fighting foreign information manipulation and interference

openaccessgovernment.org/article/fighting-foreign-information-manipulation-and-interference/191418

10 April 2025



El presidente de Ucrania, Zelensky sabe que una imagen vale más que mil palabras.

Source: Maldita.es

image: © Maldita.es

Highlighting the EU-funded ATHENA project, which supports Europe’s defence against foreign information manipulation and interference (FIMI). Dr David Wright and Dr Richa Kumar discuss various incidents and tactics used by countries to influence public perception and recommendations to improve media literacy and combat disinformation

Russia, China, Saudi Arabia, North Korea, Iran and others are engaged in information warfare, otherwise known as foreign information manipulation and interference (FIMI), against Ukraine, Europe and other countries.

Together with our partners, as part of the €3.2 million EU-funded ATHENA project, we developed 32 case studies of FIMI, including these:

- In 2023, the US Republican Party swallowed the lies of a pro-Russian agent who had been working for the FBI that Joe and Hunter Biden took $5mn each in bribes from a Ukrainian energy company. He was later exposed and convicted.
- When the US Congress passed a multi-billion-dollar aid package for Ukraine in April 2024, the Russians purveyed messages such as ‘The USA controls Ukraine.’ A Russian foreign affairs spokeswoman said: ‘Military aid to the Kiev regime is direct sponsorship of terrorist activities.’
- Russia tried to create fissures in German society by linking a German €8 billion aid program for Ukraine with cuts in subsidies to the agrarian sector.
- Russia claimed Sweden supported the burning of the Quran in a bid to undermine Sweden’s bid to join NATO. It characterised Finland’s new membership in NATO as war- mongering and claimed that Europe was going to invade Russia.
- During the civil war in Mali in 2022, the Wagner group, a Russian state-funded private military company, and the Malian army massacred citizens in the southern town of Mora and blamed it on UN peacekeepers. A surveillance drone exposed their lies.
- US intelligence revealed that Russia had allocated more than $300mn to corrupt foreign politicians, including several Members of the European Parliament, in the guise of payments for interviews appearing in the Voice of Europe, a pro-Russian website.
- To justify its invasion of Ukraine, Russia has sought to portray Zelenskyy as a pro-Nazi leader. Among other things, they doctored an image of the Ukrainian leader holding a football jersey with a swastika. They also claimed that Zelenskyy had a villa in Florida and was going to flee his native country.
- Russians spread disinformation about Pfizer COVID-19 vaccines, telling followers the vaccine was responsible for hundreds of deaths, unlike their Sputnik V vaccine.

Two-thirds of our case studies focused on Russian state initiatives, as Russia is responsible for the propagation of more FIMI than any other country by far. We also included case studies based on China, Iran, North Korea, Saudi Arabia and Turkey.

Each case study was structured as follows:

- Introduction
- Threat actors purveying FIMI
- Presumed objectives of the actors
- Incidents and observables
- Targets
- Tactics, techniques and procedures (TTPs)
- Channels through which FIMI is spread
- Languages used in FIMI
- Effectiveness of the spread of FIMI
- Countermeasures
- Conclusions and recommendations.

We encourage others conducting disinformation case studies to use the above structure to facilitate detailed comparative analysis and build a repository of cases. The structure is based on the DISARM Framework, a methodology used to analyse and counter FIMI by categorising disinformation TTPs to enhance detection, response and resilience.

The case studies generated many findings and recommendations, including the following:

- States need to increase the media literacy of the public through well-funded campaigns to educate citizens on how to recognise and report suspicious content, critically assess the information they encounter online, and evaluate the credibility and motives behind information sources. EU Member States should promote image and video fact-checking skills to identify manipulated content and other forms of digital deception.
- Collaboration between fact-checkers, NGOs, and states should be encouraged institutionally to expose and counteract FIMI campaigns and make it harder for disinformation to take root. Strengthening trustworthy institutions as exemplars of reliable information will help. They should establish rapid response teams tasked with debunking misinformation and providing clear, evidence-based responses to propaganda claims. The #UkraineFacts initiative, part of the International Fact-Checking Network, is an example of successful collaboration.
- Heads of state and other high-profile figures are particularly vulnerable to hostile influence operations aimed at manipulating public perception and decision-making processes. The susceptibility of these individuals poses significant risks not only to their personal reputations but also to national security and public trust. Therefore, it is crucial to recognise and address the challenges faced by those in influential positions.
- An EU Member State should not act alone but as a member of a unified front. European countries should deepen their cooperation in intelligence-sharing mechanisms to swiftly detect and disrupt foreign interference efforts, particularly ahead of elections. The EU should also enhance cooperation with international bodies and third countries to prevent the relocation of disinformation operations to jurisdictions outside the EU and strengthen the global fight against disinformation.
- The EEAS should prioritise investment in multilingual tracking tools capable of detecting disinformation across different languages.
- The EU should focus on the robust enforcement of existing laws such as the Digital Services Act (DSA), General Data Protection Regulation (GDPR) and EU AI Act to mitigate the spread of false information online. Member States should strengthen the verification and legitimacy of EU-registered online domains and companies to protect legitimate news media from being impersonated.
- The EU should fund research analysing the psychological and communicative effects of FIMI campaigns to deepen understanding of how disinformation influences human perceptions and behaviour.

These and other case studies and recommendations appear in David Wright (ed.), Foreign Information Manipulation and Interference: Case studies from the ATHENA project, Springer, forthcoming, 2025.

References

1. For a prediction about information warfare, see Wright, David, “AI and Information Warfare in 2025”, 2019 IEEE SmartWorld, pp. 317–322. https://ieeexplore.ieee.org/document/9060412
2. The European External Action Service (EEAS) defines FIMI as “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, by state or non-state actors, including their proxies inside and outside of their own territory. See “1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence”, January 2023. https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en
3. Ibid., p. 11.
4. https://www.disarm.foundation/framework

The ATHENA project is co-funded by the EU and UKRI under grant numbers 101132686 and 10107667.