



AI or Reality?

www.euawareness.org

#KnowledgeAgainstManipulation

AI or Reality? #3

David Dondua

One Playbook, Several Countries

The opinions and conclusions expressed are those of the author and do not necessarily reflect the views of the EU Awareness Centre.

© [2026] EU Awareness Centre. All rights reserved

September 2026

In August 2026, the German public broadcaster Mitteldeutscher Rundfunk (MDR) confirmed something unusual. Its staff [found fake videos online carrying the MDR logo](#) that MDR never made. The channel's editor-in-chief called it an attack on the credibility of free media.

That single case is worth pausing on, because it is not really a story about Germany. It is one entry in a much longer catalogue. The same operation that faked MDR has faked broadcasters and politicians in France, Ukraine, and Moldova. Different countries, different political fights, but the same method, repeated with almost mechanical precision.

This article looks at how that method works, why it keeps succeeding even after exposure, and why the usual advice—"learn to spot the fake"—isn't enough to deal with it.

What is Operation Overload

Researchers know this campaign by two names: Matryoshka, after the Russian nesting doll, and [Operation Overload](#). Both point to the same Russia-linked network, active since 2023, that builds fake news content and pushes it through a coordinated system of bot accounts, fake profiles, and direct outreach to journalists.

The mechanics are fairly consistent. A fake video or article appears, usually branded with the logo of a real, trusted outlet. It gets seeded through networks of accounts that repost and amplify it. This is what makes the operation unusual: the accounts often contact real fact-checkers and newsrooms directly, tagging them or emailing them and inviting scrutiny. Investigators at [CheckFirst](#), who studied the campaign closely, found that these direct contacts sent more than 200 targeted emails to newsrooms across Europe in just a few months, alongside thousands of social media posts.

At first glance, inviting fact-checkers to debunk you looks like a mistake. It is not. A debunking article still repeats the claim, still shows the fake logo, and still spreads the story further, just wrapped in a correction. Being exposed does not stop the campaign. In some cases, it helps it.

Four countries, one pattern

Germany. The MDR case is not isolated. Fake videos, carrying the logos of MDR, Tagesschau, and other German outlets, have accused regional politicians of corruption, abuse, and worse. One candidate in Saxony-Anhalt [was falsely accused of killing his own grandmother](#). The timing lines up with Germany's state elections this September — in Saxony-Anhalt, Berlin, and Mecklenburg-Western Pomerania. German security services describe a campaign run centrally that avoids attacking the parties already friendly to Moscow.

France. Ahead of the 2027 presidential race, fake videos using the visual identity of Le Figaro, Libération, and Le Monde have targeted two possible candidates, [Gabriel Attal and Édouard Philippe](#). The fabricated content linked Attal to political scandal and, separately, spread false claims about his health, including a fake hospitalisation and a false Parkinson's diagnosis. Attal filed a formal complaint alleging foreign interference. When the campaign's early narratives around Attal lost traction, researchers observed the same network simply redirect its effort toward Philippe.

Ukraine. In July 2026, [a video using a fraudulent Euronews identity](#) claimed that President Volodymyr Zelensky's parents were under investigation for corruption. The video used an AI-generated voice and cited a supposed article in Ukrainska Pravda that does not exist. It reached millions of views before Ukraine's Center for Countering Disinformation confirmed it was fabricated and traced it to the Matryoshka network. This was not the first such attempt — earlier fakes have used the BBC's identity to claim, falsely, that Ukraine's first lady tried to flee the country.

Moldova. Ahead of the country's 2025 parliamentary elections, the same network pushed [dozens of fabricated stories a month targeting President Maia Sandu](#) — among them, false claims that she embezzled \$24 million and that she was addicted to psychotropic drugs. A separate AI-generated video showed her rapping, in Russian, as an incompetent leader. Independent monitoring found Sandu was named in these fake stories more often, in some periods, than either Ukraine's or France's president — a sign of how much priority Moldova's EU path has earned in this campaign.

The common thread

Take away the details of each case, and the method is always the same. Steal a trusted name. Attach a claim that makes people angry, not one that tries to convince them. Time it around an election or a summit. And make as many of them as possible. Most fakes are cheap and quick to produce, and they don't need to last long.

The operation does not need any single video to be convincing. They just need enough of them so people stop being sure what's real.

Why "spot the fake" is not the answer

The instinctive response to all this is to get better at detecting fakes — watch for unnatural voices, mismatched lip movement, telltale AI artefacts. That instinct is not wrong, but it is incomplete, and treating it as the whole answer is a mistake.

Look again at the four cases above. The MDR videos used a real logo. [The Euronews fake about Zelensky's parents](#) used real footage conventions and cited what looked like a real news outlet. The France cases borrowed the actual visual identity of real newspapers. In each case, the fabrication was not in inventing something from nothing — it was in combining real elements with a false claim and false context. Asking "was this made by AI?" misses the point when the logo is genuine, the format is genuine, and only the underlying claim is not.

This is also where the fact-checker-baiting tactic becomes important again. Even a thoroughly debunked fake keeps a kind of half-life. It keeps circulating among people who saw the original clip but never saw the correction. Over time, this produces something researchers call the liar's dividend: once audiences know convincing fakes exist, real evidence becomes deniable too. A genuine scandal, a genuine leaked document, a genuine recording — all of it can now be waved away as "probably one of those fake videos." The operation does not need to win every argument. It only needs to make every argument arguable.

That is the real target, and it is worth stating plainly: not one politician, not one election, but the basic public habit of trusting a source because it looks official.

What "think before you trust" actually means

If detection alone will not solve this, what does?

The more durable habit is verification before belief, not after. A few concrete practices worth building into how you read anything with an official-looking logo attached:

- Check whether the outlet itself has published the story. Go to the source directly, rather than trusting a screenshot or a repost.
- Treat a familiar logo as a starting point for checking, not as proof. Familiarity is exactly what these campaigns exploit.
- Notice when a claim seems designed to provoke a strong reaction rather than to inform. That is often a better signal than any visual artefact.
- Be slower to share, especially around elections, when the timing itself should raise a question.

None of this requires technical expertise. It requires a shift in the default question, from "does this look real?" to "have I checked where this came from?"

A pattern, not an incident

The MDR case will likely be forgotten within a news cycle or two, replaced by the next fabricated video and the next outraged headline. That is, in a sense, the point that the operation is built to outlast any single story about it. Germany, France, Ukraine, and Moldova are not four isolated incidents. They are four data points in the same campaign, run with the same method, adjusted only for local politics.

This is why the EU Awareness Centre is tracking this case, and others like it, under our *AI or Reality?* line. These cases raise a question that isn't really about artificial intelligence at all. It is about whether the habit of trust — trust in a familiar logo, a familiar voice, a familiar format — can survive an environment built specifically to exploit it.

Think before you trust.



David Dondua

Ambassador David Dondua is a diplomat and expert in international security, conflict resolution, and European integration. During his diplomatic career in the Georgian foreign service (1993–2022), he held key positions, including Ambassador to Austria, Greece, Serbia, the OSCE and NATO. He serves as Chairman of the Board of the EU Awareness Centre.