

Fraunhofer FOKUS Institute for Open Communication Systems

---

# Assuring provenance and authenticity: Challenges and solutions for HbbTV

Naomi Schoppa [naomi.schoppa@fokus.fraunhofer.de]



# Disinformation in the Wild

HOME > SHOWS > TRUTH OR FAKE

## Israel-Iran conflict: Disinformation war plays out on social media

MIDDLE EAST



Issued on: 16/06/2025 - 22:33 - 05:25 min

From the show **TRUTH OR FAKE**

As the conflict between Israel and Iran enters its fourth day, fake viral videos have been spreading on social media targeting both sides. We debunk the false claims that are going around in this edition of Truth or Fake.

### Disinformation:

Source: <https://www.france24.com/en/tv-shows/truth-or-fake/20250616-iran-israel-tensions-disinformation-war-plays-out-on-social-media>



### Deep fake:

The ZDF news anchor Christian Sievers was cloned using AI to create an advertisement for a dubious financial product.

Source: <https://www.zdf.de/nachrichten/video/politik-sievers-ki-fake-102.html>



### Pope in a puffer jacket:

created in March 2023 using the AI tool Midjourney and showed the Pope in unusually fashionable clothing

Source: <https://www.cbsnews.com/news/pope-francis-puffer-jacket-fake-photos-deepfake-power-peril-of-ai/>

**bioRxiv**  
THE PREPRINT SERVER FOR BIOLOGY

New Results

This article h

**Uncanny similarity of unique inserts in the 2019-n protein to HIV-1 gp120 and Gag**

Prashant Pradhan, Ashutosh Kumar Pandey, Akhilesh Mishra, Parul G Manoj Balakrishnan Menon, James Gomes, Perumal Vivekanandan, Bi  
doi: <https://doi.org/10.1101/2020.01.30.927871>

This article is a preprint and has not been certified by peer review [what d

### Misattributed scientific preprints:

text spread on social media and was misused by conspiracy theorists as alleged proof of targeted genetic manipulation

Source: <https://www.biorxiv.org/content/10.1101/2020.01.30.927871v1>

# Misinformation, Disinformation & Fake News

## Misinformation

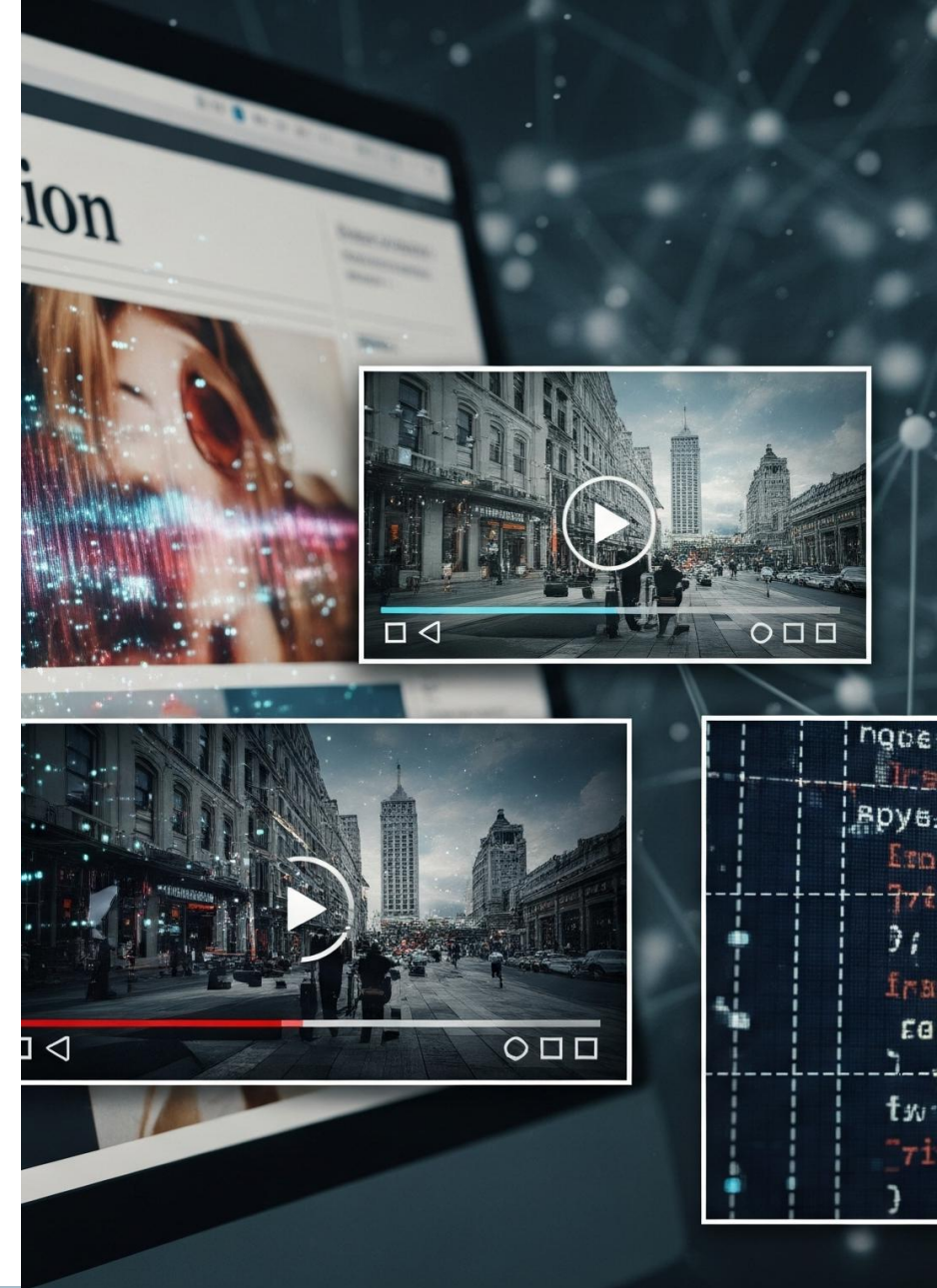
- false, but not intended to harm

## Disinformation

- intentionally misleading or wrong

## Fake News

- Fictional news stories that imitate the format of genuine journalistic reporting but have no factual basis.



# Further threats from hacking attacks

## SPECIFIC THREATS TO THE BROADCAST AND EVENT SECTOR

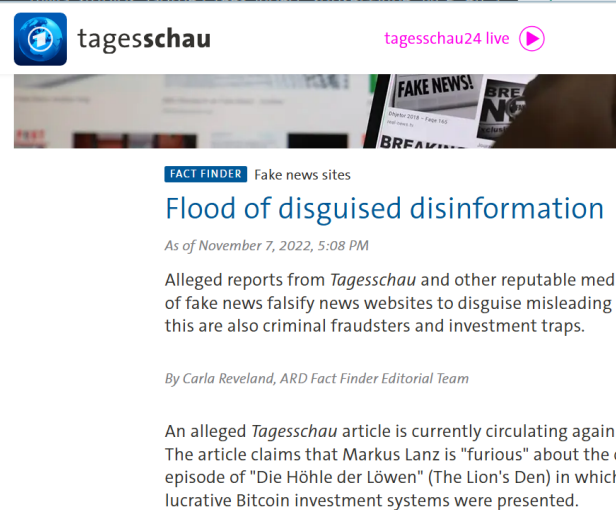
### TV Broadcasters & OTT Providers (ARD, BBC, ESPN, Netflix, DAZN, Sky, etc.)

- DDoS attacks → Streaming services or live TV broadcasts can be disrupted.
- Ransomware attacks → Critical production systems and broadcast signals can be encrypted.
- Signal hijacking → Hackers could inject illegal content or fake news.
- Data breaches → Customer data or subscription information could be stolen.

Sporting events have increasingly become cyberattacks. Here are some notable examples.

Source: [https://lp.riedel-networks.net/hubfs/BROADCAST%20Cybersecurity\\_en.pdf?hsLang=en](https://lp.riedel-networks.net/hubfs/BROADCAST%20Cybersecurity_en.pdf?hsLang=en)

### Production Companies (IMG Studios, Game Creek Video, Sunspot Video, NEP, etc.)



The screenshot shows a Tagesschau article with the headline "Flood of disguised disinformation" under a "FACT FINDER" banner. The article discusses fake news sites and mentions a report from Tagesschau. A red box highlights the article title and the "FACT FINDER" banner.

Source: <https://www.tagesschau.de/faktenfinder/fake-news-serioese-marken-103.html>

Deutschlandradio | Deutschlandfunk Kultur | Deutschlandfunk Nova



Topics ▾ broadcasts program Podcasts Audio archive



Live

Homepage / The news / Hackers take over Arte's YouTube channels

### Cyberattack

## Hackers take over Arte's YouTube channels

Unknown individuals temporarily hacked two YouTube channels belonging to the Franco-German cultural channel Arte. The broadcaster stated that the unauthorized access had been blocked and that a comprehensive analysis of the cause and extent of the attack was underway.

08.09.2025

Subscribe



Source: <https://www.deutschlandfunk.de/hacker-uebernehmen-youtube-kanale-von-arte-100.html> translated to english



## What is Provenance?

- The **origin, history, and ownership** of content, data or things
- Helps track “**where it came from**” and “**how it evolved**”
- Comparable to a chain of custody or **trust trail**

“**Provenance** in our context means not **only information about proving the origin** of a piece of media content, but also **proving the edits and other actions** that have been made to the content during its production and publishing process.” [1]

[1] <https://iptc.org/media-provenance/what-is-media-provenance/>

## What is Authenticity?

### Confirm a source of information, data, or product

- Trustworthiness: Do we have reason to believe it?
- Verifiability: Can we confirm the source?
- Truthfulness: Is it correct?

“**Authentic content** is media in any form built upon a base of honesty and **connection with its creators**, that goes beyond results, products, or sales. This content pierces through the noise and **builds a genuine bridge with the audience** through shared interests or values.” [2]

[2] <https://www.adobe.com/learn/express/web/create-authentic-content>

## Technologies

### Binding integrity information to the content

#### Embedded binding (in the file)

- Enables validation by directly checking the content
- Protection through digital signature or embedded hash
- Metadata such as provenance and authenticity are stored in the file itself

! Independent of external infrastructure, but we need a validation process

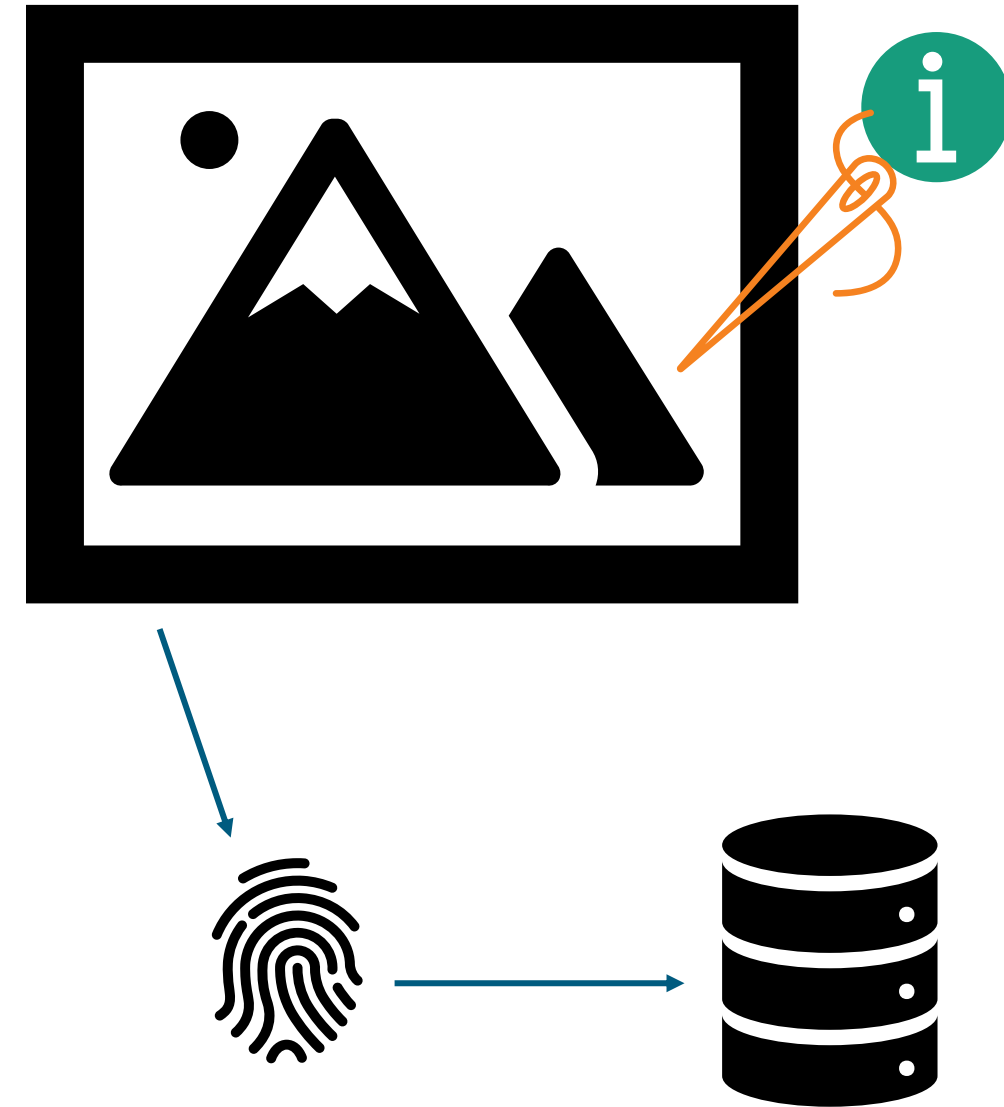
! Any change to the file also changes the hash → loss of integrity

#### External binding (via e.g. database)

- A fingerprint is calculated from the content
- The hash is stored centrally on a server
- During a check, the current hash is compared with the stored hash

! Robust against metadata loss, manipulations can be reliably detected

! Dependence on network and server availability



## UNCONFERENCE SESSIONS?

### Open discussion about:

---

Is this relevant for HbbTV and DVB?

Should the standard define how provenance metadata is transported, displayed, or verified?

How can this technology be integrated into existing ecosystems – for example, via OTT, live, broadcast, and social media distribution channels?

How can users verify the origin of content without being overwhelmed by technology?

What else needs to be considered with DVB-I?

# Thanks for your attention!

---



**Naomi Schoppa**

Research Associate

Research areas: Artificial intelligence, provenance and authenticity in digital media content

[naomi.schoppa@fokus.fraunhofer.de](mailto:naomi.schoppa@fokus.fraunhofer.de)



Fraunhofer FOKUS  
Berlin, Germany