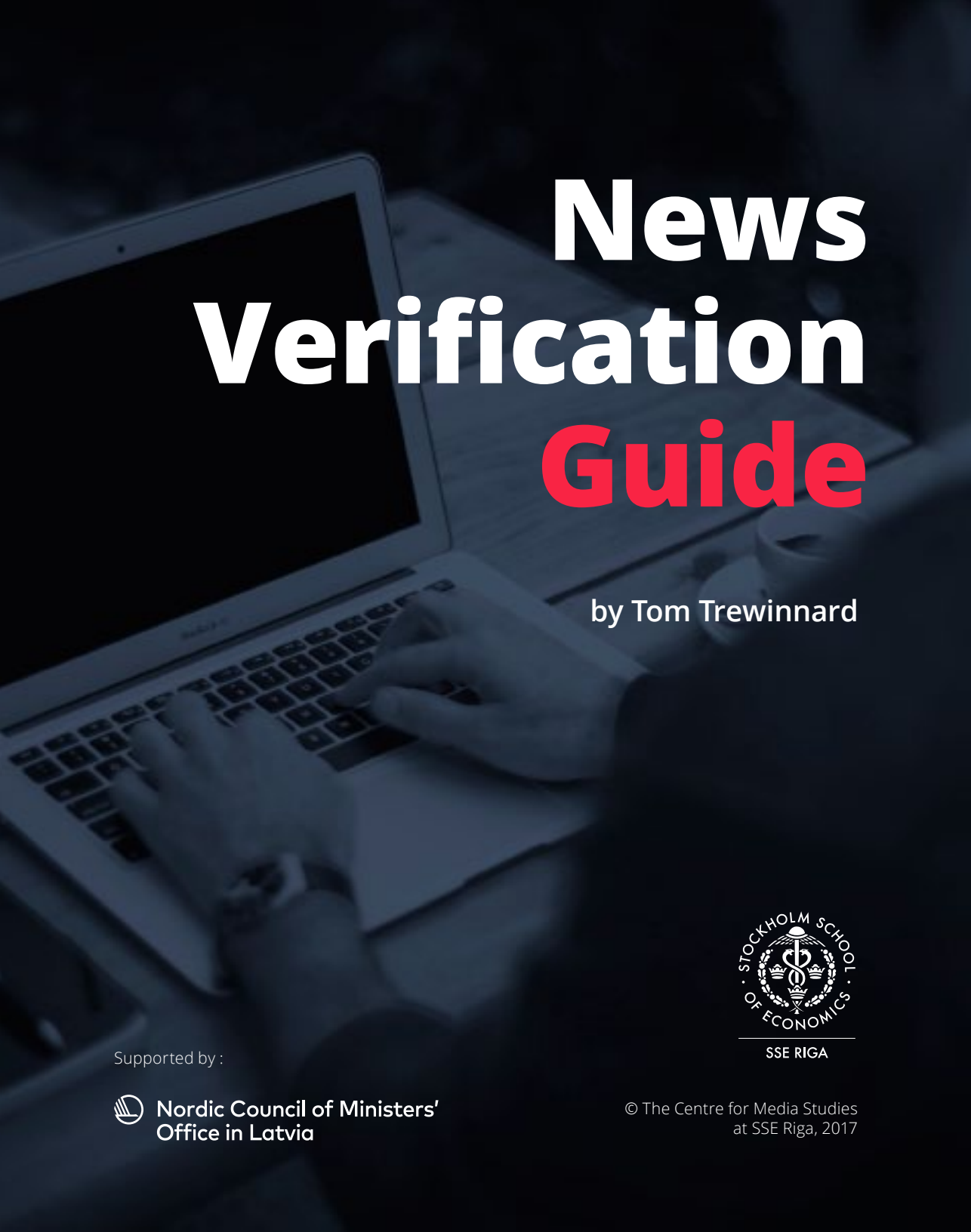


News Verification Guide

by Tom Trewinnard

SSE RIGA

Supported by :

Nordic Council of Ministers' Office in Latvia

Contents

Common Types of Fakes

The Verification Process

Introduction

The rise of camera-enabled smartphones and high-speed mobile data services has led to a proliferation of photo and video content being shared via social networks. It is now often the case that for an international, breaking news story, the first reports, videos and photo to emerge will come via social media.

This is both a great opportunity and challenge for journalists: we have access to first-hand footage from around the world of breaking news events, and so are able to cover stories that we otherwise couldn't report on. At the same time, social networks are contested spaces that are often awash with fake and mis-contextualized content designed to mislead and confuse.

If journalists are to benefit from sourcing content via social media, we need to take care to carry out a series of steps to establish the credibility of a photo, video or source. This guide is designed as a series of checklists to help you find answers to key questions about content you're investigating online. Below each checklist are some useful tips to bear in mind when conducting your investigations.

Remember: It's better to be right than to be first

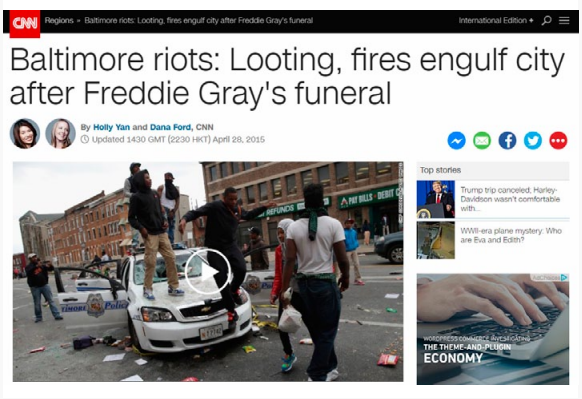
Common Types of Fakes

As we work with social sources, it's important to understand the most prevalent types of fake content shared via social networks.

Wrong time / wrong place

The most common type of misleading content comes in the form of old photos or video which have been stripped of their original context and re-uploaded alongside claims about a current news event. This content is often shared unwittingly on social networks, and is usually simple to debunk using the techniques outlined below.

- **For example** Aleksandrs Kirsteins, a Latvian MP from the nationalist VL/TBLNNK party opposed to resettlement of predominantly Middle East and African refugees within EU, posted a tweet on June 20, 2016, mocking the notion that highly-skilled workers would be among the arrivals. To illustrate his point, Kirsteins chose a picture of dark-skinned protesters vandalising a car.



In reality, the picture had nothing to do with the thousands of refugees arriving in Europe that summer: it was taken in Baltimore, USA, after a local man died in police custody.

(http://edition.cnn.com/2015/04/27/us/baltimore-unrest/)

- A similar case happened in Dec 13, 2015, when another supporter of VL/TB/LNNK, the mother of an MP, claimed in a tweet that in the village where the country's only asylum seeker accommodation centre of is located, migrants had violently robbed a 17 year-old girl in a bus stop. According to a tweet by Elita Dombrava, attackers stole the girl's mobile phone and police did not show up after being called.

The tweet was accompanied by a picture which is often used by US alt-right websites to express a negative view on Mexican immigrants, but which haa nothing to do with the described situation which turned out to be fake itself, sourced via unproven claims from another social network and denied by police later. The original image dates back to Long Island, New York, 2004.

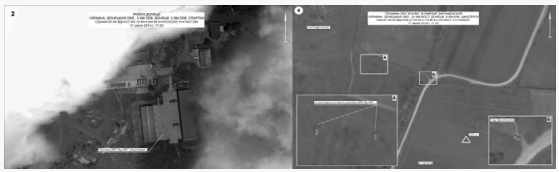
Manipulated content

Less common than "wrong time/wrong place" content is content that has been digitally manipulated using Photoshop and other image or video manipulation tools. This content has likely been shared with the intention to mislead, and can be more difficult to detect than "wrong time/wrong place".

- Prominent examples of manipulated content were witnessed in the case of MH17, a Malaysian Airlines passenger plane shot down over Eastern Ukraine, killing 298 people. In 2015, in response to video evidence that suggested Russian state involvement in the incident, the Russian Ministry of Defence displayed an "enhanced" image showing an advertising billboard which features in a video clip of the BUK missile launcher which is thought to have fired the missile which downed the plane.

- The "enhanced" image features text which claims the billboard was located in a Ukrainian-held part of the country. The enhancements, however were proven to be manipulations as a local in Luhansk visited the site and took a clearer image of the billboard (later when journalists from Correctiv and 60 Seconds Australia visited the billboard, it had been conveniently vandalized).

- Other groups investigating the incident have also made substantiated claims that Russia has also manipulated satellite imagery on numerous occasions to build a body of "evidence" that absolves Russia of any role in MH17.



These slides release by the Russian Federation purport to show a Buk missile launcher absent from a Ukrainian military base (left), and a pair of Buk missile launchers in a field on the day of the shootdown (right).

https://medium.com/@DFRLab/lie-in-the-sky-224186b6e98c#.87e60968x

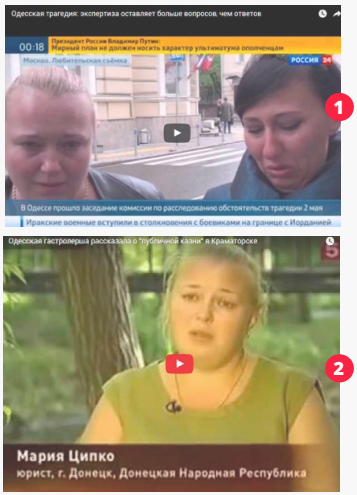
Staged content

Staged content is the least common type of fake content, as it requires the most work by the faker to produce. This is fake content that has been created and uploaded with the intent to mislead, and falls into a number of categories:

Staged videos

Staged videos, such as the Syria Hero Boy video, which was filmed by a professional filmmaker with actors – this type of content can look and feel very authentic.

During Ukraine's conflict with Russia, which culminated in the annexation of Crimea in 2014 and was supported by an aggressive propaganda campaign on Kremlin-controlled television channels, a woman named Marija Cipko came to prominence in Ukraine as a "roadshow actress": She played several roles in the TV news bulletins.



- On June 21, 2014, on a "Rossija 24" broadcast about a tragedy in Odessa in which over 40 people died in a fire after pro-Russian activists clashes with Ukrainian nationalists, she played a local resident offering information about state repression against pro-Russian activists.

- On Aug 4, 2014, Russian "Channel 5" broadcast a story where Cipko had turned into a lawyer, based in the conflict zone (in Eastern Ukraine, the self-proclaimed Donetsk People's Republic) and was telling the reporter how Ukrainian forces had publicly murdered the family of one of the pro-Russian rebels, although no proof was provided then or later.

- She has also been presented also as a member of the election committee in so-called independence referendums in Lugansk and Donetsk in 2014 and also the representative of pro-Orthodox church foundation, but under a different name.

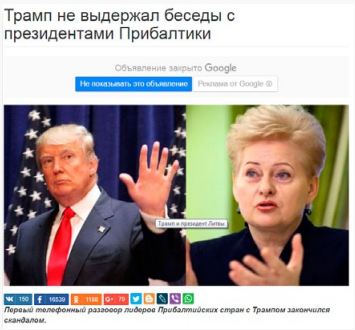
3

Fake news sites

The Estonian public broadcaster operates the site err.ee (the Russian version can be found at rus.err.ee). In parallel, a website with the address eer.ru exists, which easily creates confusion for less savy internet users, also because the sites are visually similar (as many news sites are). It calls itself the "Foreign Trade Relations" information agency and is run by NGO called "International Institute Of The Problems Of Sustainable Development" («*Международный институт проблем устойчивого развития*»). A print-out of the company's self description in Spravkaforme.ru shows that it considers itself an internet media business with 5 news sites and over a million unique users every months and it "works closely" with Russia's Ministry Of Foreign Affairs. It hires freelancers for whom the pay is calculated based on the clicks their stories receive.

- The site recycles Kremlin foreign policy narratives. Using the search terms "Latvia", "Estonia" or "Lithuania" in Russian, the stories which pop up are not about economic relations, but about Baltic countries fearing the demise of NATO due to Donald Trump being elected president of US, them being nationalists or anti-Russian. They are often sourced from Kremlin-sponsored news agencies TASS (state news agency) or RIA Novosti and a selection of translations into Russian from the global media content (http://inosmi.ru/) which are both part of Russia's official media conglomerate Russia Today., and also from marginal web pages.

- Another example is the fake news story about the first conversation between president-elect Trump and three Baltic presidents which supposedly ended with him shouting "Shut up!" and ending the conversation on Nov 28. The story is attributed to US television channel CNN, but such a piece was never broadcast. Diplomats from all three countries have confirmed that the conversation never took place. It sources the story from a site which also calls itself an "information agency", but most news are related to the autonomous Russian republic of *Khakasiya* in Siberia and the local weather forecast is for its capital Abakan.



- The same story is published on site hich claims to publish news about Russia's regions. It has no contact information for its newsroom, but shares the same address in Moscow and also chair of editorial board, Maxim Fedorenko, as the eer.ru.

- The same *EER.RU* team of people appear as an editorial office of internet site MK - London which calls itself the representatives of newspaper "Московский Комсомолец".

Local viral content

Local viral content is a recent trend whereby fake content sites report stories related to specific locales - with topics ranging from terrorist attacks to celebrity fights. The sources of these reports are always highly dubious, but occasionally local media will pick up the stories and re-publish them as if real.

- In 2013, a movement started in Russia against foreigners' adopting of local children. Part of the campaign was portraying Norwegians as paedophiles and ridiculing Scandinavian acceptance of LGBT rights. Even the special term, "Gejropa" or Gay Europe, was coined to be portrayed as nemesis of Christian, spiritual Russia which was defending conservative values from the "rotten" West.

A GONGO (Government Organised NGO) was created, called “Russian Mothers”. Its leader, Irina Bergseth, claimed Norwegians raped her little son while dressing him up in a Putin mask (she was having a nasty family dispute after divorce in Norwegian courts).

- A mass protest involving 12,000 people, supported by state actors, was organised in Moscow. In June, the internet newspaper “Segodnia.ru”, registered in Russia, published a story claiming that Norwegian minister has proposed to introduce incest as a subject taught in schools as it is a Norwegian “social tradition”. The story did not convey the meaning of what the minister said: that children have to be taught how to recognise and report unwanted advances. It was sourced from the GONGO press release.

https://rg.ru/2013/03/07/voina.html

- In 2013, three similar NGOs were created in Latvia mirroring the ideas already in place in Russia. The main support came from Latvian nationalist and pro-Russian parties. The idea of “incest as social norm” in Norway started to circulate in Latvian media. Respected members of society, such as a famous children doctor, repeated it in newspaper interview which went viral in social networks and parental websites. It appeared in the interviews of pro-Russian and conservative members of Latvian parliament, and was widely shared on the Russian-speaking websites and YouTube, as well as on TV channels broadcast from Russia.

- Some examples are much simpler: a bleak video of a youngster lamenting Latvia as a failed state quickly gained popularity and went viral on Latvian Facebook pseudonews sites in Dec, 2016. Within a week it was viewed 155,000 times on YouTube alone. The video itself was a copycat of similar American story “Dear future generations: sorry” which has been watched almost 5.7 million times at the time of writing. A simple YouTube search revealed the author to be a wannabe YouTuber whose videos usually get around 5,000 views. However, the video was passed as a genuine and popular opinion piece in the Latvian social networks and pseudonews sites.

The Verification Process

01 Is it the original?

As we've seen, the most common fakes we see are old video and photos recirculated alongside claims they're from a current event or story. It's a top priority to make sure that the content we're looking at is the original version (i.e. not something that has been posted online before, and not something that has been digitally manipulated) or as close to the original as we can find.

We can get to the original by:

- doing a reverse image search on Google Image Search or TinEye;
- checking for scraped videos with Amnesty's Data Viewer;
- checking for consistency in shadows and reflection;
- speaking to the source, ask them to send you the original file (which should have EXIF data);
- for images, use image analysis and authentication tools like Izitru or Forensically to detect any digital manipulation (this works best with the original files - i.e. not those uploaded to social media).

TIPS

- A "scraped" video is one which has been downloaded from the original account and re-uploaded using a new account. It's very common to find scraped videos of major news events, and can be difficult to find the original.

- Watch out for slight manipulations such as image inversion (flipping the image) and recoloring.

What is: **Reverse Image Search?**

- Reverse image search allows us to check whether an image has already appeared online and to find all the webpages where a given image exists. Reverse image search is the **first check** you should run on a photo being shared via social networks: it takes 30 seconds and 2 clicks, and is the fastest and most effective way to avoid sharing **"Wrong time/wrong place"** content.

- There are two main reverse image search engines: Google Images and TinEye. It's worth checking both, as they have separate indexes each featuring billions of images. If an image doesn't return any reverse image search matches, this **doesn't mean** it's definitely an original or authentic: further checks (outlined below) need to be carried out.

- Free Chrome Extension RevEye gives a quick search of a number of reverse image search engines, including Google, TinEye, Yandex, Bing and Baidu.

What is: **EXIF data?**

EXIF data is metadata encoded into photos that can provide a wealth of information including device ID, time of capture and location of capture. EXIF data, however, is removed from photos posted to social networks (like Twitter and Facebook) or shared via messaging apps (like WhatsApp, Viber). Ask the source to send you the original photo via email to view EXIF data through free online tools.

02 Who?

In addition to verifying the content of a post, photo or video, it's also essential to verify the source. Several well-made, high profile fakes have been debunked through researching the source in cases when the content has given away few clues.

Gather information about the source's social footprint by:

- analyzing any information present on their profile page and watch for "red flags" (very new accounts, accounts with very few posts/followers/following, previous content that may place the account user at an inconsistent geography, etc.);
- looking for social media presence on other networks (search Google for the username or full name if given) and gather any relevant data or information;
- investigating links in profile (including checking WHOIS domain registration information);
- reverse image search profile photo (**Tips** - watch out for slight manipulations such as image inversion and recoloring);
- searching for exact tweet wording to see if others have posted the same tweet.

- testing for bot tendencies using social media source analysis tools like BotOrNot;
- speaking to the source, ask them to corroborate information (such as weather - checked via Wolfram Alpha; EXIF data, if available).

TIPS

- The person who uploaded a photo or video isn't always the person who filmed it. Try to find the **person who filmed it, as they'll be best able to answer** questions regarding verification.
- A good way to spot troll and bot accounts is by looking at the first people an account followed, or the first people who followed a certain account - bots and sockpuppet accounts tend to follow other bots and sockpuppets (to give a veneer of credibility).
- Tools like Pipl, PeekYou, Spokeo and Foller.me can quickly provide useful information about a person or social account, but vary in utility from country to country.

What is: a sockpuppet account?

Sockpuppets are online accounts used for the purposes of deception. The motivations of sockpuppets vary greatly, though one emergent trend has been the rise of state-sponsored sockpuppets: real people paid by governments to create accounts on social networks and publishing platforms under fake names, used to spread misinformation and create a sense of public opinion for or against certain individuals or policies (this is called *astroturfing*). Sockpuppet accounts can be traced through investigative techniques (such as analyzing an account's social media network) and more technical approaches (such as IP address analysis).

03 Where?

Corroborating the location of a post, photo or video can help establish credibility, and is a strong way to debunk fake content. This is a process known as geolocation, which takes advantage of a number of data sources including maps, satellite imagery, street-view imagery and geotagged photos and video.

Try and locate the photo or video on a map by:

- carefully analyzing the content for distinguishing visual landmarks. These could be distinctive buildings, street signs, car number plates, or geographical features such as mountains, rivers;
- try to find these distinguishing landmarks or buildings on a map, using satellite imagery, street-view imagery, geo-tagged images (such as Panoramio) or annotated maps (such as WikiMapia);
- if you're able to access the original file, check the EXIF data for any geolocation data embedded in the image;
- check the source's other recent posts on social channels to see if they shed any light on where a user may have been when a photo or video was shot.

TIPS

- Tweets, Facebook posts, YouTube videos and Instagram posts can all be "geotagged" by the user uploading the photo, video or post. These geotags can be extremely useful, however they require further investigation and corroboration, as they are editable by the user at point of upload. This means a user *could* take a photo in Riga, but assign a geotag for anywhere in the world, although in practice this is not a common trend. The vast majority of content uploaded to social networks is not geotagged, and requires manual analysis and geolocation.

- For videos - take still frames (possible using screenshot tools on YouTube, or video editing tools for offline video) and create composite images that can give a clearer sense of landscape, and annotate these images with clear visual annotation that corresponds to an annotated map or satellite imagery.

https://www.bellingcat.com/news/2016/10/22/exit-corridor-shelling-west-aleppo-open-source-analysis/

04 When?

Determining when a post, photo or video was captured is crucial in establishing credibility, especially as we know that many fake posts rely on old content recycled with claims about current events.

To find out when a photo or video was captured:

- do a reverse image search on Google Image Search or TinEye;
- check for scraped videos with Amnesty's Data Viewer;
- if you're able to access the original file, check the EXIF data for any time of capture data embedded in the image;
- corroborate the weather shown in the time and place with historical weather records on Wolfram Alpha;
- if you have established the date and exact location, use SunCalc to determine the approximate time of day based on the direction and length of any visible shadows in the photo or video.

TIPS

- Be aware of the timezone rules of the network where you've found the content. YouTube videos and Instagram posts are given a timestamp based on US Pacific Time. Twitter posts are given a timestamp based on your profile settings. Facebook posts are given a timestamp based on your computer settings.

- One way some fake content has been debunked has been through noticed changes in urban landscape: in some cities in Syria, for example, certain buildings and mosques have been destroyed during the course of the conflict - so any photos/ videos claiming to show events after the destruction that features the building are likely to be miscontextualized.

05 Why?

Understanding why a social media user has uploaded a given piece of content can also be valuable in determining its credibility. Some social sources are accidental eyewitnesses, others tourists. Others might be professional journalists, while others are activists, and others can be government employees. Determining the motivation of the source can be relevant: activist or government sources may be using social media to tell only one side of a story, or to paint another group in a bad light.

- Analyze any information present on their profile page and watch for "red flags": very new accounts, accounts with very few posts, followers / following; previous content that may place the account user at an inconsistent geography, etc.

- Look for social media presence on other networks (search Google for the username or full name if given) and gather any relevant data or information.

Author **Tom Trewinnard** (UK) is Director of Development at **Meedan**, a social technology non-profit working on the **Check** project to develop collaborative verification tools and open training curricula. He leads Meedan's participation in the First Draft Coalition, a group of thought leaders and pioneers in social media journalism launched by Google News Lab in 2015.

Tom has moderated panels on digital journalism at Personal Democracy Forum and the Prix Italia, and convened a daylong pre-conference workshop for MENA-region journalists and digital rights activists at the Stockholm Internet Forums 2015 & 2017.

Tom has worked extensively with journalists in some of the Middle East and Europe's leading newsrooms, as well as with citizen journalists from around the world, to research eyewitness media and lead training in verification skills. Tom curates the verification and viral debunk newsletter The Checklist.

Additional Resources

For additional resources on how to conduct some of the analysis outlined above, and for case studies, and how-to guides, the following resources are extremely valuable:

First Draft News is a coalition of journalism and technology partners who produce training guides, case studies and research on social newsgathering and verification. First Draft News has numerous video resources and interactive training activities to test and improve your skills on the above techniques.

Verification Handbook is the first comprehensive resource for news verification, and includes several case studies. The book has two supplementary additions, one specifically for investigative reporting, and one for verifying digital content for emergency coverage.

Supported by :

Nordic Council of Ministers' Office in Latvia

STOCKHOLM SCHOOL OF ECONOMICS
SSE RIGA