TOWARDS A SAFER UKRAINIAN MEDIA ECOSYSTEM AND CIVIL SOCIETY: HOW OSINT CAN HELP

TOOLS AND SAFEGUARDS FOR USE IN DEBUNKING PROPAGANDA AND VERIFYING INFORMATION ONLINE DURING THE ONGOING CONFLICT WITH RUSSIA

NATALIA ANTONOVA

ROMAN OSADCHUK

LUKAS ANDRIUKAITIS

AUGUST 2022

IST | Institute for SECURITY + TECHNOLOGY

CONTENTS

SITUATION OVERVIEW

Verifying information and combating deepfakes is an essential skill for any journalist, one that is all the more crucial in wartime. With the ongoing Russian attack on Ukraine, both the Ukrainian media ecosystem and the global media ecosystem are suffering an onslaught of Russian military propaganda and disinformation, designed to confuse and demoralize Ukrainians and their allies.

This guide is intended for Ukrainian journalists and journalists covering Russia's war in Ukraine, with the purpose of introducing readers to some of the best tools and practices for identifying and combating disinformation disseminated via videos, images, and Telegram channels.

According to the United States and other Western governments, Russia maintains lists of key people to capture and potentially kill on Ukrainian territory. This means that safeguarding key information is of utmost importance in resisting the Russian threat.

This guide provides practical tips to safeguard your digital activities and improve your digital hygiene. For the purpose of this guide, we define digital hygiene as a set of regular practices to keep one's digital assets and footprint secure.

Note: As technology evolves, so does the disinformation threat. It is important to stay current on the latest developments in the online disinformation sphere. Use this guide, but continue to monitor reliable sources on Russian disinformation and propaganda to remain up to date on any developments or changes in tactics.

HOW TO VERIFY VIDEO IN A TIME OF CONFLICT

Videos are an important tool in the Russian disinformation arsenal, particularly because most members of the public have a hard time analyzing visual and aural components. Deceptive editing can also further Russian disinformation. Therefore, when considering the importance of video, remember the overall popularity of resources like YouTube in Russia:

YouTube users

Year	Users
2012	800,000,000
2013	1,000,000,000
2014	1,100,000,000
2015	1,200,000,000
2016	1,400,000,000
2017	1,500,000,000
2018	1,800,000,000
2019	2,000,000,000
2020	2,300,000,000

Source: YouTube

Top-5 Countries by Youtube Users

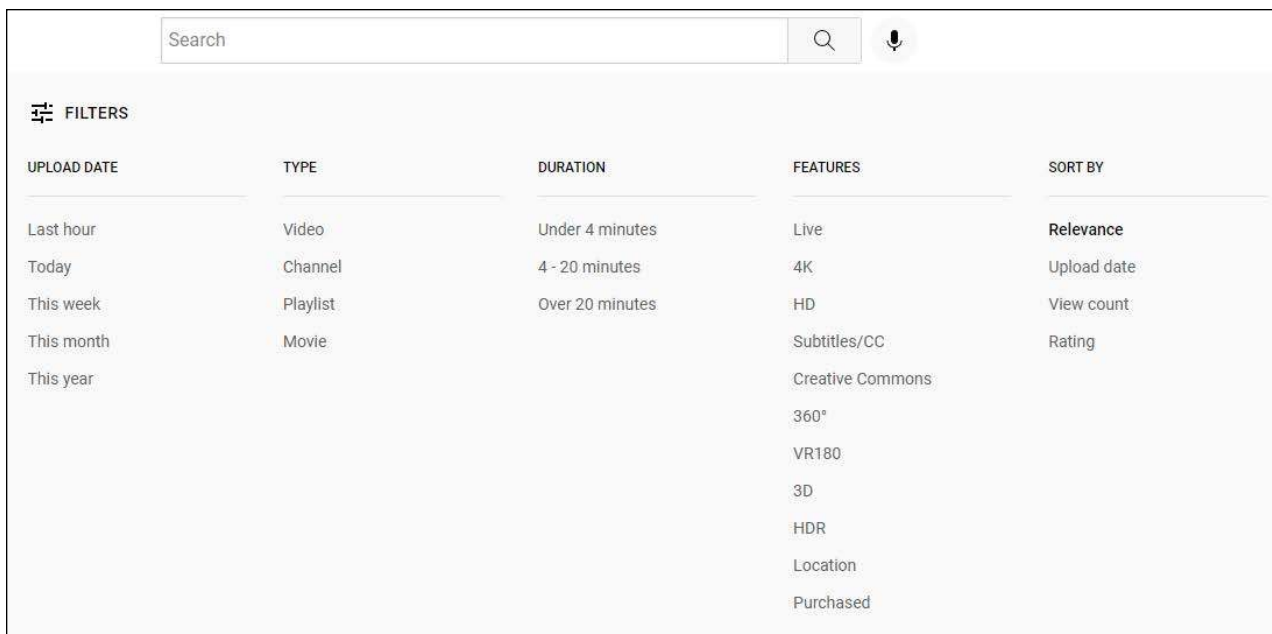|	Country	Users
1.	India	225,000,000
2.	USA	197,000,000
3.	Brazil	83,000,000
4.	Japan	60,000,000
5.	Russia	58,000,000

Source: Global Media Insights

As multiple reports and studies have shown, YouTube algorithms aid in spreading misinformation on the platform, as they create endless loops of recommended content that includes disinformation and conspiracy theories. Russian disinformation is no exception, and is thus able to easily spread on the platform—this can harm the Ukrainian war effort at home and abroad, and sow confusion and distrust among Ukrainians and their supporters around the globe.

ADVANCED SEARCH AND YOUTUBE

In order to thoroughly research videos on YouTube and understand their potential impact, as well as debunk any lies or misinformation you might encounter, it is important to first familiarize yourself with YouTube filters and advanced search on the platform. This will be especially useful should you want to determine the history of a certain video (for example: when it first appeared). It is also useful for looking at videos by subject, to see how a particular topic or theme is being publicized on the platform—a process that is useful in debunking, reporting, and documenting potentially harmful content:

YouTube Filters and Advanced Search

Simply using the standard YouTube search is not likely to be enough for advanced research, as the YouTube algorithm may skew your results and cost you time (and during war, time is of the essence). Using advanced search, videos can be filtered by upload date, duration, and features, and the searcher can use different sorting methods.

Note: Use quotation marks when searching for a specific phrase.

Identifying the source of a video and identifying specific people and places in the video can be easier if you use reverse image search on screen grabs of said video. Reverse image search is the process by which you can establish where else a particular screenshot or image has been published.

Note: Ideally, you should use more than one reverse image search tool to verify your findings.

Here are some of the tools you can use by uploading a specific screengrab:

Reverse Image Search Tools

| Name	URL
YANDEX	**yandex.com/images**
Bing	**bing.com/visualsearch**
TinEye	**tineye.com**
Google Images	**images.google.com**

Google, TinEye, Bing, and Yandex are popular reverse search image tools. Please note, however, that Yandex is a Russian company. Exercise caution when using platforms with connections to Russia in the context of the conflict in Ukraine.

USEFUL TOOLS AND PLUGINS

For trickier/more advanced subjects where more data is needed to verify or debunk a video, video analysis tools are widely available. These include Amnesty International's **YouTube DataViewer** and the **InVID plugin**.

The InVID plugin can save a researcher time when conducting a reverse-image search by analyzing YouTube thumbnails. We have observed examples of videos claiming to depict real footage of COVID-19 victims, which resulted in such videos spreading rapidly at the beginning of the COVID-19 pandemic, that, once analyzed via InVID, were proven to actually be footage from a cinematic film. These instances have confirmed that searching screenshots with the plugin can aid in stopping the spread of disinformation.

An InVID search via image screengrabs immediately leads us to a movie that has nothing to do with Covid, as seen above. Recognizing this type of misinformation and disinformation is especially important, because Russia will routinely launder deepfakes by trying to make them go viral in other nations—note how Indian Twitter users are spreading Russian fakes targeting Ukraine today.
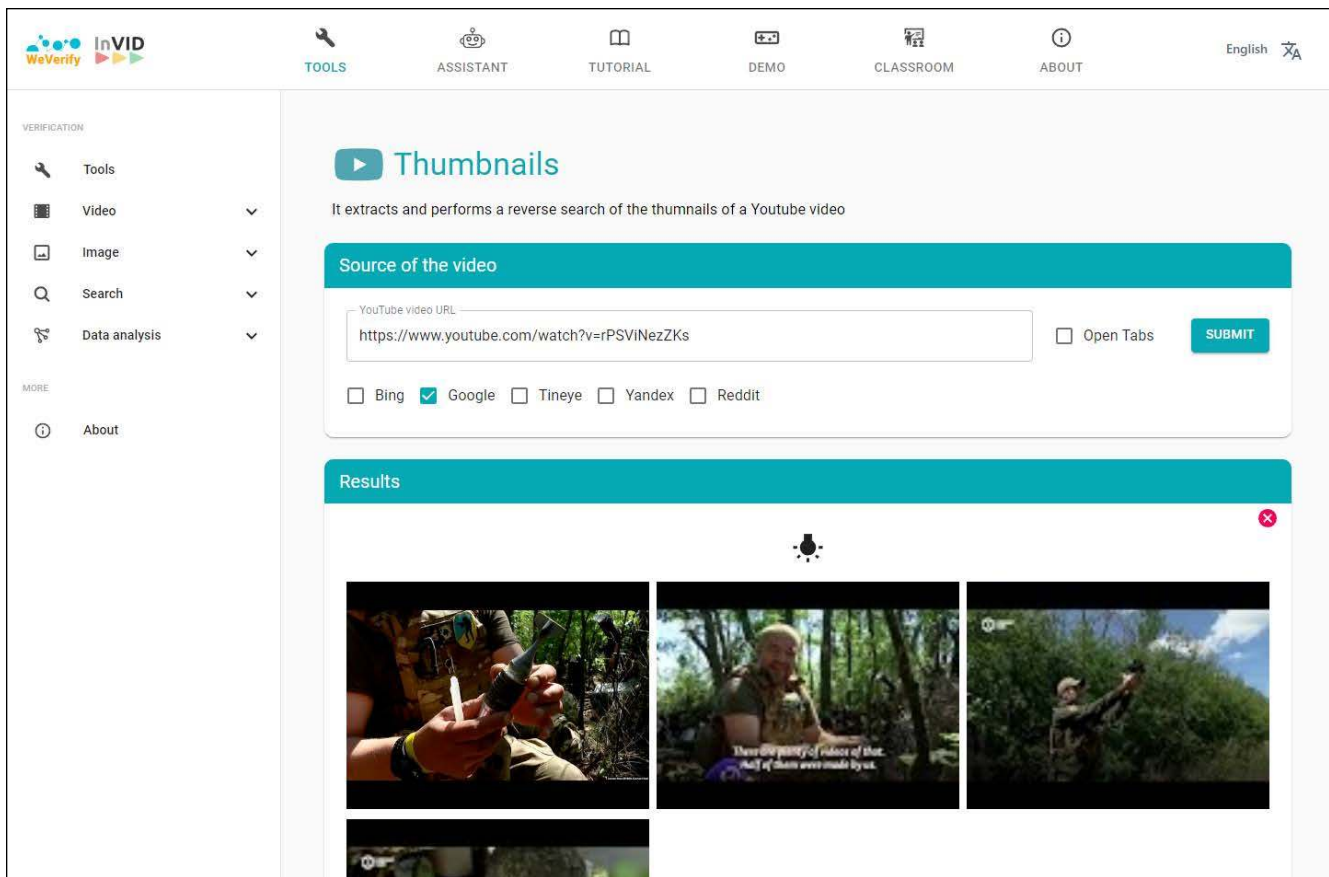
When using InVID, you can easily select which engines to employ in your reverse-image search—all are standard engines, and you will not need to download them in order to use them:
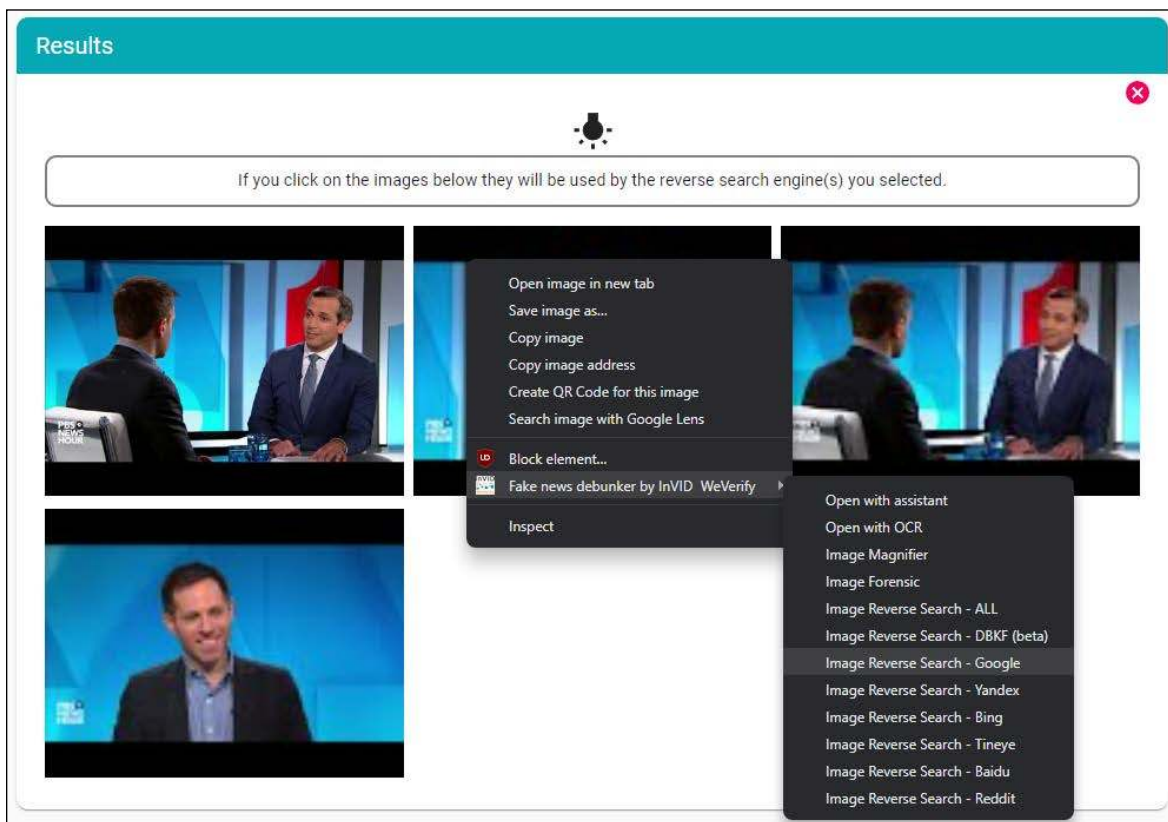
When debunking disinformation, it is important to understand the reach and metrics that a particular video has had—this way, you can estimate its individual impact and track its spread.

The **Keywords Everywhere** Chrome tool is particularly useful for this purpose. Note the information it provides for this example BBC video. You can use this tool to analyze videos from sources far less reputable than the BBC to provide much more transparency:

RESEARCHING EXTREMISM

If you are working in the sphere of radical extremism, consider using Raditube as a guide for understanding extremist video output. Keep in mind that far right extremists in the United States have a long history of helping spread Russian propaganda as it easily percolates from one respective ecosystem to another.

Raditube can help to uncover links and common topics between channels, as well as the channels' histories:
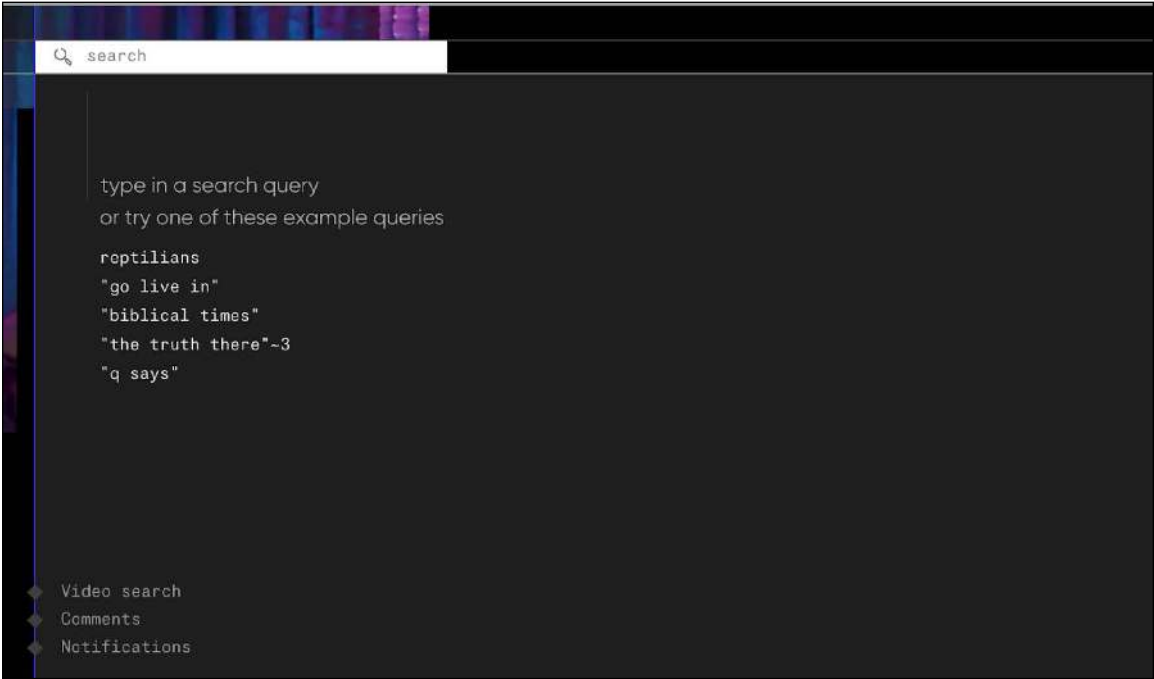
Raditube is useful in that it shows the status of individual channels, as well as their statistics—this way, you know which ones continue to be active:

channel name	status	views	subscribers	videos	since
#PedoGate	removed	9.882 views	0 subs	19 videos	2017-(
#SeekingTheTruth JoshWho News	removed	21.813.536 views	98.500 subs	833 videos	2016-(
AMTV	active	527.951 views	693.000 subs	11 videos	2007-(
And We Know	removed	21.773.688 views	346.000 subs	110 videos	2011-(
Annette Cividanes	removed	10.932.824 views	88.300 subs	424 videos	2014-(
Anon 7	removed	76.855 views	1.500 subs	141 videos	2014-1
April LaJune, copyright Holder	active	1.363.434 views	78.000 subs	513 videos	2010-1

SEARCHING VIA GEOTAGS

Finally, **YouTube GeoFind** is a tool that can help you save time by searching geotagged videos by location. This is extremely useful during times of conflict, as multiple videos from the same vicinity are frequently uploaded during combat operations and beyond.

Here is a typical search for all videos geotagged to Kyiv, Ukraine. Please note that you need to hit "submit" once you have input all of the relevant filtering data in the prompts on the page:

Results will appear below the "Submit" button:

HOW REVERSE-IMAGE SEARCHING, VERIFYING, AND EXPLORING METADATA CAN HELP COMBAT DISINFORMATION

Image analysis during wartime is crucial for identifying disinformation and checking facts. While it follows many of the same principles as video research, different tools are in play.

Working with one image also means that you have less searchable surface area—and must hone in on the tiny details that are often missed by the casual observer.

AI-GENERATED IMAGES

Frequently, you must start with analyzing the source of the image. Today, AI-generated images can help conceal trolls and propagandists, and even aid in creating entire fake identities online, for the purposes of spreading disinformation.

This Person Does Not Exist is a website that will help you familiarize yourself with how well this AI can work. Click "refresh" to easily generate a fake face that can be used to establish a fake identity.

Please note that asymmetry can be a giveaway when it comes to AI-generated images. Such is frequently the case when an image shows a person wearing glasses. Note how they do not render properly:
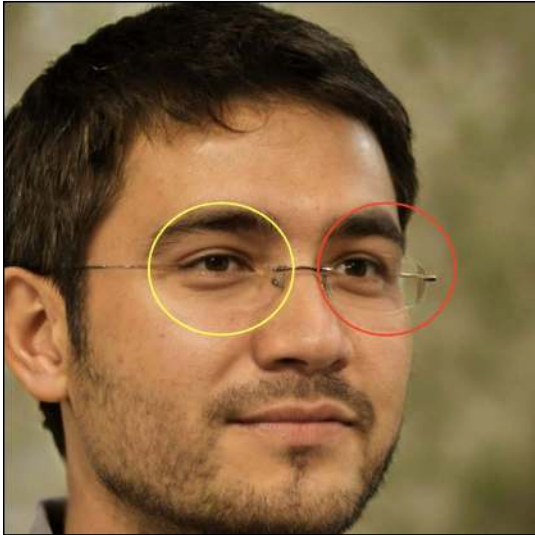
However, as AI continues to advance, more and more people will be easily fooled by fake profiles. This is why it is important to remain vigilant and do a deep dive on any source you may consider suspect— remember that trustworthy sources usually have sizeable digital footprints with granular detail, i.e. they will seem "human," as opposed to identities tailor-made to fit your interests and make you ignore any red flags with regard to the account's identity. Granular detail can include everything from embarrassing photos to close family connections, visible as part of a profile's individual digital footprint.

REVERSE IMAGE SEARCH & PHOTO ANALYSIS CAN COMBAT PROPAGANDA

A major concern as far as images go is how they migrate from the Russian ecosystem to the Western one, often without the necessary context.

For example, this image was claimed to be that of Katerina Prokopenko, wife of a Ukrainian Azovstal defender, by Russian military propaganda. The purpose of the image was to discredit Prokopenko as she visited the Pope to ask him to intervene on behalf of trapped Azovstal defenders in Ukraine. The image then spread to English-language Twitter, where it was unwittingly shared by American users, thus aiding the Russian propaganda effort:

While the woman on the right bears a passing resemblance to Prokopenko, a quick visual analysis will have you note the Polish flag on the t-shirt of the woman on the left. This is the first clue that we are dealing with disinformation.

A quick reverse image search via a useful tool such as **TinEye** can confirm that one of the earliest instances of the image being used was on a Russian meme site twelve years ago. By uploading the image to TinEye, we can see its lengthy history of use on various websites, including Russian meme sites from over a decade ago, and determine that the woman on the right of the image merely bears a resemblance to Prokopenko and is not tied to her:
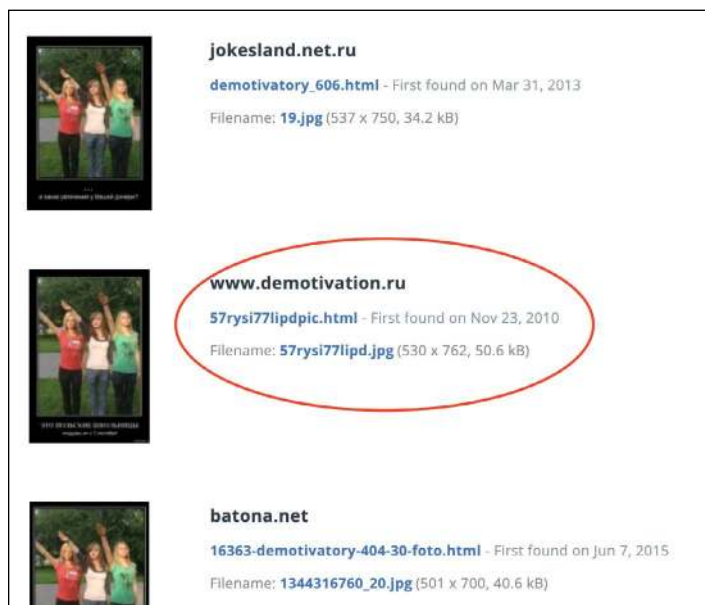
With an image like this, you can often explore more of its elements. Using a tool such as Forensically, you can see the different levels to this image by doing a level sweep. Clearly, this image was lifted from one of the sites featured in our reverse image search, followed by a new level which was added by circling the photo and typing Prokopenko's name in order to discredit her (the color difference is your clue):
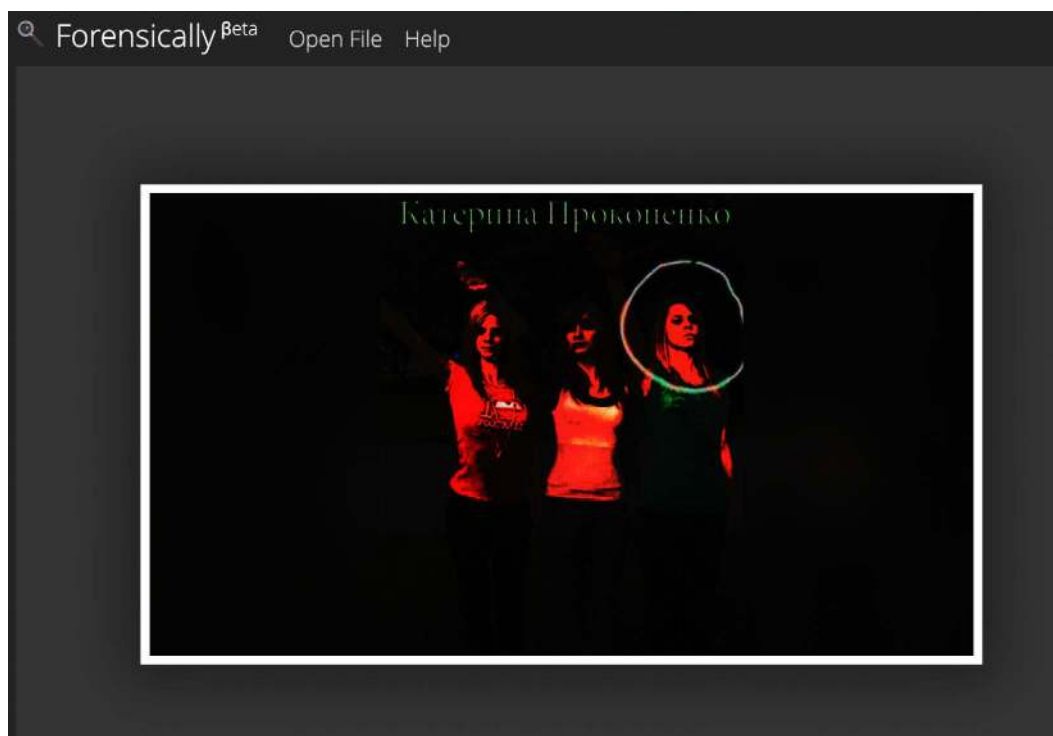
Another good example of a similar tool is **FotoForensics**, where you can upload photos just as you do at Forensically. This is how FotoForensics renders an altered image of Kim Jong-un. The color differences, again, show you when an image has been manipulated and where exactly on the image changes have been rendered:

Finally, while social media platforms strip metadata—i.e. location, time, device info, and other information that can give away an image's provenance—from photos, if you find a photo original in an online folder or library, you can use a variety of tools to analyze its metadata.

Here is a good example of the output that FotoForensics provides for an image that did not have its metadata stripped—note the detail that is available:

In the absence of reliable metadata, geolocation and chronolocation skills and tools can help you zero in on the location of an image.

FROM GOOGLELENS TO GEOLOCATION

Today, GoogleLens is a rapidly improving tool for identifying landmarks. If there is a particular landmark in your photo, crop the photo so that the landmark is clearly visible and no other elements will throw off the tool, upload the cropped photo to GoogleLens, and see what results you may get. For harder cases, wherein a landmark or an easily recognizable photo feature is not available, you may need to use satellite data.

While it may seem daunting at first, remember the two basic principles of geolocation:

1. It is not a guessing game, it is a game of elimination.

2. Reliably matching elements in the photo to elements in satellite imagery can help you confirm a location if reverse-image search did not return desirable and/or helpful results.

Both SentinelHub and Google Maps can provide you with free, easy-to-use tools for geolocating a specific, out-of-the-way place and noting when an image has been taken by recording changes in the local environment/infrastructure. Here is an example of how the geographic elements in a photo of a soldier can be matched to satellite images, thus helping you chronolocate the photo as well as geolocate it:

INTRODUCTION TO USING SHADOWS IN PHOTO ANALYSIS

If you are confused about which direction is which in a given image, a tool such as **SunCalc.org** can come in handy. Suncalc calculates shadow length based on an individual location and time of year, and provides helpful animations to help researchers track shadow movements throughout the day.

This tool can be invaluable if you have geolocated an image but are unsure when it was taken. It can also help with shadow analysis in photos where the approximate location is known, and you are trying to find what way certain elements of the photo are facing in order to help you discover the exact location where the photo was taken.

Start by using an address of a landmark you are very familiar with. In the example below, we are using the Duke Chapel in Durham, NC.

Note that you must press the button in the purple circle to run an animation of how the Chapel's shadow will behave during the day. You can input different dates in SunCalc in order to see how shadow behavior changes at different times of year. As you move on to analyzing more unfamiliar places via SunCalc, you will learn how to understand shadow behavior in order to improve your chronolocation skills and spatial understanding:

HOW TELEGRAM OPERATES & SPECIFIC PLATFORM VULNERABILITIES

As the ongoing conflict in Ukraine has demonstrated, the lack of regulation of the messaging service Telegram's has provided a perfect vehicle for disinformation and deepfakes. Being able to analyze Telegram channels is an important part of an investigative toolkit today.

Until recently, Telegram did not run ads on its platform. This created a so-called shadow economic model wherein channels accepted publications for financial remuneration and/or cross-promotion.

In Russia, journalists have documented connections between several popular Telegram channels and the Kremlin, and have discovered that it is possible to publish virtually any post on a certain Telegram channel, provided you have the money. In Ukraine, the Security Service of Ukraine uncovered a network of channels specializing in subversive activities and tied to the Russian Main Intelligence Directorate. Ukrainian media and CSOs investigated more extensive networks that spread subversive propaganda and disinformation both before and during the escalation. The Security Service of Ukraine and the National Security and Defense Council uncovered subversive propaganda channels and listed them publicly.

It is the lack of moderation in particular which allows Telegram to be such an enormous hub for deepfakes and disinformation.

SHADOWY TELEGRAM NETWORKS

Many of the Russian Telegram channels that you should be aware of pretend to have "insider" information on the Kremlin, from Moscow, or in occupied territories of Ukraine. Trolls and paid propagandists frequently pretend to have privileged information for the sake of sowing confusion.

Here are just some popular Russian Telegram channels with likely links to the Kremlin:

Russian TG channels linked to Kremlin. Source: *project.media*
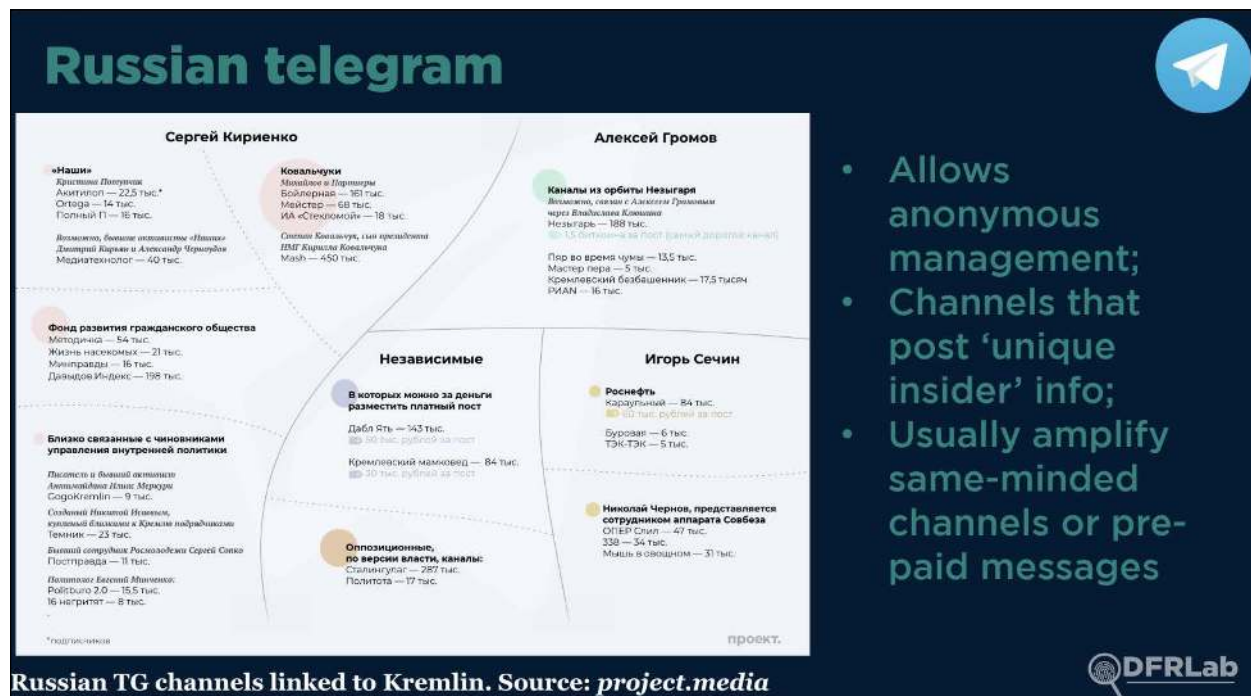
A prominent giveaway is when you see multiple channels reposting the same message. Always be wary of apparently coordinated efforts.

TOOLS FOR ANALYZING TELEGRAM CHANNELS

When it comes to researching channels, manual search will only refer you to channels that you already follow in Telegram. For more advanced searches, you will need tools like TGStat and Intelligence_X.

Note that although TGStat is the most powerful tool for Telegram analysis as of this writing, it is Russian-made and, as with Telegram itself, we recommend you use a burner phone and sock puppet Telegram account if you choose to research on Telegram.

TGstat can search deleted Telegram posts (more on that below). This feature is invaluable in propagandists' errors—for example, when they delete a report on a military strike after it is revealed the strike resulted in civilian casualties. The post below references a strike on Kramatorsk that killed many civilians, which explains its deletion from a pro-Russian channel:
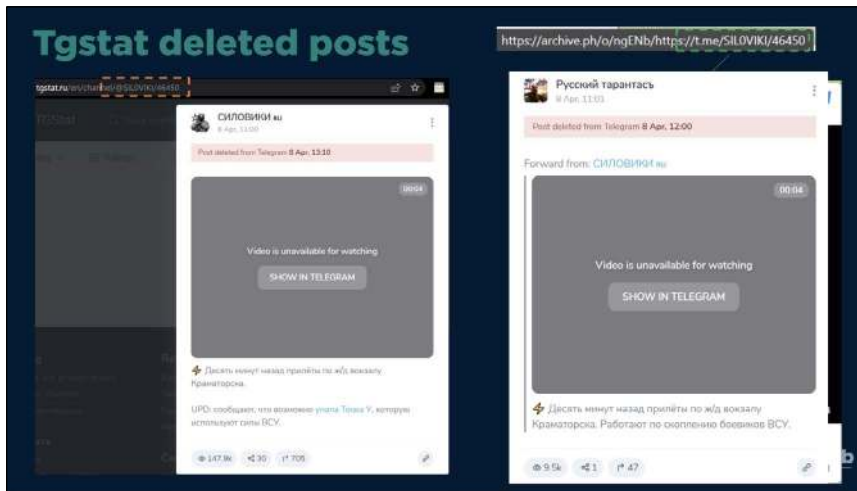
You can use Telegram and TGStat without creating a Telegram account. For the most part, TGstat archives posts and allows you to review them even if the original was edited or deleted. It is useful to spot information manipulation, check metadata of the video that was replaced, and see the original publication.

To see the post through TGStat, copy the link from the Telegram post you are interested in through the web or desktop version of Telegram. Let's say you are interested in a post by RIA at the link `https://t.me/rian_ru/168574`. To see it on TGStat, insert a part of the URL to TGStat, like this `https://tgstat.ru/en/channel/@rian_ru/168574`. Please note the part "`rian_ru/168574`" that was copied from the original link and added to the construction "`https://tgstat.ru/en/channel/@`"

The posts on Telegram are using sequential numeration, meaning that the number at the end of the URL from the channel is the post number. If you see that some page has two consecutive posts that skip one number, there is a high chance that the post in-between was deleted, so you could check it on TGStat, and if it was archived prior to deletion, observe the published info.

If you see the message, "This channel cannot be displayed," simply copy the link from the Telegram ecosystem (web app, desktop app) and paste it to any browser. This will make the post readable despite your location.

If you want to open more than a specific post, such as the 'about' page, *and* be able to scroll a bit of the channel, you can edit the URL. The abovementioned URL: `https://t.me/rian_ru/168574` needs to be modified with 's/' before the channel name to make it scrollable. So, the final link will look like this: `https://t.me/s/rian_ru/168574`.

Intelligence_X is a good tool for analyzing which channels are using the same wording. In the search below is an example which shows which pro-Russian channels are quoting the same source:
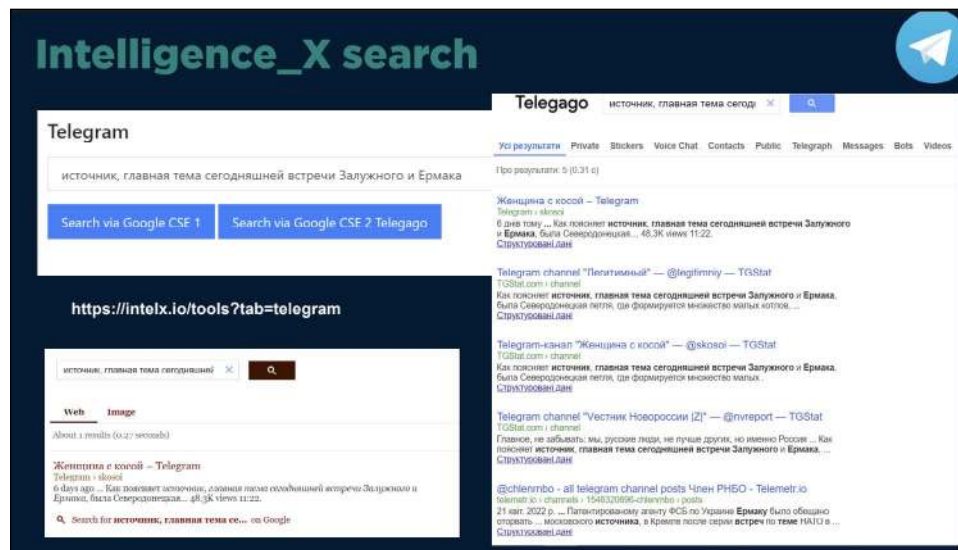
Again, Ukrainian anti-disinformation sources such as NSDC (the National Security and Defense Council of Ukraine) keep updated lists of Telegram channels tied to Russian propaganda efforts, such as the one below:

These lists can be a good starting point for anyone who is new to Telegram and is interested in exploring its vast disinformation networks.

CONCLUSION

The information environment in wartime is a fast-paced and frequently challenging space. By using the tools explored here, we hope that you can debunk disinformation safely.

When doing so, it is important to always remember the aims of any disinformation campaign: It is meant to confuse, demoralize, and exhaust its audience.

This is why it is important for any journalist and researcher to take breaks, unplug from this content, and let themselves rest. Be safe, health-conscious, and proactive—and you will be able to push back against Russian disinformation and propaganda more effectively.

ADDITIONAL RESOURCES

Below, we have included other resources of interest:

CPJ's Safety advice for journalists covering war and related unrest

War reporting: English | Ukrainian | Russian

Arrest and detention: English | Ukrainian | Russian

Civil disorder: English | Ukrainian | Russian

Internet shutdowns: English | Ukrainian | Russian

Risk assessment template: English | Ukrainian | Russian

INSTITUTE FOR SECURITY AND TECHNOLOGY
www.securityandtechnology.org

counterdisinfo@securityandtechnology.org