

# *Max Rizzuto's Portfolio*

Welcome!

In this document you will find a collection of my work which serves to illustrate my capacities as a naturally curious critical thinker with a breadth and depth of interests and capacities ranging from data analysis to teaching to graphic and research design, and more...

Reporting  
Lead Author

**AI Propaganda Will Be Effective and Easily Accessible**

The capacity of AI tools has grown in tandem with the potential threats they pose to our information space or: How AI generated images of Donald Trump's arrangement could serve as a bellwether for the future of AI propaganda.

**DC anti-mandate rally leveraged to broaden audience for anti-vax narratives**

January 23 anti-vax rally softened messaging and utilized support from anti-mandate doctors to reach broader audiences

**Extremists on Telegram exploit Parler's de-platforming to ramp up recruiting**

Rebranded Proud Boys Telegram group saw massive subscriber growth after it was converted into a refuge for Parler users

**New York City's open-source "cop watch"**

How a group of civilian volunteers monitor police activity using open-source methods

**Russian disinfo targets UK Prime Minister's hospitalization**

Russian campaign transforms Boris Johnson's supplemental oxygen support into far more ominous ventilator treatment

**Conservative group manipulates Pelosi footage to support Trump coronavirus policies**

State of the Union speech edited to make Nancy Pelosi appear dismissive of COVID-19 threat

**U.S. politicians exploit coronavirus fears with anti-Chinese dog whistles**

Political tensions rise as leading conservative politicians repeatedly term COVID-19 as a Chinese or "foreign" disease

**Tracking narratives around James Le Mesurier and the White Helmets**

How conspiracies resurfaced and shifted after Le Mesurier's death

Reporting  
Co-Author

**Kremlin outlets exploit suspicious user comments on German Navy chief's resignation**

Outlets cited suspicious comments giving the impression they represented broader German public opinion

**QAnon's hallmark catchphrases evaporating from the mainstream internet**

The conspiracy's followers on alternative platforms have failed to out-post their counterparts on mainstream ones

**Facebook shuts down Egyptian disinformation network, bans two marketing companies**

Facebook removed more than 1,700 assets linked to Egyptian digital marketing firms targeting audiences in Middle East and North Africa

**Disinfo targeting South African Defence Force surges amid COVID-19 lockdown**

South African Twitter accounts recycled old images and decontextualized videos as the country began a 21-day military enforced lockdown.

**The yellow poster behind the “no more lockdowns” protests**

How the poster spread and mutated alongside the protests

**How Manny from Diary of a Wimpy Kid galvanized political activism on TikTok**

How Manny from Diary of a Wimpy Kid galvanized political activism on TikTok

**UK-based far-right Telegram channels amplify disinfo targeting U.S. election integrity**

The flourishing domestic demand for disinformation in the U.S. attracts far-right groups from across the Atlantic

**UAE Facebook pages targeted Qatar and Muslim Brotherhood**

The multi-regional operation spread anti-Qatar content online and attacked the Muslim Brotherhood

# Collaborative Reporting

## Long-Form Reports

### [\*\*Narrative Warfare: How the Kremlin and Russian News Outlets Justified a War of Aggression against Ukraine\*\*](#)

**Atlantic Council / DFRLab.** Designed and implemented data collection tools and codifying process using Python, AWS Lambda and S3, and the Slack API. Gathered data and wrangled data from relivent sources with Selenium and Pandas for Python.

### [\*\*#StopTheSteal: Timeline of Social Media and Extremist Activities Leading to 1/6 Insurrection\*\*](#)

**DFRLab, Justsecurity.** Contributed research and a breadth of materials I had archived during my monitoring efforts in the days leading up to January 6, 2021.

### [\*\*The Long Fuse: Misinformation and the 2020 Election\*\*](#)

**Election Integrity Partnership (Washington University, Stanford Internet Observatory, Graphika, DFRLab).** Performed monitoring and managed interns and student volenteers. Lead and designed data reconciliation and cleaning process. Authored sections on data fidelity and showcased findings in several EIP's daily briefs to press, academia, and public.

### [\*\*Foreign Interference Attribution Tracker \[Github\]\*\*](#)

**DFRLab.** Led data collection and cleaning efforts and designed and monitored data pipeline. Worked with peers to establish and iterate codebook and taxonomy. Wrote the RFP for the visualization and interviewed web developer candidates. Elected to hire Mattias Stahl, who now leads Data Visualization at Der Speigel.

### [\*\*#OperationFFS: Fake Face Swarm\*\*](#)

**DFRLab, Graphika.** Led reasearch on a portion of the accounts which were connected to New Tang Dynasty pages. Provided insight on techniques for spotting GAN Generated images.

### [\*\*Dichotomies of Disinformation \[Github\]\*\*](#)

**DFRLab.** Lead and designed data reconciliation and cleaning process. Consulted on visualization design (within the confines of what partners allowed). Collaborated with peers in the iterative development of a taxonomy and codebook. Calculated and assessed coder agreement with Cohen's Kappa.

Private Research Products

# Institute for Constitutional Advocacy and Protection

In partnership with Georgetown Law's Institute for Constitutional Advocacy and Protection (ICAP) I have produced nearly of 70 weekly, daily, and special-edition monitoring reports centered on the movement of domestic violent extremist (DVE) groups operating in the United States.

The typical report details the most recent activity of DVEs with attention to how they act to effect democratic processes. The frequency and focus of monitoring reports varies as events unfold, switching from weekly to daily products around elections with special-edition reports produced in step with pertinent news events or direct action by DVEs. Reports are distributed to project partners including lawyers, community organizers, and civil society, and members of the law enforcement and intelligence community.

Credible threats highlighted in the monitoring report have been actioned on in the past.

In September 2022, I traveled to Portland Oregon to present my work to regional stakeholders and project partners.



As per the partnership, the work produced is a private research product which cannot be circulated to parties outside the project partners. I've tried to outline what the work looks like in my portfolio with respect to my agreement with ICAP, but it does leave a bit of a hole in my published outputs.

## Private Research Products

# Unofficial ISIS Website Uses Blockchain Tech to Evade Deplatforming

In August 2021 I discovered a network of sites promoting the recruiting materials, media publications, and instructional tutorials from the Islamic State of Iraq and Syria (ISIS). The most interesting of the sites was one by the name “oqq.lv” which hosted a breath of materials and was frequently updated. The site’s address did not appear widely on social media, instead traffic was routed through a number of proxy sites hosted on the InterPlanetary File System (IPFS). Hosting the proxies which fed the site on the decentralized file system would place them out of reach of governing bodies. In order to make sure that the sites remained accessible to those seeking to access ISIS, the Ethereum Name Service was employed to tie the IPFS hash to a human readable “.eth” domain. One such proxy was “elokab.link.eth” which has since been withdrawn, however records remain.

The screenshot shows the Ethereum Name Service (ENS) registration for the domain `elokab.eth`. At the top, it says "The Ethereum Name `elokab.eth` resolves to this Address: `0xb0a0fdc52e2ba7a08b0efe41ff9f5863d1eddb9a`". Below this is the "Overview" section, which includes fields for Controller (with address `0xb0a0fdc52e2ba7a08b0efe41ff9f5863d1eddb9a`), Registrant (with address `0xb0a0fdc52e2ba7a08b0efe41ff9f5863d1eddb9a`), and Expiration Date (set for July 14, 2022, at 02:07). There is also a "Related Transactions" section with columns for Transactions, Age, From, and Actions.

Screenshot of Ethereum blockchain where ENS is used to connect the IPFS hash

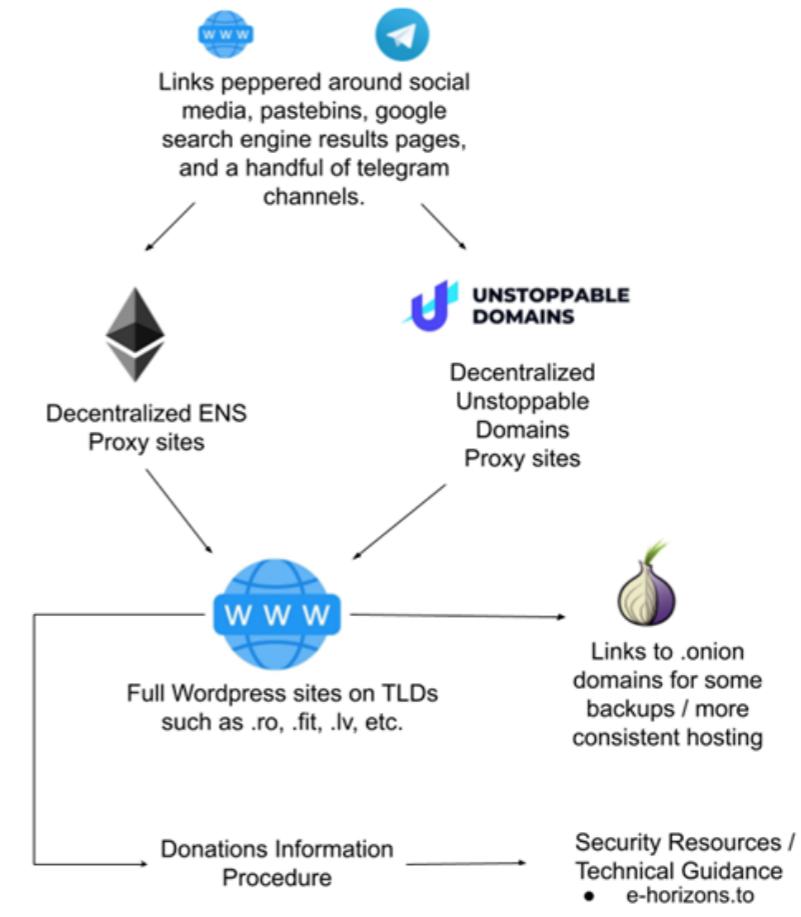


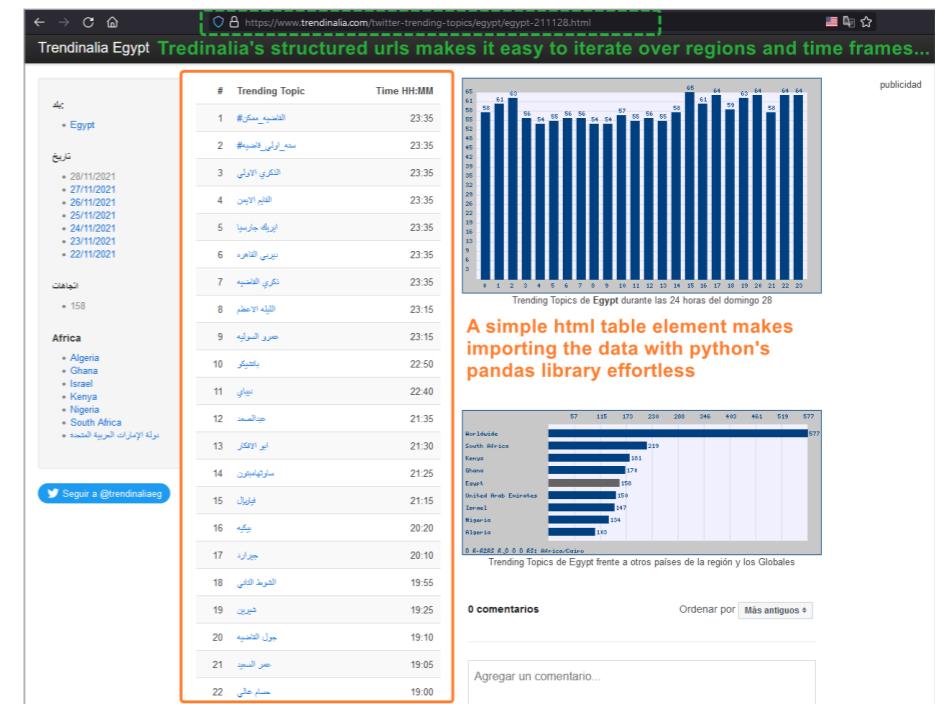
Illustration of how the site and its proxies work to connect users to recruiting materials

Once past the proxies and on the actual site, instructions directed users to telegram channels, onion domains, and resources for more technical guidance. At the time of the initial research in August, the site and its proxies operated in a structure illustrated in the diagram above.

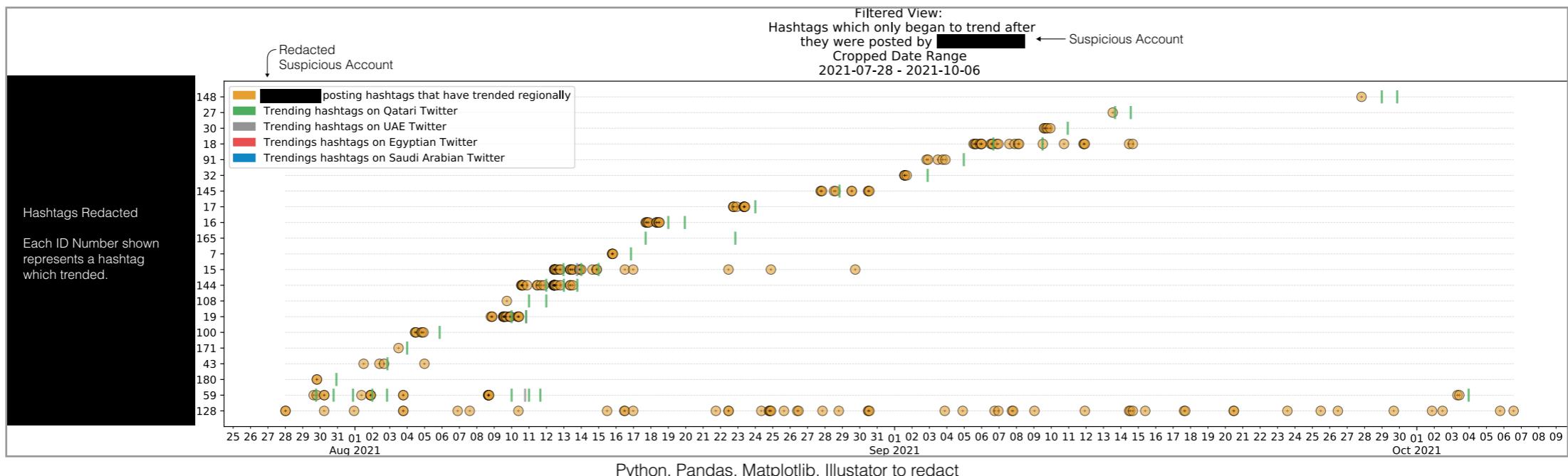
## Private Research Products

# Qatari Twitter Influencer

A tip alerted us to the activity of a Twitter profile which was able to make original hashtags trend, sometimes within minutes of posting a hashtag for the first time. In order to test this hypothesis I scraped the website trendinalia.com to get a record of terms as they trended on Twitter in Qatar, Egypt, and Saudi Arabia from 2019 to Present. I then scraped all of the Tweets from the suspicious Twitter user and extacted the dates and times of every hashtag used. This chart (which is actually a modified scatter plot) illustrates how the user pumps hashtags in their Tweets (orange circles) and in just a short time the same hashtags trend (as indicated by the colored bars) in various regional Twitter spaces.



Annotated screenshot of Trendinalia's trending records



## Education Materials

# “Artificial Intelligence” Enabled Disinformation

**Mechanized Harm**

This kind of exploitation was not unforeseeable considering the computer science cannon.

Lena.png  
First ever CRT image  
See losinglena.com

**What is Artificial Intelligence?**

DATA FEATURES + - 2 HIDDEN LAYERS OUTPUT

**A.I. to Deceive**

**The Liars Dividend**

The mere existence of deepfakes and other forms of hyper-real manipulation afford liars with greater capacity to deceive by simply citing the efficacy of these techniques.

"Deepfakes will make it easier for liars to deny the truth in distinct ways." (Chesney 2018)

e verifiability of led to erode ice previously ges and video.

**A.I. to Deceive - Video**

**DeepFake**

target video source video

- Manipulated video
- Mouth Movement is altered to accommodate translated audio
- Unaltered video
- Subject's mouth is manipulated in target video to match English translation

**A.I. to Deceive - Images**

GAN Profile Pictures supporting Argentine Kirchner movement

DFRLab and Graphika

Graphika and SIO

GAN profile pictures from a network of accounts on Facebook associated with the Epoch Times

Some slides from one of the training sessions

“DeepFakes” and “Artificial Intelligence” are both widely misunderstood technologies. Having focused my undergraduate thesis on DeepFakes and continued that work into my research career, I have taken the lead on all trainings and internal capacity building related to AI enabled deception techniques, how they were developed, how they are used, and how to research their application in various information spaces.

In the presentation of my research, I attempt to deescalate the perceived threat these technologies pose and explain the underlying statistical principals behind the discipline such that trainees can more easily understand the true capabilities, spot their identifying artifacts, and approach their research with a more nuanced perspective.

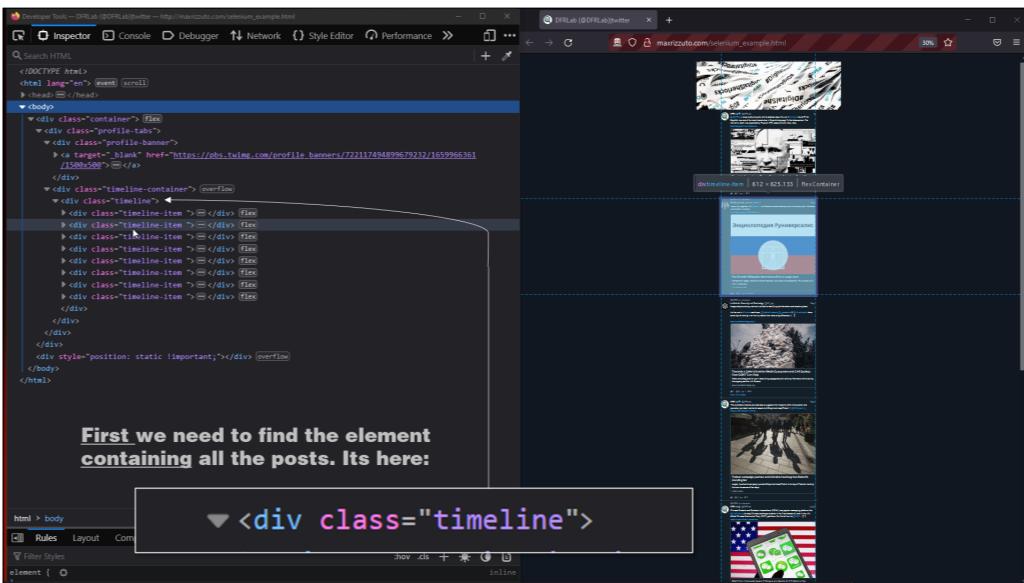
# Internal Capacity Building

## Suite of Scrapers

Data access continues to be a challenge for internet researchers. In the past few years we've seen platforms roll back API and researcher access while communities have fragmented across a host of alternative sites. In an effort to regain some ground and elevate the work of my team, I developed a suite of website scrapers using Python, accompanied by a detailed training on how to write and deploy purpose built scrapers on any site (except Facebook).

The suite of scrapers cover general data collection for accounts and keywords for Gab, GabTv, Parler, Gettr, Rumble, Odysee, RuTube.ru, Patriots.win, TGStat, and two prominent 4chan archives (4plebs and desuarchive). The tutorial and training session I put together also included a [static sample site](#) based on a simplified clone of Twitter and a scraper for educational purposes.

To accompany the slides there is also a [Google Colab](#) where participants can follow along with the introductory steps of the process.



Screenshot of a slide from the training session outlining how the scraper should navigate the basic structure of the website.

Some more slides, why not.

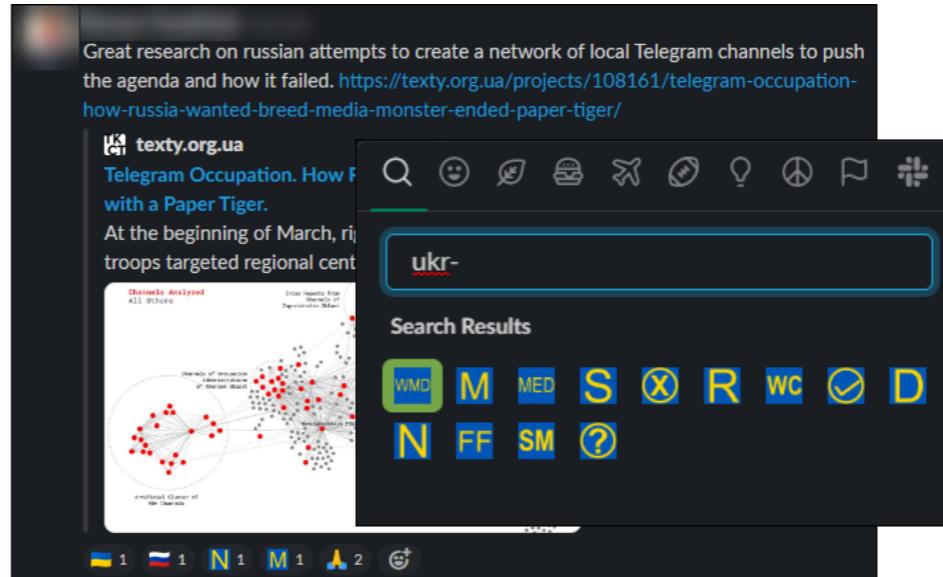
## Internal Capacity Building

# Collaborative Research Repository using Slack

In the immediate aftermath of Russia's full scale invasion of Ukraine in February 2022, I began ideating on a process for our research team to collectively archive and codify events as they developed. Soon after, I deployed a solution that meshed with our research team's existing slack channel, that would not task our researchers with any undue work, and would add considerable value to their collective monitoring efforts. The data collected by my tool was the subject of a mainstage presentation at the [360/OS](#) conference in Brussels, the foundation of a partnership with Stanford University's Starling Lab, and will be featured in a forthcoming DFRLab report.

A	B	F	G	H	I	K	L	N	O
index	message	datetime	text	urls	attached_text	attached_ts	attached_author	country_codes	all_codes
2399	Reply	2022-03-06 16:26							
2400	1330 Post	2022-03-06 16:05	["https://twittt/#Russia's sta [1646581595, 1] 'Julia Davi [ ]						['narratives', 'false flag']
2401	1331 Post	2022-03-06 16:17	["https://twittt/'Message fror [1646576858] 'peter por [ ]						['security', 'war crime']
2402	1332 Post	2022-03-06 16:25	["https://tass.r [ ]						['narratives']
2403	Reply	2022-03-06 16:40							
2404	1333 Post	2022-03-06 17:55	["https://twittt/'The ludicrou [1646588943, 1] 'Ben Collir [ ]						['narratives', 'false flag']
2405	1334 Post	2022-03-06 18:14							['narratives', 'false flag']
2406	1335 Post	2022-03-06 18:16	["https://twittt/'Let's discuss [1646580934] 'Kamil Gal [ ]						['narratives']
2407	1336 Post	2022-03-06 18:32	["https://twittt/'Russia aircr [1646591056] 'Franak Vi. [belarus flag] [ ]						['security']
2408	1337 Post	2022-03-06 18:42	["https://twittt/:exclamation [1646591544] 'MFA Russ [ ]						['narratives', 'false flag']
2409	1338 Post	2022-03-06 19:33	["https://twittt/'Horrifying fo [1646594964] 'Golnaz Es [ ]						['war crime', 'graphic', 'security']
2410	Reply	2022-03-06 19:33							
2411	Reply	2022-03-06 19:40							
2412	1339 Post	2022-03-06 21:11	["https://twittt/'Dear friend! [1646590751] 'Kamil Gal ['china flag] [ ]						
2413	1340 Post	2022-03-06 21:32	["https://twittt/'Outside the F [1646579269] 'Mike Gals [ ]						
2414	1341 Post	2022-03-06 22:55	["https://twittt/'Russia Recrui [1646606398] 'Nancy Yoi ['sryia flag] [ ]						
2415	Reply	2022-03-07 00:25							
2416	1342 Post	2022-03-06 23:18	["https://twittt/:exclamation [1646608349] 'MFA Russ [ ]						['false flag', 'narratives']
2417	1343 Post	2022-03-07 02:57	["https://twittt/'Have any Rus [1646621495, 1] 'Emerson [ ]						['social media', 'narratives']
2418	Reply	2022-03-07 02:55	["https://t.me/ 'Внимание се [ ]						
2419	Reply	2022-03-07 03:00							
2420	Reply	2022-03-07 08:15	["https://www ['Google, Metz [1646253711] [ ]						
2421	1344 Post	2022-03-07 03:40	["https://www ['Chemical wh [ ]						['security']
2422	1345 Post	2022-03-07 04:15	["https://www [ ]						['plugotare']
2423	1346 Post	2022-03-07 05:35	["https://twittt/'Вооруженн [1646630485] 'Ленга,ovy [ ]						['refugees']

A sample of the Excel formatted output of the data. Several columns are hidden for brevity.  
Additional pages are generated automatically to show filtered outputs of the data.



Screenshot of a codified post on the #ukraine-research slack channel and the project's custom emojis

Python code run remotely on AWS servers collects all new posts from the Ukraine research team's slack channel and saves any images or files posted, and archives all URLs on a cloud server. The slack channel contains several custom emojis that enable researchers to codify their contributions in real time with categories such as: "WMDs," "false-flag," "war crimes," and others. The data collected has been instrumental in the DFRLab's collaboration with Stanford University's Starling Lab which used portions of our data as a platform for their Web3 based digital evidence certification program. At this time the dataset numbers roughly 10 thousand archived assets and is still used every day. The program is entirely autonomous.

# Internal Capacity Building

## Inter-coder Reliability Toolkit

**Case selection field**

**Research questions posed to coders**

**Coders responses and indication of agreement or discord for each question**

**Reconciliation field for review and correction of incongruent values**

All data entry ranges react to coder selection field

Annotated screenshot of the reconciliation user interface where project managers would review inter's data entry tasks.

When embarking on the task of building a dataset using inter-coder reliability it is imperative that project managers have a trusted, transparent, and reliable tool for processing data. I created this tool with zero overhead that enables project management to view and reconcile the entries of coders. This enabled our team to assess the efficacy of our dataset as cases were coded, and to iteratively improve our language as

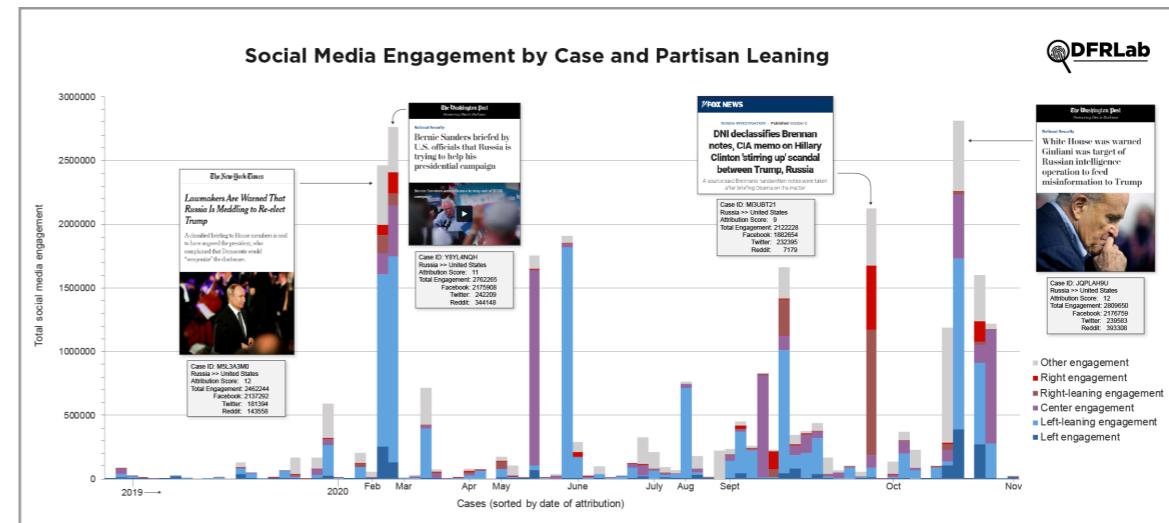
the project advanced. Part of this process is based on an utter abuse of free Google services wherein a data aggregator based in Google Colab would create and populate a new workbook in a Google sheet for each case. The resulting data was accessed from a master document which treated the external document as a sort of relational database. This tool was used for the DFRLab's [project](#) with Google Jigsaw, [The Foreign Interference Attribution Tracker](#), and [The Election Integrity Partnership](#).

## Design Work

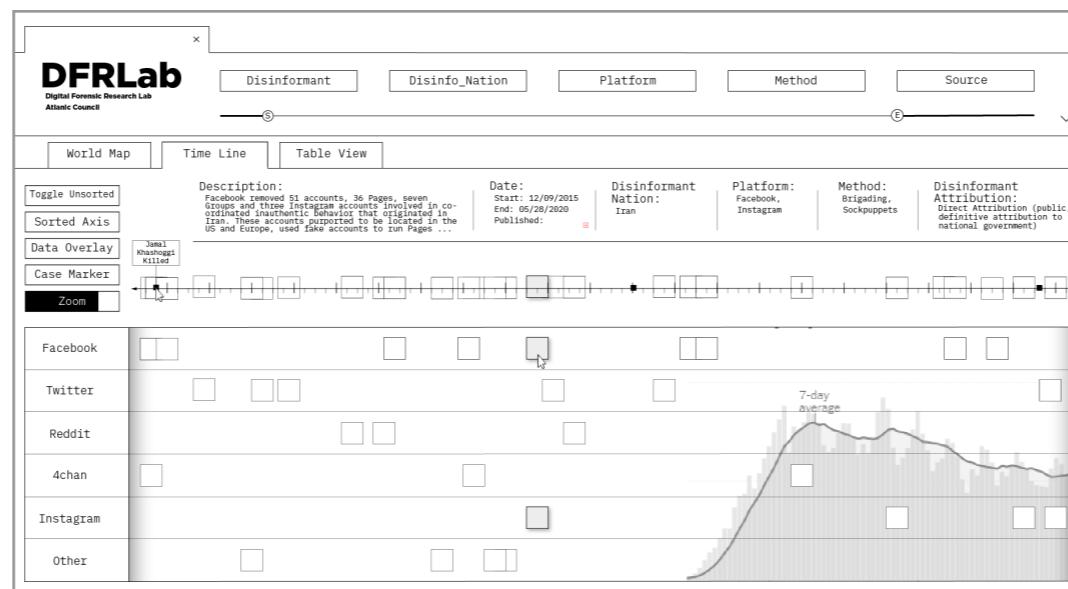
# Graphics made for the Foreign Interference Attribution Tracker



Banner graphic for the Atlantic Council publication on the Interference 2020 project



Plot of the dataset stacked by attribution source partisan leaning



Pre-Alpha mockup of a possible user interface for navigating the dataset.

## Design Work

# DFRLab Website Redesign Mocks

As the DFRLab works to establish a more original online identity and move away from Medium for hosting reporting, I took the opportunity to play with some visual ideas that could compliment our reporting, while aligning with Atlantic Council design expectations. This example serves to demonstrate my familiarity with Adobe Illustrator.

**Concept for Re-Styling AC Publications on the DFRLab website and for DFRLab Reports:**

The Image on the left features an article published to AC's website, reformatted to appear in a DFRLab style, tags are transferred over from the AC website (and truncated). The Image on the right is a DFRLab report similarly stylized. My thinking was that reports and posts from AC may be formatted more extravagantly than our normal research and publications.

**Concept for website taxonomy stickers**  
Inspired by Github shields ([github.com/badges/shields](https://github.com/badges/shields)), the badges are colored by category.

To the right of the report mockup, a note says: "Took with a simplified DFRLab logo that resizes a little better."

Wordpress element ideation

Thats all folks.

I hope you've enjoyed reviewing my  
application materials.

If you have any questions, or would like more  
information about anything I included or didn't  
include, please don't hesitate to drop me a  
line at: [maxbrizzuto@gmail.com](mailto:maxbrizzuto@gmail.com)

