Visualizing fakenews as reported by euvsdisinfo.eu

Jesper Henrichsen
Supervised by: Pedro Ferreira

December 15, 2017

Contents

List of Figures

1 Introduction

Misinformation, and in turn: *fakenews*, is not a new phenomenon, on the contrary, it far predates modern day in the information age with social media and an ingrained expectation of internet access independent of time and place. Even a sense of a printed distribution of misinformation dates as far back as the 18*th* century where, in London, the printed newspapers would publish snippets with stories from questionable sources [4]. The same article provides an insight into how compromising information already then had political impact and played a part in the public support for the execution of the queen of France, Marie Antoinette. This was inspite the fact that it was not possible to publish news of the sort avaiable in London, so snippets were left on benches in the parks of Paris [4].

Since the introduction of the internet, information has been able to reach further and faster than ever before. Recent developments of omnipresent social media has created the perfect platform for the spread of this information within the internet. In 2016, 62% of americans received their news from social media [6]. For the sake of advertisement social media platforms has, since their introduction, only become better at targeting their audience with information that will capture their attention. As put by the team behind the newsfeed at Facebook: "*The goal of News Feed is to deliver the right content to the right people at the right time (...)*"[1]. However, a relevant question would be to whom it is implied to be *right* for. That it is not necessarily the user, has recently emerged as a likely answer.

The nature of social media has proved to be an effective way for the spread of information, genuine as well as fake.
This report will describe the process of scraping and visualizing information from euvsdisinfo.eu, an EU run campaign that debunks pro Kremlin news stories. One objective of this project was to investigate whether these cases could be used to view fakenews as attacks. And if so, could there be identified a perpetrator either as an outlet or country, and a victim such as the country being mentioned in the information.

2 Background

The concept of *fakenews* is not a new invention. The term emerged on the public conscious especially during the 2016 american presidential election, where it was mostly used as a deflection of criticism. However, the underlying properties of the recent years fakenews stories are heavily influenced by authentic, mainstream journalism. Some of these properties, in the form of sensationalism which is a type of exaggeration for the purpose of further circulation, occured already in american press in the late 19*th* century and was refferred to as *yellow journalism* [13]. The yellow journalism brought about sensationalism and

[1] See: https://www.facebook.com/business/news/News-Feed-FYI-A-Window-Into-News-Feed

eyecatching headlines which in todays digital world is equivalent to what is commonly denoted as *clickbait* titles. Also, just as yellow journalism was about monetizing on circulation, so is much of the fakenews today, but perhaps with the distinction that today, anyone can become the publisher. To exemplify this, a Macedonian village was traced as the origin of many fakenews websites that appeared during the 2016 american election, the incentive was to profit on the generated traffic through advertisement [9].
The notion of clickbait refers to articles with titles that leaves a cliff hanger in order to lure the reader to follow a link to the outlet that hosts the article. Therefore, titles are as important as ever for the circulation since content sharing on socialmedia often only leaves limited space to include relevant information. That fakenews has been successful in terms of exploiting the properties necessary for circulation on social media is highlighted by the fact that the most popular fakenews stories were shared more than the most popular mainstream news stories [2]. The fact that socialmedia targets their content towards the endusers individually tends to accellerate the sharing of certain news more rapidly than ever before. This targeting of content also has the effect of creating so called *filter bubbles* for the end-user, where they do not see an evenly distributed sample of the content available, but rather a predefined subset that by socialmedia platforms is deemed more likeable for the users to engage with.

Despite a common claim to oppose fakenews, a consensus of when a story can be labelled as fake is diffuclt to distill. Largely because the term itself has become part of a tactical repetoire for deflecting unwanted criticism. Though more importantly is the inherent opposing interests that gave birth to the stories in the first place.
Hunt and Matthew suggests that from an economical perspective fakenews materialize from an equilibrium between producers and readers. The fakenews is much cheaper to provide rather than authentic news. While for the reader it is not costless to deduct inaccuracies, and the reader might even enjoy the partisan news [2]. The last part consequently means that the fakenews provides utility for the reader, though at the cost of providing the reader with a false state of the world.

Therefore, as the fakenews is hard to distinguish from authentic news as illustrated by *A field guide to fakenews* [10], the challenge arises to combat the false information. In Europe the experience in later years has been dominated by a narrative battle that has especially unfolded over the Ukranian conflict [8]. This presents a reason for the existence of fakenews articles different from the objective of monetizing on circulation through ads. The fight for a narrative through information spread online, is reminscent of traditional propaganda, with the obvious exception that it utilizes modern technologies.
Although fakenews might pose a threat to the common empirical foundation that is implicitly assumed by a democratic society, the multifaceted properties of fakenews makes it a difficult problem to approach [1]. For this reason, there exists many initiatives that seeks to debunk the false information. Examples

of such are the privately run fact-checking website, http://snopes.com, which historically has focused on debunking or validating urban legends. Another site is the ukrainian fact-checking site: http://stopfake.org, a domain bought in 2014[2].

This report focuses on the debunked cases provided by euvsdisinfo.eu, even though both of the fact checking websites listed above has existed for longer. The reasoning for this choice, is that for the purpose of this project, the euvsdisinfo.eu was sufficient as it provided access to a wide variety of cases in a structured way. At the same time it is an interesting aspect that the repository is maintained as an EU funded campaign.
The campaign has existed since 2015 and is run by the European External Action Service East Stratcom Task Force. The primary focus of the campaign is to identify and debunk pro-Kremlin disinformation. The campaign includes cases of debunked information from sources spanning from official news sites to twitter accounts, to non-online content such as interviews. The website euvsdisinfo.eu includes, at the time of writing, more than 3400 such cases, these are the cases that this report is based on. The cases are all reported either by the campaign staff themselves, or one of the 400 collaborating organizations and individuals. In fig. 1 is seen how cases are listed on the website, the order of which is chronological with respect to the date it was reported.

[2] See whois: https://whois.icann.org/en/lookup?name=stopfake.org

Figure 1: Example listing of disinformation cases on euvsdisinfo.eu

02.11.2017	Brussels are closing the door they opened with visa freedom for Georgians	Rezonansi	Europe, Georgia
02.11.2017	EU wants to ban information about the of country of origin on the food labels	Vlastenecké Noviny, eOdborar.cz	Italy, EU
02.11.2017	The West supported the terrorists during hostage crisis in Dubrovka in Moscow ("Nord-Ost attack") in 2002 and in the school of Beslan, North Ossetia, in 2004	Vremya pokazhet @Pervyi kanal, 19:15	Russia, The West
02.11.2017	The US destroyed the European values and culture, so now Russia is the only flagship of the European civilization	Vremya pokazhet @Pervyi kanal' TV-channel, 41:08	Europe, US
01.11.2017	The EU teaches journalists how to properly inform about Islam and migrants	ac24.cz	Ireland, Italy, Austria, Slovenia, Hungary, Greece, EU, Germany, Spain
31.10.2017	Finland wants Russia to join the European Centre of Excellence for Countering Hybrid Threats	Sergei Lavrov, Russian Foreign Ministry's website	Russia, Finland
31.10.2017	The West, primarily the United States, is collecting biological material in Russia to create a biological weapon that destroys the Russians.	Mesto vstrechi @NTV TV-channel, 1:12:48	Russia, The West, US
31.10.2017	Czech MP prefers there were 5 million Muslim migrants in Czech Republic rather than 5 million voters of Czech president Miloš Zeman	BezPolitickeKorektnosti	Czech Republic
31.10.2017	Estonia has opened a new military base in the town of Tapa under the pretext of fear of a Russian attack.	cz.Sputniknews	Russia, Baltic states, Estonia
31.10.2017	US is using sanctions in trying to push Russia out of the European energy and arms market	cz.sputniknews	Europe, Russia, US

As seen by fig. 1, the cases are listed showing the date they were reported, an english title to the story, a name of an outlet that published the story, and a country of origin.

3 Acquiring a dataset

In this section, the approach to acquiring and extracting information for visualization will be described. The initial dataset was scraped from euvsdisinfo.eu, however, this dataset was gradually extended in a number of steps. These steps will be described in this section.

3.1 Scraping the cases

The cases listed at euvsdisinfo.eu consists of information regarding the case, such as who reported it, in what country or countries did it originate in, as well as the disproof that debunks the information as invalid. Other information for each case is meta information about the information and its source. In fig. 2 is seen an example of the information listed for a specific case.

Figure 2: An example of the information for each case

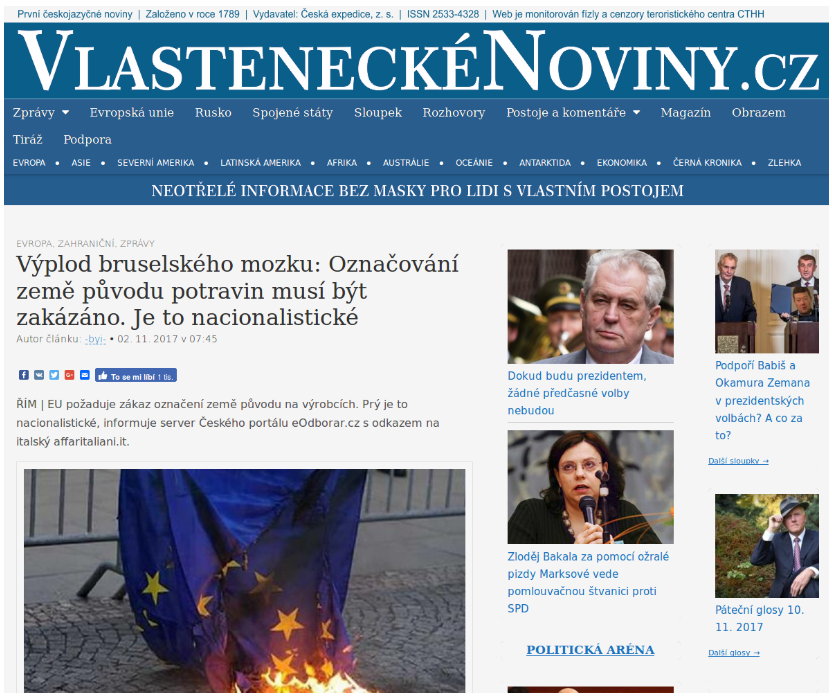
There is no API, or otherwise download button on the campaign website to get the whole dataset as is. However, there is no mention in their `robots.txt` file that indicates that scraping is not permitted. Therefore, the intial dataset was achieved after writing a scraper in Python[3]. The list of cases is an overview list with a pagination of 10 cases per page, an example of this list is shown in fig. 1. The offset is given by the URL, and so the crawling to acquire links to each specific page can be done in a well defined way, without having to worry about the specific structure of the website. However, parsing of the structure of the website is necessary in order to scrape the information of each specific case. For this, the python library BeautifulSoup[4] was heavily used.
In the end, the information was saved into a csv file containing one disinformation case per row, and in total 3071 data rows.

[3] https://github.itu.dk/jeshe/fakenews-scraper/blob/master/news_scraper.py
[4] https://www.crummy.com/software/BeautifulSoup/

3.2 Article scraping and content extraction

In order to get more information than was already available for each case at euvsdisinfo, information from the original source was also included and added to the dataset. This section will describe the approach that was used in order to reliably get information across the many differently structured websites.

Figure 3: An example of a debunked news article from a Czech website



A general approach to extracting content is difficult because source of information can be any sort of media, whether digital or physical, in writing or a video. And, because each website is different, then even building a scraper to extract the content of the subset of sources that are online articles, will be difficult. In fig. 3 is seen an example of a source article.

One important property for the purpose of this project is that in order to consider the names of locations that are being mentioned in the articles, the entire content is not strictly necessary. Therefore, I chose to use the meta tags to extract information about the content, summary, titles, author, and descriptions of each online resource. I would also filter on html tags such as the header tags, `h1`, `h2`, `h3`, `h4`, `h5`, `h6` as well as the `title` tag used for setting the window title. I found through experiment that only considering the first occuring header tag worked best, the reason is that other header tags than the first one would often be titles of other news articles that the news site wants the user to click on.

Figure 4: Meta tags defined in python scraper

```
metatag_list = [
    ("name", "description", "content"),
    ("property" "og:title", "content"),
    ("property", "og:description", "content"),
    ("name", "twitter:title", "content"),
    ("name", "twitter:description", "content"),
    ("name", "language", "content"),
    ("name", "keywords", "content"),
    ("name", "subject", "content"),
    ("name", "topic", "content"),
    ("name", "summary", "content"),
    ("name", "subtitle", "content"),
    ("itemprop", "name", "content"),
    ("itemprop", "description", "content"),
]
tag_list = [ ("h%s" % i, None) for i in range(1, 7) ] + [("title", None)]
```

Extracting content by meta tags proved to be a very reliable approach, since most news sites are interested in their content being shared. So, in order to optimize sharability almost all online resources had optimized for search engines, often reffered as just: *SEO*. In fig. 4 is seen the defined metatags that the scraper was looking for, defined in the variable: `metatag_list`, as well as the list of header and title tags defined in `tag_list`. Each metatag is defined as a tripplet. The first value defines what attribute to look for when finding a HTML tag of type `meta`, the second what value such attribute should have. When a match is found for the first two, then the third string in the tripple is used to know from what attribute to extract text from. In the metatags listed in fig. 4 all content was extracted from attributes of the same name regardless of the match on the first two. However, defining triples makes this method generalize to any other metatags that might be relevant to add in the future. The reasoning behind the list of other HTML tags being defined as tuples, is similar. Although, for my purposes, the second string was set to `None`, in which case the script would scrape the inner HTML of the element instead of the content of a named attribute.

In order to avoid duplicating content as much as possible the content of a meta tag or html tag was compared to the content that was already found in previous tags. This approach resulted most often in a short paragraph of information about the article, including keywords, title and summary. Before applying the approach to the articles scraped from euvsdisinfo.eu, it was tested on arbitrarily chosen articles, such as articles from danish news outlets. It was also tried on

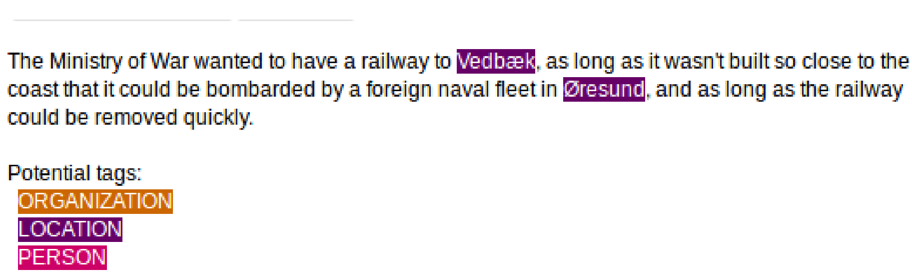
a sample of articles taken from the subreddits: r/politics, r/news, and r/worldnews[5], because these were collections of news articles with a good variety of news outlets. The results were used to evaluate qualitatively on the smaller sample. None of which turned out to have no content, and only one resulted in an extract only consisting of keywords. Interestingly, among the keywords for that particular result were also the name of the country that the news story revolved around.
One thing that was clear from this, was that locations were not always mentioned if the news concerned well known state leaders such as Putin, Merkel or Trump. In such cases, often only the names of the state leaders were present as indication of what countries were mentioned in the articles.

3.3 Named entity recognition

One initially desired outcome was the possibility to extract location information about what countries were being mentioned in the articles. This section will describe the approach to using stanford NER tagger to quantitatively extract location names from the meta information acquired for each article.

Named entity recognition is a research field within natural language processing concerned with recognizing names of things such as people, company names, or, as relevant for this project, locations. The study of recognizing location names within texts is one of the most studied areas of named entity recognition, however, still an ongoing research. As such the NER tagger used in this project is released open source as part of the Stanford nlp library[11] which also includes many other models and methods relevant to the field of natural language processing. A more in depth explanation of named entity recognition or even natural language processing, is however, beyond the scope of this project. In fig. 5 is seen an example of tagging a sentence using the graphical interface of the NER tagger. The sentence in fig. 5 is arbitrarily chosen from Wikipedia, and is not part of the content of the dataset.

Figure 5: NER tagging on a sample sentence



The input that was given to the NER tagger was the concatenation of title,

[5] https://reddit.com/r/politics+news+worldnews

summary (as provided by euvsdisinfo), keywords, and the meta tags content scraped from each individual site.

3.4 Facebook likes

The initial dataset, provides only a uniformly weighted list of debunked news cases. In order to provide different weights to the articles in any future visualization, each source URL in the dataset was looked up via facebooks open graph API. The result of the API lookup was a mapping for each source article to a number of likes on facebook, in the case that the information was ever shared on facebook. In fig. 6 is seen the essential part of the python code used for fetching the number of likes of each url. The function get_shares takes as argument a url and returns dictionary of the response from Facebook's API.

Figure 6: Fetching facebook likes for each source URL

```
def get_shares(url):
    enc_url = encode(url)
    access_token = get_access_token()
    fields = "og_object{engagement}"
    api_endpoint = "https://graph.facebook.com/v2.11/%s?fields=%s&access_token=%s"
    return requests.get(api_endpoint % (enc_url, fields, access_token)).json()
```

4 Results

In this section findings findings and results achieved through the process described in the previous section will be presented.

4.1 Overview

The resulting dataset from the previous section includes 17 columns as can be seen in table 1.

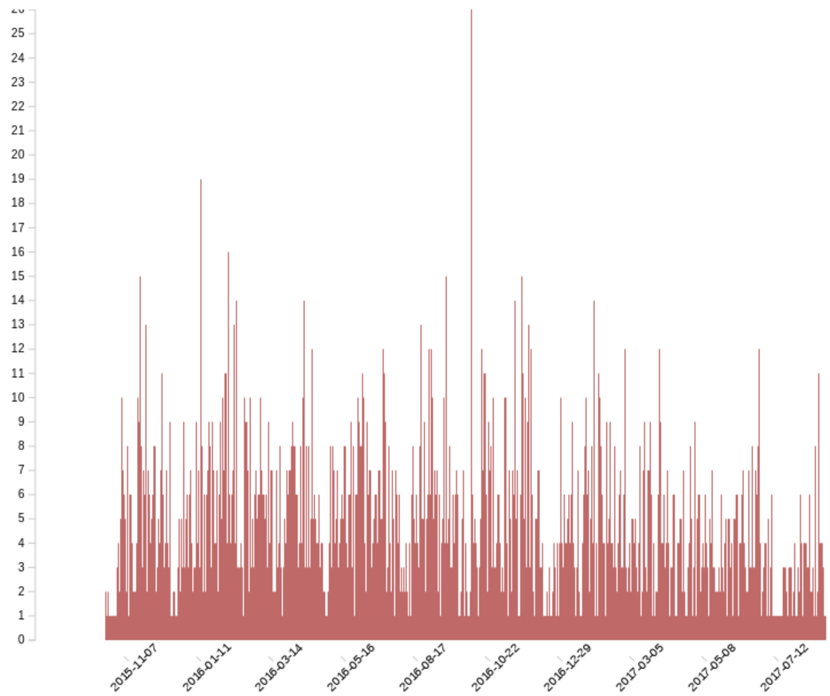
Table 1: Resulting columns in the dataset

Column name	**Description**
`issue`	The issue number refers to the review the case was published in as given by euvsdisinfo.eu.
`date`	The date the case was reported.
`outlet`	The outlet that published the information.
`language`	The language the information is provided in.
`origin`	Origin of the story, this is sometimes a satirical piece from a different country.
`reported by`	The person or organisation who reported the case.
`keywords`	Keywords describing the published piece of information.
`source`	The URL to the original story, this is not always present i.e. if the source is an interview.
`title`	The title of the debunked information.
`summary`	The summary of the information that was debunked.
`disproof`	The reasoning for `euvsdisinfo` to flag the information as dishonest.
`metatags`	The types of metatags that included information from the original source during scraping.
`metatags_content`	The content of the metatags that was scraped from the original source.
`locations`	Any locations found by the NER tagger.
`misc`	Miscellaneously tagged words or phrases tagged by the Stanford NER model.
`people`	Recognized names of people by the NER tagger.
`likes`	Number of facebook likes registered to the source URL, if any.

The last 6 columns of table 1 are additions to the initial dataset acquired from euvsdisinfo.eu, namely: `metatags`, `metatags_content`, `locations`, `misc`, `people`, and `likes`.

In fig. 7 is seen the number of articles per date over the period of time that the campaign has been reviewing news information. As seen from the figure, the spread of articles reported over the period remains roughly similar. The graph was created using rawgraphs.io[12].

Figure 7: Articles over time



As seen in fig. 7, there is a spike in the middle, on 16th october 2016. The spike is largely due to one russian twitter account: `Vremya pokazhet` that accounted for 10 of the 26 reported cases on that day.

4.2 Victims and perpetrators

In this section, the focus will be on the findings that could be of interest towards the initial objective of trying to identify victims and perpertrators in terms of fakenews.

4.2.1 Locations

The most mentioned location is, expectedly, Ukraine. Equally unsurprising is the most frequent language, russian, given the focus of the task force behind the campaign on pro-Kremlin news. The top 5 mentioned locations and the 5 most frequent languages is seen in fig. 8.

Figure 8: 5 most frequent languages and top 5 mentioned locations

language	**% of articles**	**location**	**% of articles**
Russian	55	Ukraine	27
Czech	16	Russia	23
English	9	USA	21
Slovak	2	Europe	8
Georgian	2	Syria	5

In general the NER tagger performed well, only 426 of the 3071 cases did not have any locations tagged. A sample of the articles tagged is shown in fig. 9. The articles shown were chosen based on having the shortest titles in the dataset, simply because they would be easilier presented while still illustrating the performance of the NER tagger. As can be seen from fig. 9, most sources have recognizable locations which seems intuitively correct given the title. However, at least one in these samples, have falsely tagged locations such as `PravdaReport`, and the word `Having`. Since measuring such false positives and equally false negatives, cannot be done quantitatively, this inspection has only been done manually on similar samples. However, it is safe to say that the tagged locations cannot be taken for granted as there will be noise in terms of falsely tagged locations. With that in mind, it can serve as a way of depicting the general pattern of locations named in the disinformation sources.

Figure 9: Sample of cases shown by their title, language and locations

title	**language**	**locations**
Crimea decided its own fate	Russian	Crimea,Russia,China,India
Ukraine is a neo-Nazi state	Russian	Ukraine,West
NATO is encircling Russia.	Czech	Russia
Ukraine is governed by Nazis.	Russian	Ukraine
Sweden wants to leave the EU.	Spain	Sweden
Georgia is a US colony.	Georgian	Georgia,US
Ukraine has a Nazi identity.	Russian	Ukraine
Ukraine is a part of Russia.	Russian	Ukraine,Russia
Savchenko is a US spy.	Russian	US
Nazis control Ukraine.	Russian	Ukraine
NATO kills Serbian children.	English	PravdaReport,West,Russia,Having, Syria,russia,Serbia,Yugoslavia
Ukraine is governed by nazis.	Russian	Ukraine
All Ukraine is Russia.	Russian	Ukraine,Russia

4.2.2 People

The NER tagger also tagged names of people being mentioned in the input, given to it. Filtering these tags for mentioning of *Hitler* as well as keywords such as *nazi* revealed a pattern of sentiment in the news. The number of articles including one or both of the words, including derivations of the two, was 137 articles. 68% of those articles were written in russian and 38% were both written in russian and mentioned Ukraine.

Another finding when looking at the most mentioned names, according to the NER tagger, the name Yekaterina Strizhenova, appears above both Vladimir Putin and Petro Poroshenko, and with some margin. Yekaterina Strizhenova, who appears by her name spelled in cyrillic as seen in table 2, is a hostess of a TV show called *Good Morning* on russian Channel One [3].

Table 2: Most frequently mentioned names

Name	**Number of appearances**
Екатерина Стриженова	68
Vladimir Putin	39
Petro Poroshenko	35

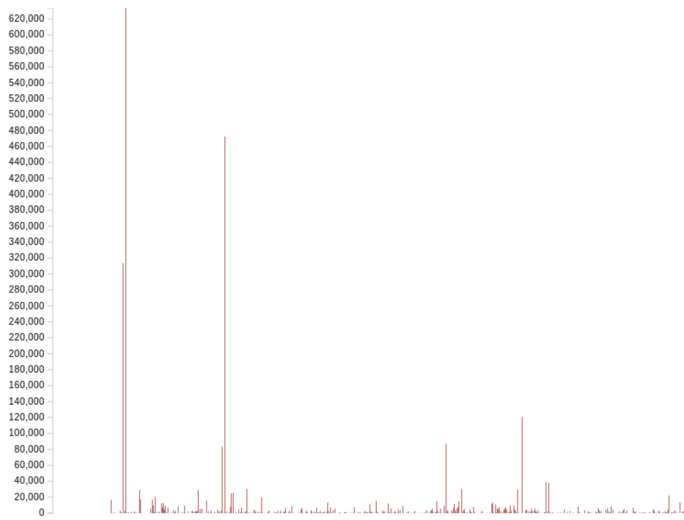
4.3 Reporters

An interesting aspect appears when looking at the values in the `reported by` column. More than $\frac{1}{3}$ of the cases has been reported by either of two journalists: Pavel Spirin (780 cases) and Oleksandr Nykonorov (379 cases). In third is the European think-tank European Values. Disregarding possible duplicates in the naming of reporting providers, only 33 entities have reported more than 10 cases out of 193 unique entity names. This is an important aspect to consider, besides the focus of the campaign, when considering skewness in the dataset. Oleksandr Nykonorov appears to be a Ukrainian journalist, while the European Values think-tank is an NGO based in the Czech Republic.

4.4 Considering Facebook likes

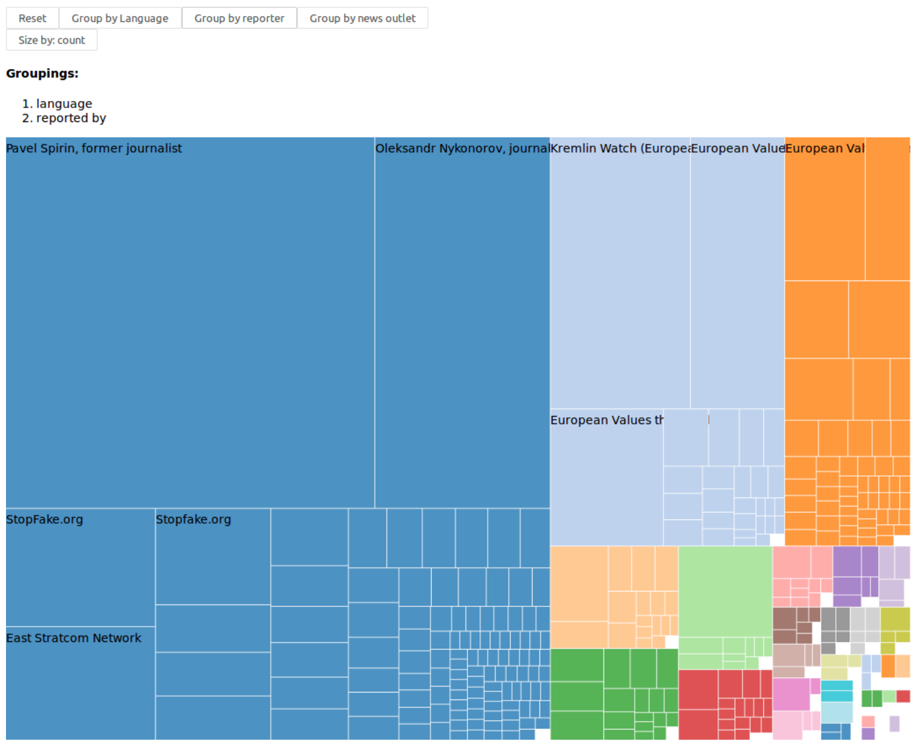
From the 3070 cases the sources averaged roughly 1200 likes on Facebook, although most likes were given to very few articles, as seen in fig. 10. Interestingly, approximately 27% of all the news sources were either never shared or not liked on Facebook at all.

Figure 10: Likes per article, created using rawgraphs [12]



For the purpose of allowing more visual inspection of the dataset, an online visualization was created using d3 and inspired from Mike Bostocks example seen in https://bl.ocks.org/mbostock/4063582. The visualization uses either of 3 predefined columns from the dataset: Language, reported by, and outlet to create a treemap visualization. While the treemap may not be optimal for all purposes, it goes a long way of showing the earlier mentioned proportionality within the dataset such as the number of articles reported by indivual entitites. In fig. 11 is seen a screenshot of this visualization, the screenshot shows the treemap of the number of articles reported by each person or organization within the different languages. The labels are hard to capture, since, for visual clarity, only entities having reported more than 50 articles have a label. On the website other labels will show upon mouse hovering. The colors as well as the squares represents the selected groupings in order. In the case of fig. 11 the color is determined by the language. The dark blue, which is most dominant, represents russian. The size of each square in fig. 11 indicates the number of articles each entity has reported. The website with the visualization is available as a proof-of-concept at http://k4lk.dk:3000, for which medium the visualization was optimized for.

Figure 11: Screenshot of the treemap visualization using grouped data by `language` and then `reported` by column



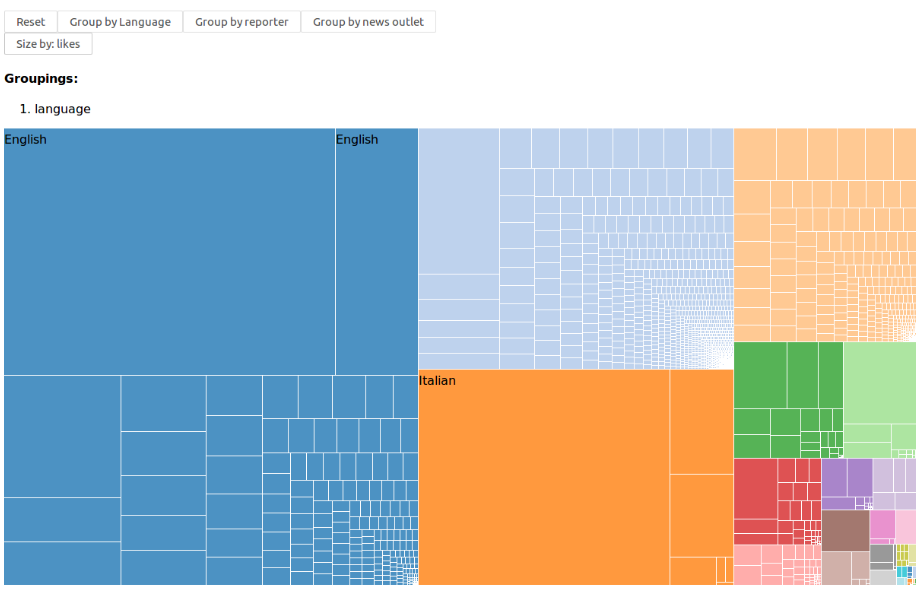
Another possible option for the user is to set the size of the squares not by number of cases, but after how many facebook likes each source url accumulated. For information that has not been shared on facebook, the number of likes defaults to zero.

In fig. 12 is shown two more screenshot illustrating how the view changes depending on what units the size of the squares is measured in. In fig. 12a the size is set by the number of articles for each language, while in fig. 12b the size is set to the number of likes for each language. Even though, the visualization is hard to convey to a report format, as it was intended for the web, it can be infered that the view changes drastically in relation to what units is used for sizes. As such, fig. 12a shows the dominating language is russian when measuring by number of articles, this is aligned with earlier stated properties of the dataset, see fig. 8. However, in fig. 12b, when looking at the number of Facebook likes in connection to each language, english emerges as largest of them all. Also, from fig. 12b it is seen that each language as distinguished by the colors, consists of a few remarkably larger boxes which is to say that a few articles succeeds in gaining a tremendous traction on social media, invariant of the language it is published in.

Figure 12: Cases grouped by language and sized either by number of cases, or accumulated likes of each case.

(a) Language by number of articles

(b) Language by amount of likes



5 Discussion

Throughout the project the dataset gradually expanded from the initial dataset acquired from euvsdisinfo.eu, the overall steps for the expansions can be boiled down to the following 3:

- Scraping content from HTML tags related to SEO
- Extracting named entitites using Stanford NLP
- Like count for each source URL via Facebook's OpenGraph API

This part of the report will focus on describing the interesting findings from the final dataset and reflect upon how it can be used.

5.1 Interpreting fake news as attacks

From this dataset there are may possibilities in terms of visualizations, for this reason it perhaps lends itself best to a dynamic visualization as the proof-of-concept website illustrated in figs. 11 and 12. This is further indicated by how the view changes drastically when weighting by likes compared to number of articles.

However, in terms of depicting who the perpetrators are, it is very difficult to extract automatically, let alone illustrate. In other areas, say IT security, for a typical visualization by an intrusion detection systems, the roles are clear and concise. A malicious agent scans or otherwise attempts to compromise the system the that the intrusion detection system is guarding. Thereby, the field of intrusion detection easily translate to so called attack maps.
Even with respect to "narrative battles" as seen in terms of the Ukranian crisis regarding Crimea, where these distinguished roles certainly exists, it is a non trivial problem to extract this information. This inspite of euvsdisinfo.eu providing as structured data as has been the case. The reason is that these sort of 'attacks' will take on many shapes and forms and to an extend will blend with regular media. Another factor, is the contextless extraction of the NER tagger. An example of this is seen in the filtered news articles as shown earlier, where an article is written in russian mentioning Putin, Poroshenko, and Adolf Hitler. Any reflection on this information would come to the conclusion that the inclusion of Hitler is most likely only related to the ukrainean president, given the language and origin of the story. However, a more automated process of interpretation may come to the false conclusion that both Putin and Poroshenko are victims of such fakenews.

5.2 Improving awareness

In any case, despite the difficulties, different views seems an adamant requirement to standing a chance in communicating what fakenews is and how it works. The dataset from euvsdisinfo.eu has obvious limitations regarding a full picture of fakenews, since it is by definition focused on false news surrounding a Kremlin agenda and because the number of cases is skewed regarding the people reporting them. The fact that a russian TV hostess shows up as the most mentioned name might mean that her TV show is a common source of misinformation. But with respect to the few people who are reporting most of the cases, it may also mean that there exists a disproportionate focus on that TV show in particular. Although, for this specific instance, it seems that Channel One is already identified as an important media for the russian governments "information warfare" [7]. Regardless, this example stresses the importance of having more views not only in terms of including different ways of inspecting the data, as in visualizations, but also to include more sources. Perhaps with respect to including other repositories, but it seems an equally good option, when the campaign already exists and have established ways for entitites to report cases, that more sources are involved with reporting the cases of fakenews to the campaign.

5.3 Limitations of the campaign

In light of the difficulties of visualizations the question arises of how to purposefully make use of the debunked articles in a way that promotes the objective of the campaign: to counter the false knowledge provided by fakenews. The campaign itself posts reviews regularly to their Facebook and Twitter accounts regarding their debunked news cases. This seems their main approach while maintaining a list of all the cases on their website. The same list that was ultimately scraped for usage in this project. However, the list of cases, while constituting a form of repository of debunked fakenews, does not provide any form of API or a download button. This seems counterintuitive to the decision of maintaining it in the first place. A download button seems a must while an API would be an optimal approach for allowing others to further extend the reach of the information that was, from an EU perspective, thought to be vital enough for a task force led campaign to be established.

On this note, another question that arose throughout this project concerns how it was even meant to reach the people who would need the debunked news to begin with. Not providing an easy access to their collected dataset other than the view they present themselves on their website, leaves it almost entirely to be distributed through their channels on socialmedia. However, this approach taps into the very same problematics that regular news is already experiencing. The body of information is too vast for anyone to gain a complete overview of. Seeing as how fakenews is already optimized to exploit all the key parameters to win the battle for attention within this context, this approach seems a lost cause.

A major challenge of relying on socialmedia to inform of cases of fakenews is that its distribution becomes controlled by the very same filter bubbles that the fakenews is already thriving in. That is, this approach may never manage to bridge between disjointed filter bubbles which likely is necessary to reach the audience who were susceptible to buying into the original false knowledge that the campaign afterwards debunked. Instead it is more imaginable that the people who finds the information via the campaigns socialmedia accounts were never targeted with the original content.

That these groups of people might be disjointed in terms of the information in its original form and the information after it has been debunked, propose a whole other issue. Considering how 27% of the cases were never shared on Facebook or was simply never liked if it was, then the campaign risks exposing the news to an audience who would have otherwise not known of its existence.

5.4 Going forward

This section will include discussion points on promising directions moving forward, besides the points already stated about the necessity for easier access to the dataset itself.
One of the approaches used in this project that proved very capable was the approach to using metatags for acquiring data from uniquely defined websites in a structured way. The approach is not a novel idea, and in fact it is by definition a method for acquiring structured data, one that is used every day by search engine crawlers. However, it is worth mentioning since it neatly utilizes the fact that fakenews is created with the common purpose of being spread. In an online context, being spread is inseparable from SEO. Because of this, the approach proved very reliable.
Furthermore, one specific aspect to this approach that would be interesting to further investigate, is whether missing tags related to the author of the article is a common phenomon among fakenews outlets. Also, to what extend the usage of author related tags deviates from that of mainstream online media outlets. This reflection came later as some of the sources were visitied manually, non of which specified an author. Unfortunately, author related tags was not included in the set of metatags as defined in fig. 4, and due to time constraints of the project it was not within the scope to rescrape the sources for further exploration.

The interest in spreading effectively is so ingrained in how online media works both, for the news outlets but also for the platforms that they get shared on. The reason is their common interest in generating revenue from advertisement. According to an interview with James Williams, a former Google employee of 8 years working on their advertisement products and tools and currently post-doctoral candidate at Oxford Internet Institute's Digital Ethics Lab [5], the threat does not reside in fakenews alone, but in the way business models based on advertisement dominates the distribution of information as a whole. A circumstance that as James Williams sees it, threatens to undermine democracy. Considering this angle, there is certainly a conflict of interest for a platform based on advertisement revenue to limit the amount of fakenews, that as stated earlier, is better at going viral than their authentic counterparts.

Furthermore, the approach of providing debunking information, implicitly assumes that free will determines the consumption of this information. However, as James Williams propose, even if the link the user clicks, is by their own choice, the chance of that click happening was never let up to the user. Putting this idea into perspective, at the other end of every individuals usage of socialmedia platforms is an entire research and development apparatus that has hyperspecialized every aspect of their platform towards engaging the user with the content they present. Engagement that is not meant to enable the individuals values and goals in life, but instead feeds into the shortsighted desires in all of us, systematically *stealing our attention* [5]. From the userinterface to the algorithms that determines what content is shown when. The motto of Facebooks newsfeed team comes to mind, and the perception that even if the choice was free, the game was already rigged.

To this end, it is interesting to notice that the website euvsdisinfo.eu, an EU led campaign, perhaps signals an entirely wrong focus when it comes to tackling the problem of fakenews. Instead, as James Williams suggests, it might be a matter of introducing a notion of *freedom of chance*, something he sees necessary to introduce in legislation. This perhaps is a circumstance that makes the current era different from historically similar occurences of fakenews. Traditionally, freedom of press and speech has been to ensure that the public had access to information to be able to base their opinions on equal empirical grounds. Today, the information is already there in abundance, however, the chance of what we see is not.

6 Conclusion

A better understanding is needed in order to be able to better deal with the phenomenon of fakenews, whether it is at an individual level, from a technological perspective or as a society. In this project a very small part of the entire body of fakenews was looked at, namely the cases available from euvsdisinfo.eu.

Repositories such as euvsdisinfo.eu can be a good source for further studying the patterns of fakenews. However, there still are noticeable limitations even to the dataset collected by a government funded campaign. As bias is inherent in all datasets, then so is the case as well for the dataset that was the basis of this project. Utilizing content from metatags and technologies such as named enti recognition can be a way of enhancing datasets over fakenews.

The most prominent visualization of this project was a dynamic webbased treemap visualization where different groupings of parameters could be configured. How the underlying landscape of fakenews appears, as indicated by this dataset, changes dramatically when trying to impose a sense of its quality rather than quantity. Facebook likes was used as measurement of the quality while the quantitity was simply based on the number of articles.

Having the possibility to view fakenews from different perspectives is important. To this extend more data is needed as well as more visualizations.

However one suggestion might be that fakenews is not ultimately defeated simply by providing countering information. It might just be that fundamental changes to the system that enables it, is needed.

References

[1] I can haz all your votes. *The Economist*, November 4-10:21–24, 2017.

[2] H. Allcott and M. Gentzkow. Social media and fake news in the 2016 election. Technical report, National Bureau of Economic Research, 2017.

[3] W. contributors. Yekaterina strizhenova — Wikipedia, the free encyclopedia, 2017. [Online; accessed 14-December-2017].

[4] R. Darnton. The true history of fake news. http://www.nybooks.com/daily/2017/02/13/the-true-history-of-fake-news/, 2017. [Online; accessed 14-December-2017].

[5] B. Gallagher. Modern media is a dos attack on your free will, 2017. [Online; accessed 15-December-2017].

[6] J. Gottfried and E. Shearer. News use across social media platforms 2016. *Pew Research Center*, 26, 2016.

[7] I. Khaldarova and M. Pantti. Fake news. *Journalism Practice*, 10(7):891–901, 2016.

[8] I. Khaldarova and M. Pantti. Fake news: The narrative battle over the ukrainian conflict. *Journalism Practice*, 10(7):891–901, 2016.

[9] E. J. Kirby. The city getting rich from fake news. http://www.bbc.com/news/magazine-38168281, 2016. [Online; accessed 14-December-2017].

[10] P. D. Lab. A field guide to fake news. http://fakenews.publicdatalab.org/, 2017. [Online; accessed 14-December-2017].

[11] C. D. Manning, M. Surdeanu, J. Bauer, J. Finkel, S. J. Bethard, and D. McClosky. The Stanford CoreNLP natural language processing toolkit. In *Association for Computational Linguistics (ACL) System Demonstrations*, pages 55–60, 2014.

[12] M. Mauri, T. Elli, G. Caviglia, G. Uboldi, and M. Azzi. Rawgraphs: A visualisation platform to create open outputs. In *Proceedings of the 12th Biannual Conference on Italian SIGCHI Chapter*, CHItaly '17, pages 28:1–28:5, New York, NY, USA, 2017. ACM.

[13] D. R. Spencer. *The yellow journalism: the press and America's emergence as a world power*. Northwestern University Press, 2007.