14. Describing an Incident

TL;DR Describing an Incident

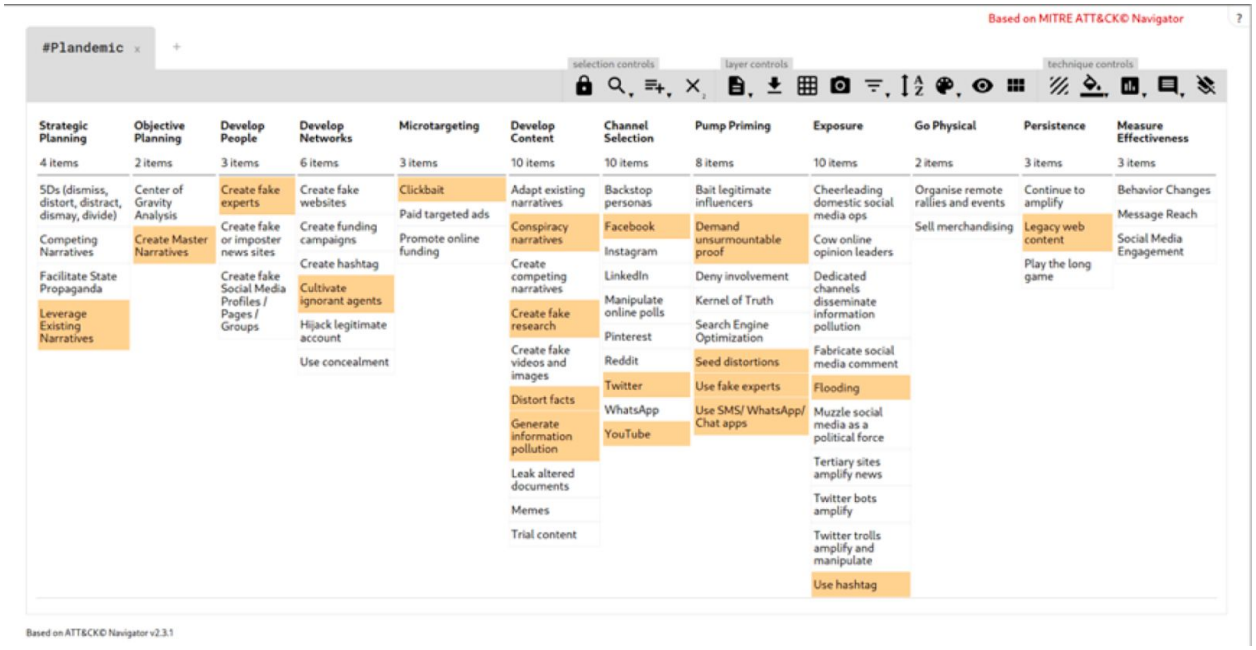
- Make a situation picture for the incident
- Share information in ways that recipients are used to
- Use visualisations to highlight patterns and connections

Situation Pictures

You have questions, artifacts, a community that you're sharing with. You still need to build a picture of what is happening - the situation around those artifacts, that most likely created them - and share that with other people.

Sensemaking includes looking at what we've collected, to work out what's happening and might happen across the whole incident. One way we do that is by analyzing the connections between incident objects. The CTI League uses MISP to help with that; other teams use tools like Maltego.

Using TTPs



TTP framework for Plandemic, 2020

We've talked about the AMITT Framework before. It's how we break an incident into techniques that we can analyze and counter.

We tick the AMITT boxes whilst we're gathering data \(e.g. during the observation part of an OODA loop\). During Orient, we look at this diagram to work out what's happening, how we might respond, and, if we catch an incident early, which downstream techniques might be used in that incident too.

The example here is Plandemic - a debunked conspiracy theory video which makes some false claims about the nature of COVID-19. We mapped it in AMITT to help us understand what capabilities the actor has and potentially how they're resourced.

Outputs to Other Groups

Data science, data analysis, starts and ends with human beings. We can do beautiful analysis, but if we don't make it accessible to the people who need to take action from it, then we haven't done our job.

There's no point building things without thinking about the end users, so let's talk about outputs. The ways we present the data we produce, and how we do that, including the forms/ formats some of the people we interact with are used to, what good visualisations in this space look like \(and how to create them\), and how to get those outputs to the right people.

Incident Reports

The most common written output is an incident report, containing a summary, narratives, techniques, artifacts and objects.

MISP events

We get a misp event that we can share with other groups either directly or by email, via their threat intelligence tools etc.

We added a few other things to MISP for this.

- Object types for common social media platforms, and code to load these into MISP using single-line commands in Slack, because speed is everything in a tactical response.
- New relationship types, to make the graphs that users can traverse in MISP richer.
- Taxonomies to cover things like types of threat actor.

Visualisations

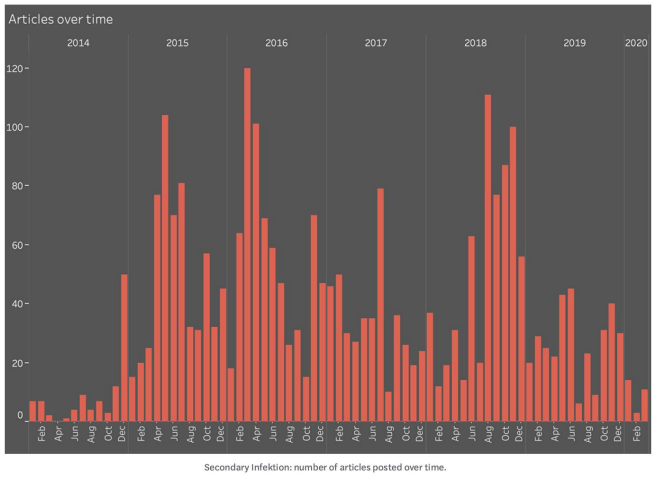
Eyeballing the data, looking at statistics, and examining machine learning outputs are good, but part of getting to know data, and explaining it to other people is being able to look at it visually. There's a lot of work on data visualisation \(read "Storytelling with Data" to see it done well\), so this section is looking at what disinformation people do with visuals.

Good places to look for what "that chart is" include

- All Charts - python visuals (most data scientists use Python)
- A Periodic Table of Visualization Methods - periodic table of visualisations

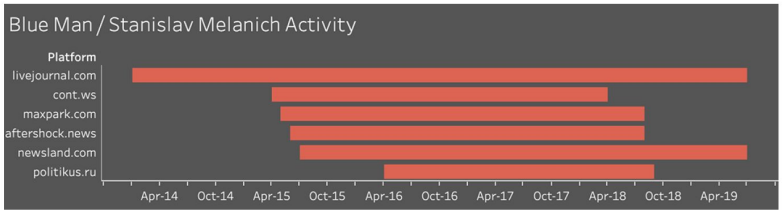
Understanding time series

Disinformation operations happen over time, so time-based plots can be useful tools. The humble bargraph, or its cousin the column plot, is really useful for this. Almost every visualisation tool has this as an option, e.g. https://matplotlib.org/3.2.1/api/_as_gen/matplotlib.pyplot.bar.html



(Sekondary Infektion report, 2020\)

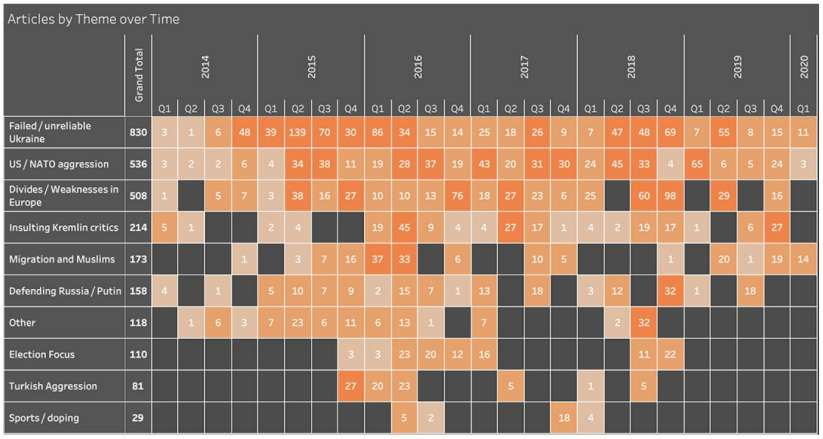
Bar graphs and line plots can be used for showing a range of entities over time.



The Blue Man's activity across different platforms, 2014-2019.

![\(Sekondary Infektion report, 2020\)]

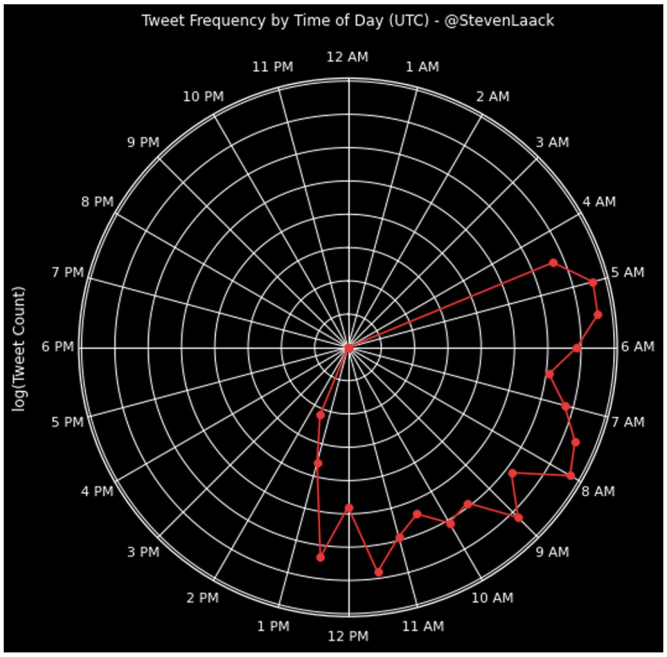
If the value range is too large to show easily \(e.g. there's a mix of very small and very large values that you can't easily plot on one axis\), heatmaps might be more appropriate. https://python-graph-gallery.com/91-customize-seaborn-heatmap/



Secondary Infektion: main themes over time

![\(Sekondary Infektion report, 2020\)]

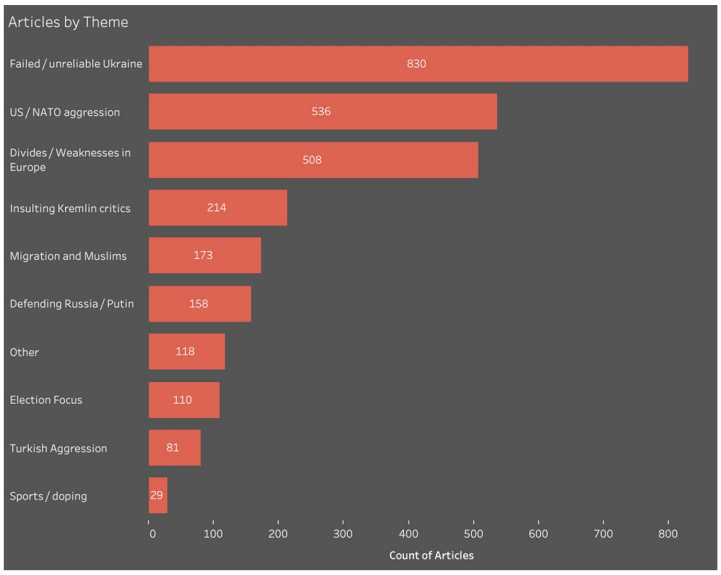
The use of spider plots for 24-hour data is good too, because they don't have a "start" or "end" time, making it easier to compare different diurnal patterns.



![\(Sekondary Infektion report, 2020\)]

Understanding relative sizes

Bargraphs can do this too: http://python-graph-gallery.com/barplot/

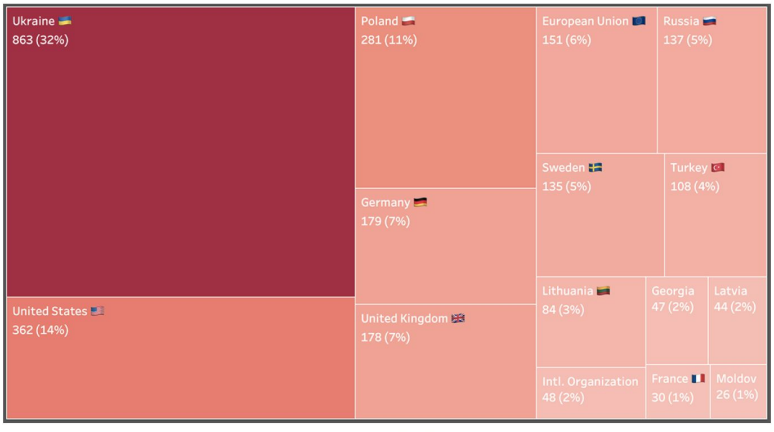


Breakdown of Secondary Infektion articles by theme and number.

![\(Sekondary Infektion report, 2020\)]

Treemaps show relative sizes as areas.

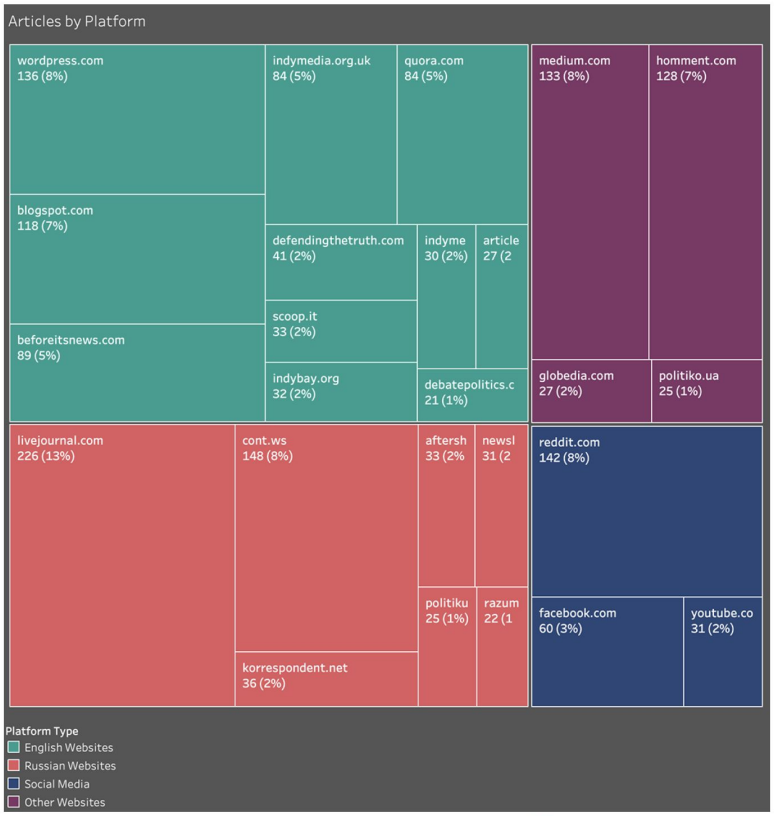
https://python-graph-gallery.com/200-basic-treemap-with-python/



Countries mentioned or targeted by Secondary Infektion, total number of stories.

Sekondary Infektion report, 2020

Colours are an extra, useful, dimension on most plots.

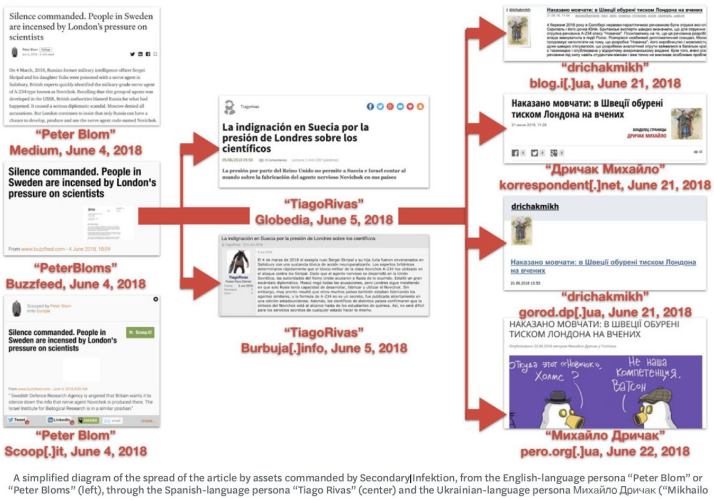


Use of platforms: where Secondary Infektion posted the most.[179]

Sekondary Infektion report, 2020

Understanding connections

Really simple graphics - think powerpoint - can help explain the connections between objects.

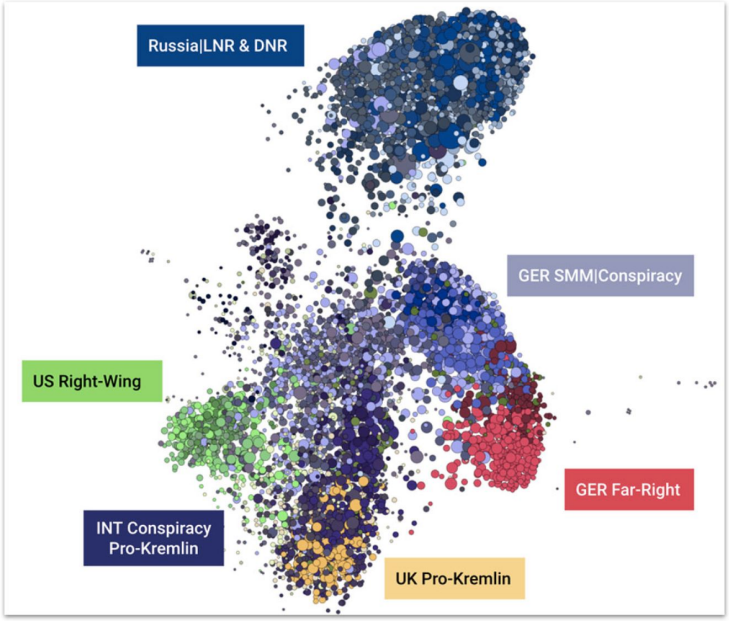


A simplified diagram of the spread of the article by assets commanded by SecondaryInfektion, from the English-language persona "Peter Blom" or "Peter Bloms" (left), through the Spanish-language persona "Tiago Rivas" (center) and the Ukrainian-language persona Михайло Дричак ("Mikhailo

Sekondary Infektion report, 2020: nice use of arrows

Simply gridding out pages or accounts with the same visuals or information can be really powerful if you're describing a network.

Graph diagrams show a large number of nodes and the connections between them - the "snurfball" images that we sometimes show to explain where the influencers are in an incident. Tools like Gephi produce these, with a little work, and liberal use of things like the Force Atlas 2 algorithm to make the network structure easier to see. Graphika produces "network maps" - one explanation is "The circles represent individual Twitter accounts. The volume of the circles represent influence by following, while the colours represent political ideologies.". This also looks like graph diagrams.



Graphika network map of the Secondary Infektion Twitter assets' followers and the followers of significant amplifiers, mapped April 2020.

Others

Some visualisations are hard to classify - is this a network diagram or the output from a dimension reduction algorithm? Dimension reduction is a type of machine learning algorithm that takes a set of objects that exist in many dimensions, and flattens it so it's easy to see - usually as a two-dimensional plot.

Specialist text analysis: look at things like Scattertext.