case study

Unmasking Disinformation Campaigns with Maltego

MALTEGO

Executive Summary

In July of 2020, the “Ghostwriter” disinformation campaign targeting countries like Poland and Lithuania came to light. A **report from the Cybersecurity firm Mandiant** pointed to a hacker group aligned with “Russian security interests” looking to discredit NATO in said countries since at least 2017.

According to Mandiant, the hacker group carried out its disinformation campaign against NATO by hacking news outlets and substituting verified news with fake ones, publishing fake news on websites accepting user generated content such as social media (UCG), and targeting websites linked to the Defense Ministries of the countries.

> NATO is not the only target of the Kremlin-backed propaganda machine. It has attacked everything from elections in third–countries to vaccination efforts during the Covid pandemic. It is also not the only actor attempting to destabilize Western nations and their alliances through the spread of disinformation.

Given the speed and reach with which information spreads these days, investigating and attributing disinformation campaigns without the right set of tools can prove to be an arduous endeavor. However, Maltego can greatly reduce the time needed to conduct investigations that would normally take an analyst several days if done manually.

While Maltego’s data mining capabilities help analysts dramatically speed up their data gathering process, its graphical link analysis combined with numerous data integrations allows them to pivot between different types of data and data sources. By combining all these puzzle pieces in one graph, analysts can find the groups behind specific disinformation campaigns.

Sourcing Outlets Spreading NATO Disinformation

The goal of the following workflow is to use Maltego to retrieve publications as well as the outlets and organizations behind the spread of disinformation seeking to compromise NATO's position in countries once belonging to the USSR or Warsaw Pact that are now part of NATO.

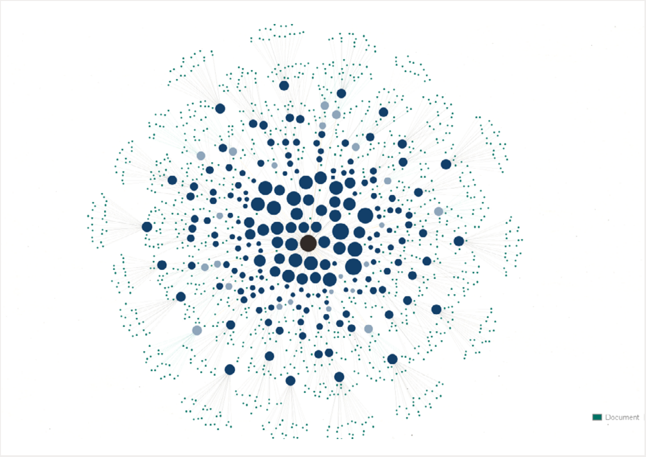
Hub Items that will be of use for this investigation are the Maltego Standard Transforms, Silobreaker, and Orbis – Bureau van Dijk Hub Items. Additionally, we will be using custom Views, which will help to visually display the information on the graph in particular ways facilitating its initial analysis.

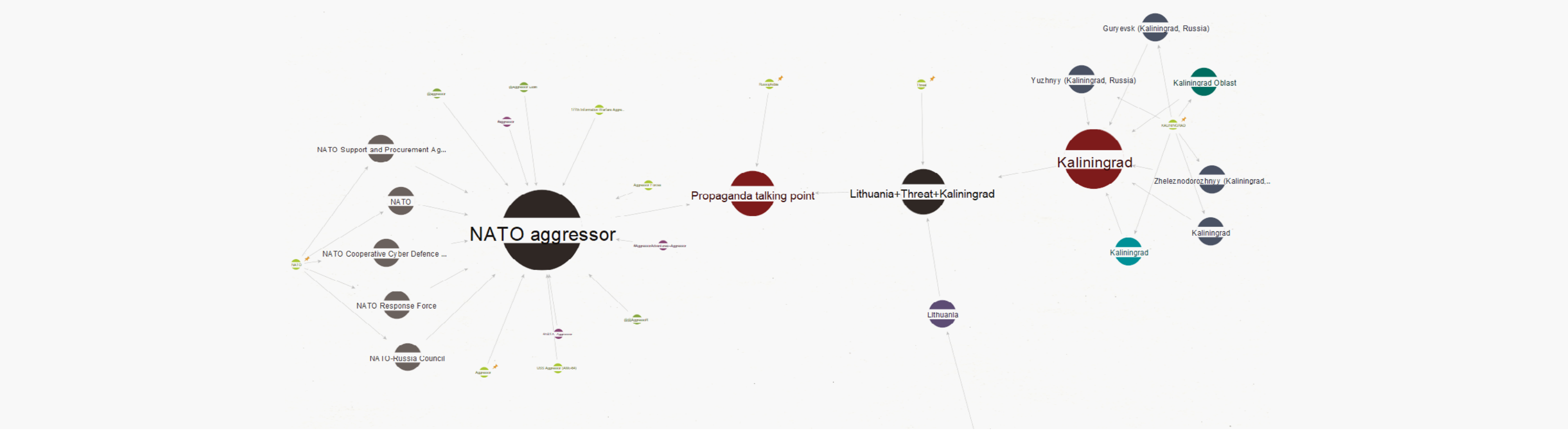
Stage One: Generate Interest Groups and Link Them to Outlets

1. We have six Phrase Entities, each of them is renamed to a specific keyword: "NATO", "aggressor", "Russophobia", "Kaliningrad", "Lithuania", and "threat". The list of keywords was developed by our analyst while researching this topic. We use the **[SB] Matching Entities** Transform to get a variety of Entity types matching the specific keywords. Results could range from organizations to outlets and publications, and from usernames to hashtags and locations.

2. Now, we use the **[SB] Group Entities (Or)** and the **[SB] Group Entities (And)** Transforms to form the following Group Entities from the results we gathered on the previous step: "Kaliningrad", "NATO aggressor", "Lithuania + threat + Kaliningrad", and "propaganda talking point". As can be seen below, while each of the groups (four bigger-sized balls) is constituted of specific Entities, all groups are also linked to one another. This will ensure our results are as coherent with our investigation as possible.

3. Now, we will attempt to link the "propaganda talking point" Group Entity to online publications by using first, the **[SB] Related Publications** Transform, and then, the **[SB] Document Evidence for Link** Transform on the resulting Publication Entities. Visualizing Entities on the Graph by number of Outgoing Links in an Or-

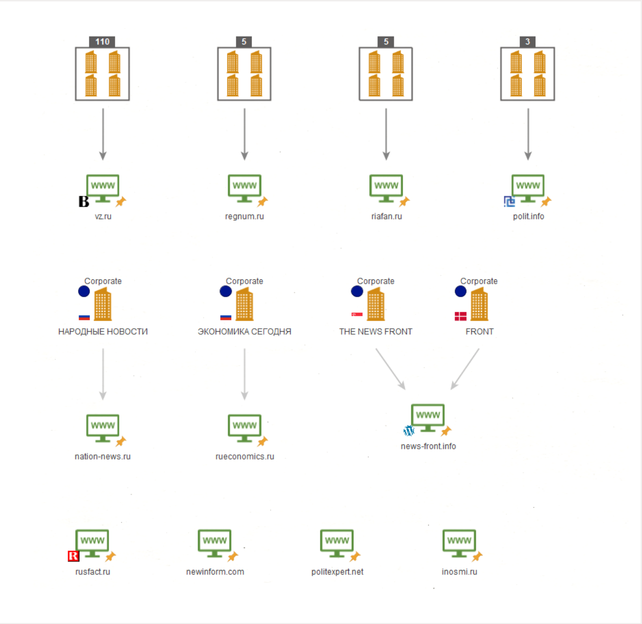




ganic layout, we can see that Entities of bigger size represent the outlets with the highest number of posts (i.e., documents) related to our topic of interest. We will use these results to continue our investigation.

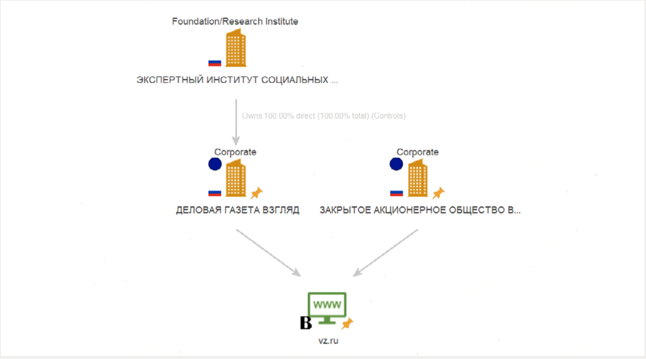
Stage Two: Looking For The Organizations Behind The Outlets

4. We go back to the eleven Phrase Entities to look for theactual organizations that own the outlets we are investigating. To do so, we will use the Orbis – Bureau van Dijk Transforms. To begin with, we convert the Phrase Entities into Website Entities to run the **[Orbis] Find companies by website** Transform. The results provided by this query need to be examined closer, as they highly depend on the level of existing oversight in the country where the companies are registered. From the sheer number of results that are retrieved for the website [vz. ru] (110 companies registering the same website), and after examining the Properties of the Company Entities such as the name (eleven companies named “ВЗГЛЯД” or “Vision”) general activity (all eleven “ВЗГЛЯД” companies providing a range of different services or products), we can infer that some of the companies are fake if not fronts for other types of operations.



5. Now, we take – as an example – what we found to be [vz.ru] publishing company, ДЕЛОВАЯ ГАЗЕТА ВЗГЛЯД (Delovaya Gazeta Vzglyad) or Business Newspaper View, to keep climbing up the hierarchy ladder of the organization behind this outlet. To do so, we run the **[Orbis] Get parent companies & owners** Transform on the Company Entity. We find an NGO named ЭКСПЕРТНЫЙ ИНСТИТУТ СОЦИАЛЬНЫХ ИССЛЕДОВАНИЙ (Ekspertnyy Institut Sotsial’nykh Issledovaniy) or Expert Institute for Social Research amongst the results.

6. After a closer inspection, we find an article on the website [gazeta.ru] deeming this “analytical center” or quasi think tank to be a creation at the behest of the Russian presidential administration. It was also found out that the organization is tied to the Russian Federal Agency for Communication. We can therefore determine the Expert Institute for Social Research to be pro-government or even controlled by the government. Further analysis could be done on the organizations we have on the Graph with regards to the people behind them, and their possible ties to the Russian Government.


Foundation/Research Institute
ЭКСПЕРТНЫЙ ИНСТИТУТ СОЦИАЛЬНЫХ ...
Owns 100.00% direct (100.00% total) (Controls)
Corporate
ДЕЛОВАЯ ГАЗЕТА ВЗГЛЯД
Corporate
ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО В...
vz.ru

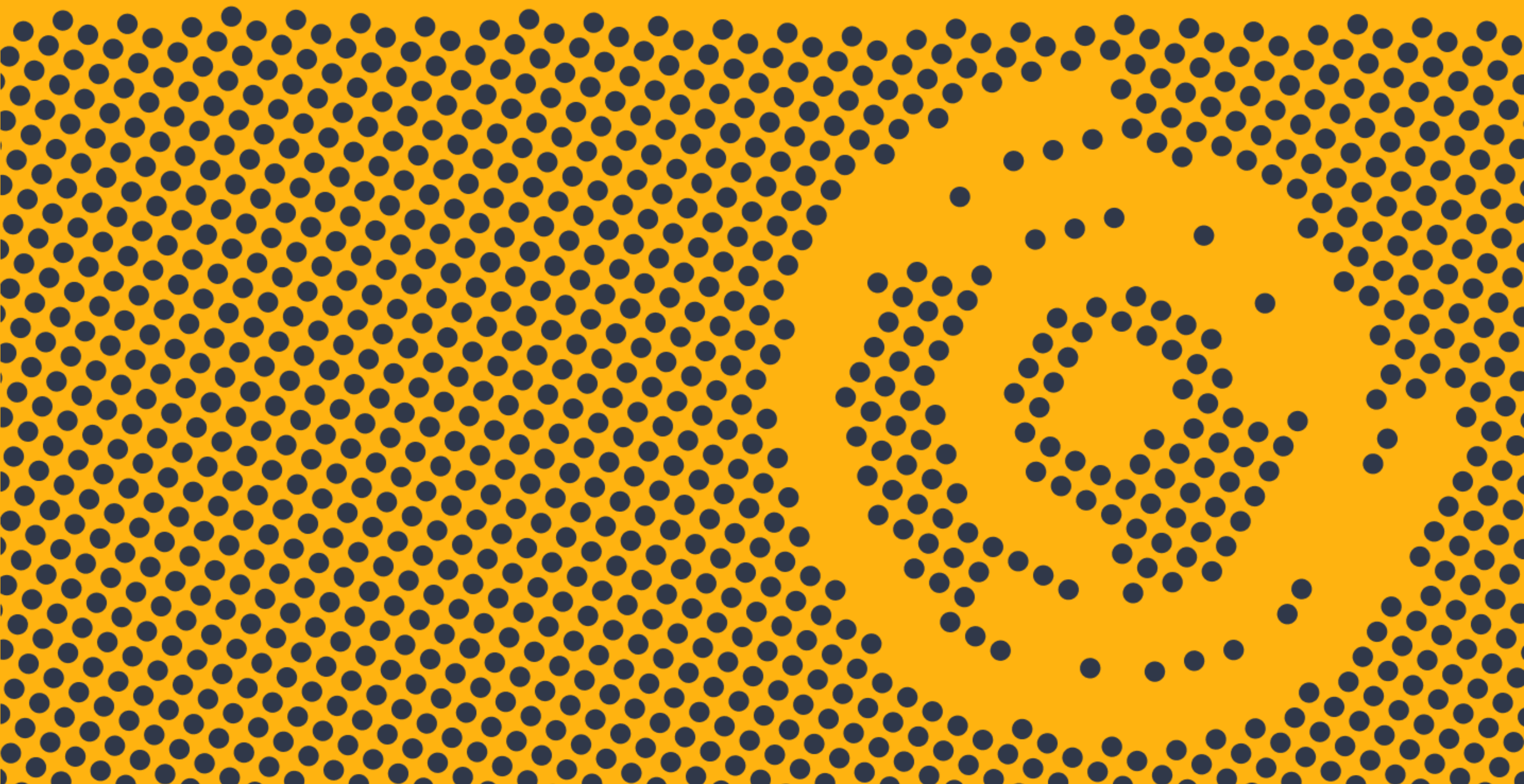
Stage Three: Conclusion

This investigation shows how it is possible with Maltego to detect publications spreading disinformation on specific topics. It is also possible to identify the outlets behind said publications and to analyze the corporate structures behind them, ultimately tying some of these organizations to the Russian propaganda machine.

For more information, please visit
maltego.com

Maltego is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable. With Maltego, you can easily mine data from dispersed sources, automatically merge matching information in one graph, and visually map it to explore your data landscape. Maltego offers the ability to easily connect data and functionalities from diverse sources using Transforms. Via the Transform Hub, you can connect data from over 30 data partners, a variety of public sources (OSINT) as well as your own data. Our different Desktop Client versions, data sources, and server solutions enable you to tailor Maltego to your specific needs in terms of data access, functionalities, and security requirements.

MINE • MERGE • MAP / DATA



case study

Email: contact@maltego.com

Phone: +49-89-24418490

MALTEGO