View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Illinois Digital Environment for Access to Learning and Scholarship Repository

Exploring Russian Information Troops Using Geography and Google Trends

Volodymyr Lysenko[1] and Catherine F. Brooks[1]

[1] University of Arizona, Tucson AZ 85721, USA
lncs@springer.com

Abstract. With this project, we focus on Russian information-based global influences or "hacks" in order to generate new ideas about disruptive digital activities that can emanate from any country and bring effects that are potentially global in their impact. Russia as both a site and political actor exemplifies a case of global, digital, and democratic disruption, and this research points to potential locations housing Russian information troops. The findings provide a way to see patterns in media-related tactics contributing overall to the existing evidence of 'hybrid' or information warfare identified in recent literature.

Keywords: Hybrid War, Information War, Cyber-Troops.

1 Introduction

Hacked data and disinformation are all powerful tools used alongside cyber sabotage and military force in different parts of the Western world. In recent years, Russia has taken central stage in the scholarly analyses of new media use and information strategies utilized for the purposes of political influence (e.g., Pasitselska, 2017). This research presented here is drawn from the authors' broader agenda exploring Russia's information war tactics more generally. To examine Russia's information hacks and related strategies, we focus on digital trends and Internet use. In doing so, we can illuminate the Russia case while also contributing to conversations about how scholars can explore digital activity to uncover political influence around the world.

2 Method

This inductive study follows an interpretive case study design (Walsham, 1995; Yin, 2002), and focuses on Russia as a case of a nation engaging information warfare tactics. This project aligns with methodological guidelines on the ways case study work can be used "to explore in depth a particular phenomenon in a contemporary context" Farquhar, 2012, p.9). The authors focused on "developing an in-depth description and analysis of a case ... " (Creswell, 2007, p. 78). Data for this project are comprised of publicly available documents and data pulled from Google Trends. Analytically, we considered the data iteratively, looking for patterns, locations, and activity in Russia. We also looked interpretively at the content of online posts and published work com-

ing out of Russia to draw patterns and to find connections across them. From this case we can learn processes by which one nation can influence many others with Internet-based tactics (e.g., generating comments, sharing propaganda on social media, hacking secured digital infrastructures).

3 Findings

Conscription still exists in Russia (a mandatory 12-months draft), and beginning 2013 its military started encouraging the civil universities' best graduates to serve it in "research companies". One such company (the Sixth research company - "military cyber-defenders", 60 people) is attached to the Shtemenko Military Institute located in the city of Krasnodar and conducting applied research related to information security. After their 12-month mandatory term, the research companies' conscripts are strongly encouraged to continue military service as officers on contract.

In August 2015 one LiveJournal's blogger ("otakvot") posted research describing an interesting "anomaly" revealed by the Google Trends service. He found several Russian small towns with an abnormally high interest in the contentious political matters. Specifically, he found that, according to the Google Trends, such small Russian towns as Olgino (4,119 people), Perekatnyy (244 people), Zelyony Gorod (2,679 people) and the slightly larger Yablonovsky (30,518 people) have higher or comparable interest in searching Google on such contentious political terms as "майдан" (symbol of Ukrainian pro-democracy revolution), "санкции" (sanctions), "референдум" (referendum), "НАТО" (NATO) (after 2013), "Порошенко" (Poroshenko), as big Russian cities where millions of people live. At the same time, search on more common and less politically-charged Russian terms in the Google Trends predictably surfaces only the biggest Russian cities. We conducted our own search in the Google Trends on the term "майдан" and can confirm "otakvot"'s findings (Fig. 1):

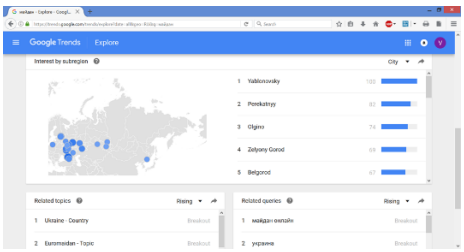

Fig. 1. Screenshot of our Google Trends search on the term "майдан".

For this project we investigated the particularly-high political interest in those four small Russian towns. In his blog research "otakvot" notes that Olgino hosts the infamous Russian troll factory, where hundreds of paid trolls – trolls that can be conceived as cybertroops – work around the clock. Our work aims to illuminate what may be happening in the other three small towns – Yablonovsky, Perekatnyy and

Zelyony Gorod. Finding the Shtemenko Institute on the map proved an informative early step, its address: ul. Krasina, 4, Krasnodar, Krasnodarskiy kray, Russia, 350035. With Google Maps we provide means for visualizing this location next in Fig. 2:

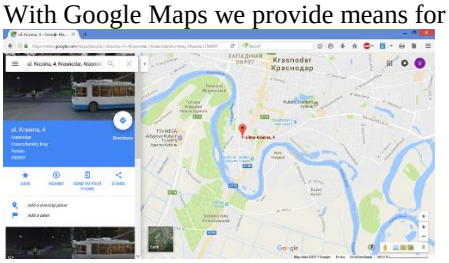

Fig. 2. Screenshot of the Shtemenko Military Institute' location on the Google Maps.

On Fig. 2 we see that both Yablonovsky and Perekatnyy ("Perekatni") are located within approximately a mile from the Shtemenko Institute. Google can, most likely, attribute the searches conducted at the Institute to those two locations. Moreover, if we look at the last "abnormal" town, Zelyony Gorod on Google Maps, we find it in close proximity to another Institute similar to Shtemenko, but this time belonging to the FSB: specifically, the Nizhniy Novgorod FSB Institute is likely causing the anomaly in politically-focused digital traffic. With Google Maps we provide means for visualizing this FSB Institute location next in Fig. 3:

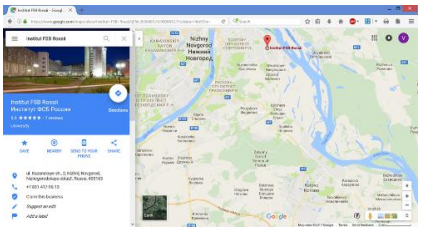

Fig. 3. Screenshot of the Nizhniy Novgorod FSB Institute's location on the Google Maps.

We thus assert that Russian cybertroops are not only the paid civilians located in Olgino, but are also the full time military and FSB personnel scattered around these rural towns in the region. Of course, Russian information troops are also likely located near or inside those bigger Russian cities we mentioned above, so their Internet traffic is "hidden" by the population of those bigger cities. Beyond providing an understanding of the geographic region and its Internet traffic, our findings suggest the existence of embedded groups engaged in political influence and disruptions to political processes around the globe.

4 Conclusion

With this research, we focus on Russia's Internet traffic and how that traffic is situated regionally and geographically. We also contribute to an ongoing and scholarly conversation about contemporary hacking for political gain. With Russia as a case, we can explore tactics and choices that can inform the ways readers might view any country, any leaders, or any media-influence happening globally in today's digital culture. Though we recognize attitude change has long been an effective military tactic, and while we know hacking and spying are not new strategies, we illuminate the nature of a current case of militarized information attacks, one that rests solely on digital/new media influences. Instead of leaflets, and rather than physical attacks with boots on the ground, that is, we raise the possibility that hacks into energy grids, intrusions into confidential email boxes, and various social media tactics (e.g., commenting, incisive propaganda sharing) are the new coordinated warfare strategy in this information age – and with this particular project, we suggest where these strategies are being deployed.

References

1. Creswell, J. W.: Qualitative enquiry and research design: Choosing among five approaches, Sage Publications, Thousand Oaks (2007).
2. Farquhar, J. D.: Case study research for business, Sage Publications, Thousand Oaks (2012).
3. Pasitselska, O.: Ukrainian crisis through the lens of Russian media: Construction of ideological discourse. Discourse and Communication (online first), (2107).
4. Walsham, G.: Interpretive case studies in IS research: nature and method. European Journal of Information Systems (4), 74-81 (1995).
5. Yin, R. K.: Case study research, design and methods, 4th ed. Sage Publications, Thousand Oaks (2009).