



PropOrNot: Is It Propaganda or Not?

*Your Friendly Neighborhood Propaganda Identification Service,
Since 2016!*

Web: www.propornot.com

Twitter: www.twitter.com/propornot

Reddit: www.reddit.com/r/propornot/

Email: propornot@gmail.com

Black Friday Report: On Russian Propaganda Network Mapping

By The PropOrNot Team
November 26th, 2016

Thanks to the Generous Sponsorship of:
Nobody
(Funding? Hah!)

Executive Summary: Russia's attempts to influence the U.S. election via hacking and selectively leaking sensitive U.S. government and political data were not conducted in isolation. They were accompanied by large-scale, long-term efforts to build online "fake news" propaganda outlets with significant audiences in the U.S. PropOrNot has so far identified over 200 distinct websites, YouTube channels, and Facebook groups which qualify as Russian propaganda outlets according to our criteria and target audiences in the United States. Drawing on existing research and using a combination of automated and manual review techniques, we estimate the regular U.S. audiences of these outlets to number in the tens of millions. We are currently gathering data to measure that more precisely, but are confident that it includes at least 15 million Americans.

Table of Contents

Introduction and Context	2
Background on PropOrNot	4
Characteristics of Identified Sites	5
Methodology	7
A Prior-Research Case Study: ZeroHedge.com	10
Spidering, Correlating, Reviewing, Spidering	16
Following a Specific Story: The Tale of the Painted Jets	19
Following a Specific Story: The Tale Hillary Clinton’s “Parkinson’s”	26
Following a Specific Story: Ourselves!	27
Using Google Trends to Measure Larger-Scale Effects	28
Preliminary Conclusions	30
Next Steps	31

Introduction and Context

Throughout the election season of 2016, an increasing number of reporters and journalists have done remarkable work investigating the origins and operations of “fake news” outlets on the internet. Some notable examples include:

[How Facebook powers money machines for obscure political 'news' sites](#)

By Dan Tynan, Aug 24 2016, The Guardian

[Online Scam Artists Are Using Hoaxes About Terrorist Attacks To Make Money](#)

By Craig Silverman, Aug 19 2016, BuzzFeed News

[Facebook Made This Sketchy Website’s Fake Story A Top Trending Topic](#)

Craig Silverman, Aug 29 2016, BuzzFeed News

[We Tracked Down A Fake-News Creator In The Suburbs. Here's What We Learned](#)

Larua Sydell, Nov 23 2016, NPR

[Seattle’s own ‘click-bait’ news site serves up red meat for liberals](#)

Danny Westneat, Nov 25, 2016, Seattle Times

[How Fake News Goes Viral: A Case Study](#)

Sapna Maheshwari, November 20 2016, New York Times

Buzzfeed News in particular has done pioneering analytical work on this, and [their stories on the “fake news” issue](#) are an excellent resource. Public discussion has now correctly recognized that “fake news” is a serious problem with real-world consequences, and a number of innovative actors have started to

discuss, research, and develop potential solutions. However, the public discussion of all this has, until very recently, generally assumed that the “fake news” problem has been mostly driven by “clickbait”-style commercial motivations:

[Renegade Facebook Employees Form Task Force To Battle Fake News](#)

Sheera Frenkel, Nov 14 2016, BuzzFeed News

[Facebook's Fight Against Fake News Was Undercut by Fear of Conservative Backlash](#)

Michael Nunez, Nov 14 2016, Gizmodo

[Here's a Chrome Extension That Will Flag Fake-News Sites for You](#)

By Brian Feldman, Nov 15, 2016, New York Magazine

[We Have a Bad News Problem, Not a Fake News Problem](#)

By David Mikkelson, Nov 17 2016, Snopes

[How to Spot Fake News](#)

By Lori Robertson and Eugene Kiely, Nov 18 2016, FactCheck.org

This evolving thread of stories analyzing “fake news” has been simultaneously accompanied by a very different but parallel thread of stories and public discussion about Russian cyberespionage, propaganda, and “active measures” targeted at the West. Reporting on this initially focused on Russian-backed comment-troll farms, but quickly expanded beyond that:

[Documents Show How Russia's Troll Army Hit America](#)

By Max Seddon, Jun 2 2014, Buzzfeed News

[The Agency: From a nondescript office building in St. Petersburg, Russia, an army of well-paid “trolls” has tried to wreak havoc all around the Internet — and in real-life American communities](#)

By Adrian Chen, Jun 2 2015, New York Times

[Salutin' Putin: Inside a Russian troll house](#)

Shaun Walker in St Petersburg, The Guardian, 2 April 2015

While the public discourse correctly recognized that “fake news” was becoming a serious problem, especially in light of the election, very few journalists and researchers sought to systematically connect the dots between fake news and Russian cyberespionage, propaganda, and “active measures” generally. However, as the election season ramped up an increasing number of intrepid reporters and researchers started investigating this connection, which had been discussed extensively in the specialist press for years. Much of this research inspired our efforts at PropOrNot. For example:

[Unmasking the Men Behind Zero Hedge, Wall Street's Renegade Blog](#)

By Tracy Alloway and Luke Kawa, Apr 29, 2016, Bloomberg

[Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign](#)

Lawrence Alexander, Apr 2 2015, Global Voices

[When Online Kremlin Propaganda Leaves the Web, It Looks Like This](#)

Lawrence Alexander, Sep 29 2015, StopFake

[Social Media as a Tool of Hybrid Warfare,](#)

Sanda Svetoka, Jul 7 2016, NATO StratCom

[The Fringes of Disinfo: A Network Based on Referrers](#)

By Andrew Aaron Weisburd, Feb 7 2016, in активные мероприятия

[Putin's Army Of Internet Trolls Is Influencing The Hillary Clinton Email Scandal](#)

By Paul Roderick Gregory, 5 June 2016, Forbes

[Donald Trump and Vladimir Putin: Russia's information war meets the US election](#)

By Chris Zappone, 15 June 2016, Sydney Morning Herald

[The Kremlin's Candidate: In the 2016 election, Putin's propaganda network is picking sides](#)

Michael Crowley, May/June 2016, Politico

[Prof. Chodakiewicz discusses Russian military and influence operations at US Army Europe Senior Leaders Forum](#)

Marek Jan Chodakiewicz, Jan 27 2015, Institute of World Politics,

Until very recently no public research connected the dots as extensively as this article:

[Trolling for Trump: How Russia Is Trying to Destroy Our Democracy](#)

By Andrew Weisburd, Clint Watts and JM Berger, Nov 6 2016, War on the Rocks

These previously separate threads of public discussion about “fake news” and about Russian propaganda are now, finally, being connected. In our view, this is long overdue. We at PropOrNot are proud to be contributing to that discussion.

Background on PropOrNot

We are an independent team of concerned American citizens with a wide range of backgrounds and expertise, including professional experience in computer science, statistics, public policy, and national security affairs. We are currently volunteering our time and skills to identify propaganda - particularly Russian propaganda - targeting a U.S. audience. We collect public-record information connecting propaganda outlets to each other and their coordinators abroad, analyze what we find, act as a central repository and point of reference for related information, and organize efforts to oppose it.

Some of our members have been aware of Russian influence operations in a professional context for quite some time, but others have become increasingly aware of existing research on the subject in light of recent events in Ukraine, Western Europe, and the Middle East. We formed PropOrNot as an

effort to prevent propaganda from distorting U.S. political and policy discussions. We hope to strengthen our cultural immune systems against hostile influence and improve public discourse generally.

We are completely independent, because we not funded by anyone, and we have no formal institutional affiliations. We are nonpartisan, in that our team includes all major political persuasions except the pro-Russian kind. We are anonymous for now, because we are civilian Davids taking on a state-based adversary Goliath, and we take things like [the international Russian intimidation of journalists](#), [“Pizzagate”-style mob harassment](#), and [the assassination of Jo Cox](#) very seriously, but we can in some cases provide background information about ourselves on a confidential basis to professional journalists. We do not publicly describe all of our sources and methods, although again, we can in some cases provide much more detail to journalists and other researchers in order to contextualize their reporting.

We are American, although our team includes Ukrainian-American, Iraqi-American, and quite a few other varieties of American members. We are united in our overall objectives: to identify, help counter, and eventually deter Russian propaganda. Any time an outlet consistently echoes, repeats, or refers its audience to Russian propaganda, we’re going to analyze it and call it out.

Characteristics of Identified Sites

We at PropOrNot do not reach our conclusions lightly. We have arrived at them after systematically employing a combination of manual and automated analysis, building on the work of other researchers and journalists, in order to map out a related collection of websites, social media, video, and other outlets, which:

1. Include official state-owned and semi-official Russian propaganda outlets, such as [Russia Today](#), [Sputnik News](#), [Russia Insider](#), etc.;
2. Consistently cite official state-owned and semi-official Russian propaganda outlets, including the Russian defense ministry and other official spokespeople;
3. Consistently reuse text directly from official state-owned and semi-official Russian propaganda outlets and government spokespeople, often without attribution;
4. Have a history of generally echoing the Russian propaganda "line", by using themes, arguments, talking points, images, and other content similar to those used by official state-owned and semi-official Russian propaganda outlets;
5. Have a history of echoing the Russian propaganda "line" in ways unrelated to the purported focus of their branding, and in sequence with (at the same time as, or shortly after) official state-owned and semi-official Russian propaganda outlets;
6. Qualify as propaganda under a rigorous definition: *“A systematic form of purposeful persuasion that attempts to influence the emotions, attitudes, opinions, and actions of specific target audiences for political, ideological, and religious purposes, through the controlled transmission of deceptive, selectively-omitting, and one-sided messages (which may or may not be factual) via mass and direct media channels”*;
7. Have in many cases already been called out by other fact-checkers, researchers, journalists, or debunkers;

8. Share technical “tells” suitable for automated analysis, such as Google Analytics IDs, Amazon affiliate codes, WHOIS data, hosting data, ad-network utilization, SEO techniques, referral patterns, in some cases strongly suggesting direct Russian involvement;
9. Refer their audiences to each other, via hyperlinks and other means, at disproportionately high rates;
10. Are consistently visited by the same audiences, both directly and via search, demonstrating that those intra-network referrals build “brand loyalty” in their audiences over time;
11. Are consistently visited by their audiences after searches for terms which congrue with the Russian propaganda “line”, and are unrelated to the purported focus of their branding;
12. Are categorized as "similar sites" by automated services in spite of their purportedly distinct focuses;
13. Have content characterized by automated services in ways that are consistently very different from their purported subjects, but align with the Russian propaganda “line”;
14. Have content aligning with the [“Eurasianist” philosophy of Alexander Dugin](#);
15. Include specialized sites targeted at a wide range of seemingly unrelated audiences, including U.S. military veterans, Wall St. finance industry professionals, environmentalists, peace activists, racists, conspiracy theorists, and political junkies;
16. Appear to be effectively influencing public opinion in significant and very problematic ways, by promoting:
 - a. Conspiracy theories about and protests against U.S. military exercises (“Jade Helm”),
 - b. Isolationism and “anti-interventionism” for the US, but not for Russia,
 - c. Support for policies like Brexit, and the breakup of the EU and Eurozone,
 - d. Opposition to Ukrainian resistance to Russia and Syrian resistance to Assad,
 - e. Support for the anti-vax, anti-Zika spraying, anti-GMO, 9/11-”truther”, gold-standard, and other related movements;
17. Have extremely large audiences in the U.S., such that tens of millions of people appear to use them as primary “news” sources, supplanting actual journalism;
18. Appear to be part of a larger “active measures”-style Russian influence operation, which also includes hacking and selectively leaking sensitive U.S. government and political data, along with more-traditional espionage and military activity, intended to:
 - a. Confuse public opinion, encourage paranoia and passivity, and distract American audiences away from relying on actually-accurate journalism,
 - b. Blunt opposition to and strengthen popular support for Russian strategic priorities.

Please bear in mind that these characteristics of propaganda outlets are motivation-agnostic. They are independent of questions about whether the sites we’ve identified are being knowingly directed and paid by Russian intelligence officers, or whether they even knew they were echoing Russian propaganda at any particular point--if they display these characteristics, they are at the very least acting as ["useful idiots"](#) of the Russian intelligence services, and are worthy of further scrutiny.

We have been following recent reporting about for-profit political, commercial, and other kinds of clickbait, hoax, and fake-news sites, and while our automated tools and our manual techniques have occasionally identified sites as Russian propaganda which others have recently identified as commercially or otherwise motivated, if they meet our criteria, we see no reason not to flag them. Our tools are evolving, but because we focus on behavior, not motivation, we are less interested in *why* any

particular outlet echoes or spreads Russian propaganda, than on *whether* they do. Whether for money or out of ideological affinity, the end results are the same.

Methodology

We use a combination of manual and automated analysis, including analysis of content, timing, technical indicators, and other reporting, in order to initially identify (“red-flag”) and then confirm an outlet as echoing, repeating, and referring its audience to Russian propaganda.

Our volunteers have developed multiple suites of software tools, leveraging publicly available data and commercial analytics services (like [Quantcast](#), [Alexa](#), [SimilarWeb](#), [uStat](#), [SiteLinks](#), [My Web of Trust](#), [AnalyzeID](#), [SocialBlade](#), and [Buzzsumo](#), among others), in order to discover and perform automated analysis of Russian propaganda outlets, but everything we do is in principle replicable using manual searching and data entry.

We started our automated analysis from the domains and social-media accounts of Russian official and semi-official media outlets, including:

[rt.com](#)

[sputniknews.com](#)

[therussophile.com](#)

[russia-insider.com](#)

[strategic-culture.org](#)

[katehon.org](#)

[theduran.com](#)

[www.fort-russ.com](#)

[thesaker.is](#)

[pravda.ru](#)

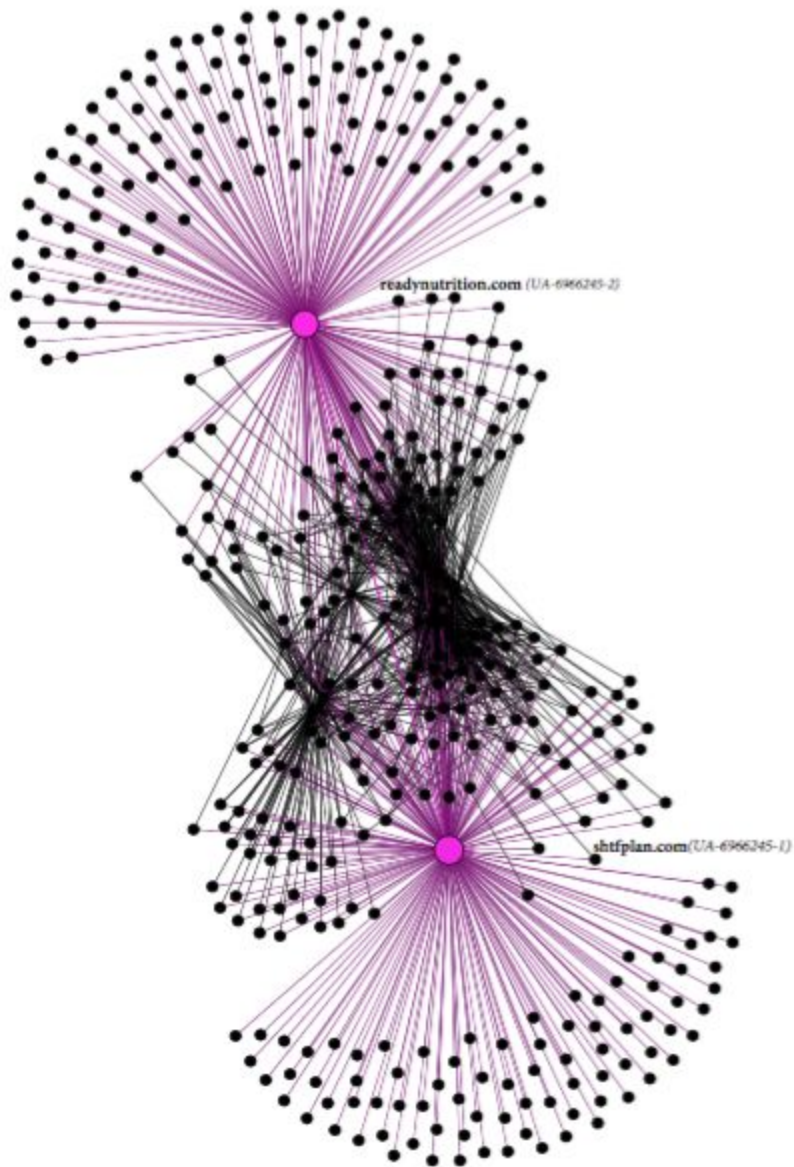
[tass.ru](#)

We also drew on other public investigative journalistic reporting which highlights outlets and social media accounts as particularly and unusually pro-Russian, and, after doing our own research sometimes use them as starting points as well. This analysis is used as an example later in this report:

[Unmasking the Men Behind Zero Hedge. Wall Street's Renegade Blog](#)

By Tracy Alloway and Luke Kawa, Apr 29, 2016, Bloomberg

We then use our custom tools to “spider” out from those identified sites and accounts, discovering new, connected propaganda sites and social media accounts by examining their technical characteristics, including Google Analytics IDs, Amazon affiliate codes, WHOIS data, hosting data, ad-network utilization, SEO techniques, social media activity, and word-frequency metrics. We can then graph the results in various ways that highlight degrees of similarity, like this [ego network diagram](#):



Ego network diagram illustrating link distance distance metric and density overlap between sites sharing technical identifiers (in this case, a Google Analytics ID)

We use previous reporting and automated analysis along with a systematic manual analysis process in order to flag, check, and double-check anything we review, in order to rigorously identify and expose Russian propaganda, avoid false positives and McCarthyism, and effectively encourage others to get their news from more reliable sources. As such, we have developed and use the following steps, or Checks, when performing manual analysis of potential propaganda outlets and highlighting them in various ways:

- 1) Check to see whether the social-media account/commenter/outlet *consistently cites obvious Russian propaganda outlets* such as Russia Today/rt.com, the Russian defense ministry, and other official Russian spokespeople.

2) Check to see whether the social-media account/commenter/outlet *has a history of reusing text directly from obvious Russian propaganda outlets, especially without attribution.*

3) Check to see whether the social-media account/commenter/outlet *has a history of generally echoing the Russian propaganda "line"* by using themes, arguments, talking points, images, and other content similar to those used by obvious Russian propaganda outlets. These themes include:

- How wonderful, powerful, innocent, and righteous Russia and Russia's friends are: Putin, Donald Trump, Bashar al-Assad, Syria, Iran, China, radical political parties in the US and Europe, etc. Investigate this by searching for mentions of, for example, "russia", on their site by Googling for "site:whateversite.com russia", and seeing what comes up.
- How terrible, weak, aggressive, and corrupt the the opponents of Russia and their friends are: The US, Obama, Hillary Clinton, the EU, Angela Merkel, NATO, Ukraine, Jewish people, US allies, the "mainstream media", and democrats, the center-right or center-left, and moderates of all stripes. Investigate this by searching for mentions of, for example, "NATO", on their site by Googling for "site:whateversite.com NATO" and seeing what comes up.
- An obvious bias towards Russia and Russian-backed policy in foreign affairs, including:
 - How fantastic Brexit and Ukrainian/Georgian separatism is, but how terrible Chechen separatists are,
 - How advanced Russian technology is, and how dangerous Western technology is,
 - How great it is when Western secrets get exposed, but how terrible it is when Russian ones do,
 - How militarily powerful Russia and their friends are, and how weak and craven Russia's enemies and their friends are, etc.
- How dangerous standing up to Russia would be: It would inevitably result in "World War 3", nuclear devastation, etc, and regardless of who shot first or is bombing civilians where now, would be the West's fault. Russian propaganda *never* suggests it would just result in a Cold War 2 and Russia's eventual peaceful defeat, like the last time.
- Pre-emptive discouragement of critical analysis: Assertions about them "having the truth", or the need to "wake up the sheeple", or how the "mainstream media" can't be trusted.
- Hyperbolic alarmism, anti-Western conspiracist insinuations, "Eurasianism", racism, gold-standard nuttury and attacks on the US dollar, 9/11-trutherism, anti-Semitism, anti-"globalism", anti-vax/anti-GMO paranoia, and generally ridiculous over-the-top assertions, which cites Russian propaganda outlets as "evidence".

Please review our [Frequently Asked Questions](#) and our [Reference Articles](#) pages on our site for more background.

4) Check to see whether the social-media account/commenter/outlet *has a history of echoing the Russian propaganda "line" in weird ways:*

- Do they have propaganda-like content that *mentions Russia in a positive light for no clear reason?*
- Do they have propaganda-like content that *randomly extols Russia and belittles the US?*
- Do they have propaganda-like content *unrelated to the purported focus of their branding?*

- Does the *timing* of their propaganda-like content *coincide with or closely follow similar content on known Russian propaganda outlets*?

5) Check to see whether the social-media account/commenter/outlet *lacks the hallmarks of good actual journalism*: Are the stories factual? Are the facts placed in appropriate context? Do the headlines match the content? Are the agendas of the sources clearly disclosed? Are there good explanations? Does it bring clarity to complicated issues? Is there an absence of hype?

6) Check to see whether the social-media account/commenter/outlet *has been called out by other fact-checkers, journalists, debunkers, etc, already*.

7) Check to see whether the social-media account/commenter/outlet *steadfastly avoids coherently proposing constructive solutions to anything*. The point of propaganda isn't just to get people worked up--it's also to create a sense of decision paralysis, and fear of a complex and seemingly frightening world.

8) Given all that, check to see whether the social-media account/commenter/outlet *qualifies under our definition of propaganda*:

A systematic form of persuasion that attempts to influence the emotions, attitudes, opinions, and actions of specified target audiences for political, ideological, and religious purposes, through the controlled transmission of deceptive, selectively-omitting, and one-sided messages (which may or may not be factual) via mass and direct media channels.

As an example of how this all can work, refer to our example post about this on our site, where we review the domain HangTheBankers.com.

After building on previous reporting, using our automated tools, and then checking our work manually, we again use our software tools to fill in the blanks, collecting a wide range of data about any new target sites discovered through the previous steps, and seeing how they might fit into the existing network of previously red-flagged and identified outlets. We have built out a significant network of websites, YouTube channels, Facebook pages, Twitter accounts, etc, which appear to be part of the same larger Russian influence operation. Every time we feel confident that we have discovered most of them, we uncover more.

A Prior-Research Case Study: ZeroHedge.com

In some cases, traditional-journalist reporting has uncovered interesting connections between outlets which we have identified, through our multiple overlapping checks and analyses, as Russian propaganda. Take, for example, ZeroHedge.com, which we review on our site, but examine in more technical detail here.

Targeted at Wall St. professionals and people interested in the finance sector, it is now the 407th most-popular site in the United States (according to Alexa.com), with 18.7m monthly page views in the U.S., averaging roughly 8 minutes a visit (according to SimilarWeb.com). It is one of the top finance-industry news sources for American audiences, and was rated as one of the top ten most popular financial blogs in the U.S. by Time Magazine.

The ZeroHedge.com homepage, sans ads, as of October 23rd 2016

New York Magazine ran an extensive profile of the site, titled [The Dow Zero Insurgency](#), in September 2009, doing some research into the site's apparent founder, Daniel Ivandjiiski, and including this comment about Zerohedge's tone:

"It's nihilist, and that kind of vision lends itself to all manner of overreaching and conspiracy," says Felix Salmon of Reuters. "You need some kind of critical judgment to separate out the [stories] that make sense and the ones that don't. Zero Hedge just seems to not care about that. It doesn't matter if it's not true."

In November 2011, the Streetwise Professor blog [did some excellent digging](#), and is to our knowledge the first writer to systematically compare ZeroHedge to Russia Today/RT:

'ZH's editorial line on the US and European economies parallels almost exactly that of RT. Moreover, although ZH is unsparing in its criticism of virtually every Western government leader, it never whispers the slightest word of reproach about Vladimir Putin or Russia. Indeed, a tweet mentioning that fact almost immediately drew a response from ZH: a link to a ZH piece spouting a common line of Russian propaganda argument about the superior fiscal foundation of Russia as compared to the US.'

Our followup research and content analysis has confirmed that that seems to be the case. The Streetwise Professor story goes on to make the connection that the the father of Zerohedge's founder appears to have been a Bulgarian intelligence officer during the Cold War:

'Its creator is Daniel Ivandjiiski, a native of Bulgaria. Daniel has a very dodgy past, including losing a job and his securities license for insider trading. None of this is hard to find out: it was

covered in a New York Magazine piece that ran soon after ZH first gained notoriety. Mr. Ivandjiiski's checkered past perhaps explains his clearcut antipathy for Wall Street. But there may be more to it than that.

In light of my flash analogy of ZH to a Soviet disinformation operation, what is really interesting is the background of Daniel Ivandjiiski's father. Ivandjiiski *pere* (Kassimir) was a Bulgarian "journalist" and "envoy" during the Cold War. A member of the Bulgarian Ministry of Foreign Trade, in the COMECON and EU departments. A journalist. A "special envoy" (hence presumably with very useful diplomatic cover) in every proxy war in Central Asia and Africa in the 1970s and 1980s.

That is an intel operative's CV with probability 1. Probability 1. Every one of those jobs was a classic cover. There is no doubt in my mind whatsoever—none—that Mr. Divandjiiski senior was a member of the Bulgarian Committee for State Security (Държавна сигурност or DS for short)—the Bulgarian equivalent of the KGB. And remember that Bulgarian DS was the USSR KGB's most reliable allied service during the Cold War. It carried out wet work in western countries, notably the "umbrella murder" of Georgi Markov in London...

Perhaps it is just coincidence that the son of an obvious Warsaw Pact intelligence service agent with the "journalistic" and "diplomatic" background commonly used in influence and disinformation operations starts a website that employs classic influence and disinformation methods, and spouts an editorial line dripping with vitriol and hostility for American (and Western European) financial institutions and governments: a line that follows that of RT quite closely. Perhaps.'

Three years later, in November 2014, the Streetwise Professor Blog ran a followup story about Zerohedge, called [How Do You Know That Zero Hedge is a Russian Information Operation? Here's How](#), which analyzed a particularly egregious case in which ZeroHedge echoed a deeply misleading story on an obscure Russian-language website, [Iskra News](#), blaming the U.S. for Ukrainian gold going missing from the central-bank vault:

'Shortly after Yatsenuk disclosed the theft of the gold, stories started appearing on the web, first on a Russian website, claiming that the gold had been spirited out the country: including on ZH, which quoted the Russian web story. This obviously serves a Russian purpose: it presents a counter-narrative that blames the theft of the gold not on Yanukovich, or the Russians, but on the new Ukrainian government and the United States.

This is the classic Soviet/Russian agitprop MO that I noted 3 years ago. A story appears in an obscure publication, typically outside the US or Europe, where it has been planted by Soviet/Russian intelligence. It is then picked up by another, more widely read publication, in Europe or the West. Maybe it works its way through several additional media sources. It then gets disseminated more widely in the west, sometimes making it to prestige publications like the NYT.

In the era of the web, the information weapon needn't make it that far. Getting into a widely-read web publication like Zero Hedge which is then linked by numerous other sources and tweeted widely ensures that the lie goes viral.

ZH is an important transmission belt moving the story from Russian propagandists/information warriors to western news consumers. It happens a lot. This is a particularly egregious example, but the transmission belt runs almost daily. ZH is as much a part of Putin's information warfare as RT. If you follow closely enough, it's as plain as the nose on your face.'

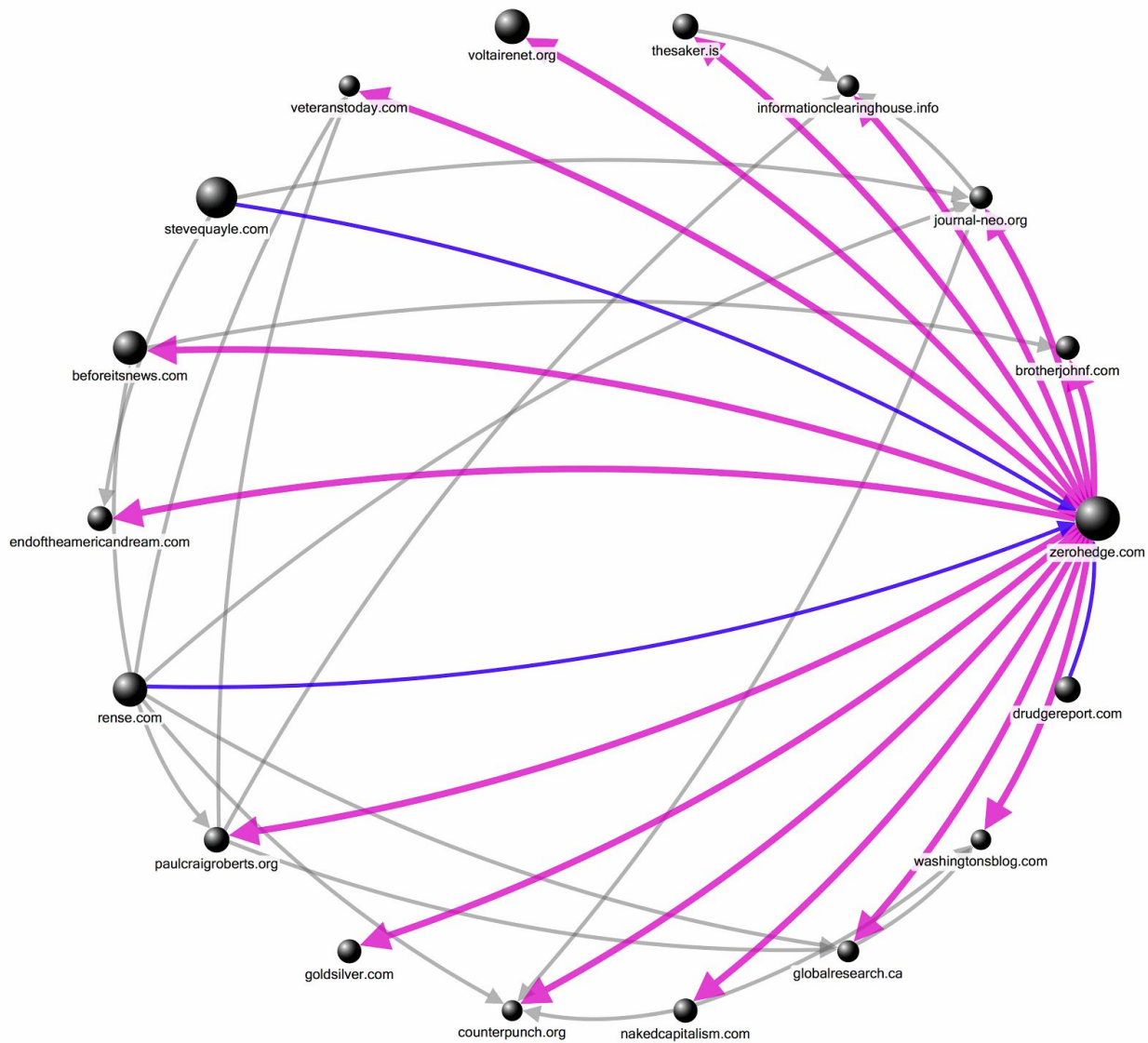
Then, in April 2016, Bloomberg ran a story called [Unmasking the Men Behind Zero Hedge. Wall Street's Renegade Blog](#), which extensively quoted a disgruntled former employee of ZeroHedge named Colin Lokey, who described "writing as many as 15 posts a day of as many as 1,500 words each", and getting some very relevant quotes:

'Lokey, who said he wrote much of the site's political content, claimed there was pressure to frame issues in a way he felt was disingenuous. "I tried to inject as much truth as I could into my posts, but there's no room for it. "Russia=good. Obama=idiot. Bashar al-Assad=benevolent leader. John Kerry=dunce. Vladimir Putin=greatest leader in the history of statecraft," Lokey wrote, describing his take on the website's politics...

"I can't be a 24-hour cheerleader for Hezbollah, Moscow, Tehran, Beijing, and Trump anymore. It's wrong. Period. I know it gets you views now, but it will kill your brand over the long run," Lokey texted Ivandjiski. "This isn't a revolution. It's a joke."

Meanwhile, in February 2016, Andrew Aaron Weisburd's blog [Aktivnyye Meropriyatiya|Active Measures](#) published an analysis of SimilarWeb referrer data, highlighting ZeroHedge, and building out a network graph of sites which refer their audience to each other, titled [The Fringes of Disinfo: A Network Based on Referrers](#). We at PropOrNot replicated and evaluated that initial work, and found it to contain a significant number of false positives. While meeting narrow technical criteria of interlinkage, many sites in his network did not have key characteristics of Russian propaganda, in terms of content or other "tells", which we outlined earlier in this report.

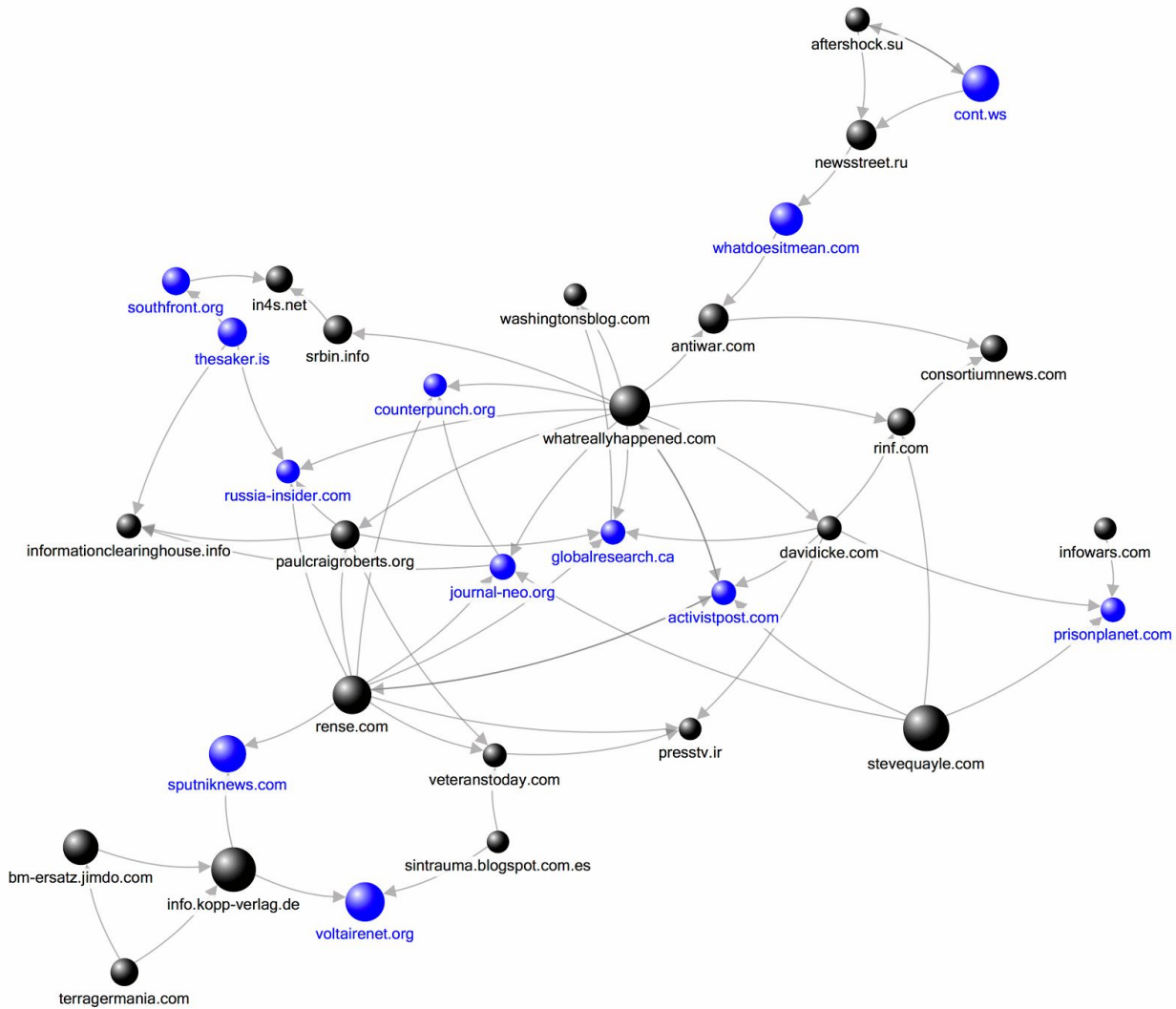
However, Weisburd's follow up research was much more focused, and we started building off it. Later in February 2016, he posted [Disinformation Flows - A Second Look](#), in which he focused down the core referrer network surrounding ZeroHedge:



ZeroHedge.com referrer network (illustration by Andrew Aaron Weisburd)

Weisburd then went on to drill down into the subset of the referrer network subset of the network which included sites that had been flagged on Twitter by the [@EUvsDisinfo](#) team as propagating Kremlin disinformation. The [@EUvsDisinfo](#) account is a project of the European Union’s East Strategic Communications Task Force, and does excellent work, which we at PropOrNot are also using to inform our efforts.

Weisburd’s network next graph just included the sites identified by EUvsDisinfo, with the ones in ZeroHedge’s core referral network highlighted in blue:



ZeroHedge.com referrer network focused on sites identified as disinformation by @EUvsDisinfo (illustration by Andrew Aaron Weisburd)

We have systematically confirmed the EUvsDisinfo/Weisburd findings in this case. Weisburd’s comment from that post bears repeating here:

‘To the extent any of these sites are involved in supporting Russian objectives that run counter to Western interests, they - and more to the point, the people who operate them - should be of interest to the security services of the Western countries in which they live, work, and acquire services related to their websites. At the same time, one frequently finds direct links from these websites to Russia and individuals in Russia clearly associated with the Kremlin and Russian intelligence services. It is always worthwhile to look for criminal activity occurring on the periphery of such websites, particularly on the backend of the operations, involving people who host the sites, register the domain names, and otherwise provide logistical support. And finally, many sites involved in Kremlin disinformation work now solicit donations online, raising the distinct possibility that the online fundraising accounts are being used to move or launder funds.’

Our analysis is clear that some of these sites Weisburd identifies are Iranian, like PressTV, which is an official state-run Iranian propaganda outlet, and Al-Masdar News, which is the official TV network of Hizballah. Nonetheless, they reuse each other's content extensively, echo messages similar to each other, and consistently refer their audiences to each other. This makes sense considering that Russia, Iran, and Hizballah are allies. It would be surprising if they did not.

That analysis of Zerohedge's referral data leads to a remarkable collection of similar sites and provides us with a useful jumping-off point for our own research.

Spidering, Correlating, Reviewing, Spidering

We at PropOrNot conducted our own research into ZeroHedge, and found that it definitely qualifies as Russian propaganda according to both our "initial red-flag" and "detailed" criteria. We also replicated and extended Andrew Aaron Weisburd's research above, and collected all relevant public-record information about the site, the people involved, etc, along with what we could about its finances, audience, and reach.

However, we have extended existing research to use tools like [AnalyzeID.com](https://analyzeid.com), as well as analysis of the site code itself, to examine whether ZeroHedge shares interesting technical "tells" with other sites. These tells include things like Google Analytics IDs, Amazon affiliate codes, WHOIS data, hosting data, ad-network utilization, SEO techniques, etc. For example, we discovered that Zerohedge shares Amazon Affiliate Codes with two other sites, which share Adsense and Google Analytics IDs with each other:

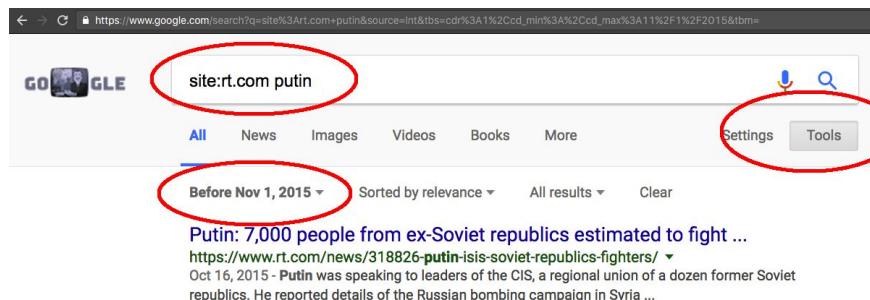
Analyze	Domain	Adsense	Google Analytics	Amazon Affiliate
Very possible	zerohedge.com		ua-11-08	123feebet-20 prepping0a-20
Very possible	readynutrition.com	ca-pub-8704497261580929	UA-6966245-2	googhydr-20 123feebet-20 splan-20 thes0d-20 stucosuccess-20 theprejou-20 natblaze-20 archive0d-20 theorgpre-20 prepping0a-20 Show less
Possible	shtfplan.com	ca-pub-8704497261580929	UA-6966245-1	googhydr-20 123feebet-20 splan-20 thes0d-20 houstzombi-20 charleshughsm-20 ccsb-20 survivalistblogshop-20 thebur01-20 theeconomiccollapse-20 Show less

This suggests that the same folks may run ZeroHedge.com, ReadyNutrition.com (“The Prepper’s Blueprint”) and SHTFPlan.com (“When it hits the fan, don’t say we didn’t warn you”). At the very least, some of the revenue derived from sales that they refer to Amazon may go to the same accounts, and this provides a useful jumping off point for further research.

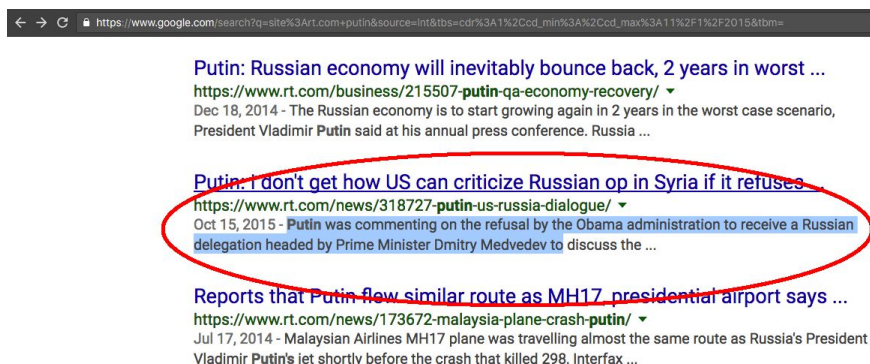
ReadyNutrition.com and SHTFPlan.com are undoubtedly run by the same team, considering that they share the same Google Analytics ID and AdSense ID. Follow-up manual and automated analysis has found that, according to our criteria, both ReadyNutrition.com and SHTFPlan.com consistently echo, repeat, and refer their audience to official and semi-official Russian propaganda outlets. They thus qualify as Russian propaganda outlets themselves, regardless of how they host advertising and “prepper”-related affiliate marketing as well.

Many of the other websites, social-media accounts, commenters, YouTube Channels, etc, that we have identified share similar technical “tells”, and we are using them to build out our map of outlets and the connections between them.

One less-technical way to explore this is by using custom search operators to identify sites which quote arbitrary snippets of text from official state-owned and semi-official Russian propaganda verbatim. For example, by using the "site:rt.com putin" syntax in the Google search bar, one can search the state-owned RT website for mentions of Putin. By using Google's Tools -> Any Time -> Custom Range feature, one can search for mentions of "putin" from a given date range, and find a presumably obscure story about Putin. Searching for text from that story in quotes reveals that a surprising set of other websites will have effectively echoed RT's story about Putin. It looks like this:



First search the state-owned RT.com website for mentions of Putin from a random time



Find some random text from a random story on RT.com and search for exact matches, using quotemarks



These domains are echoing RT.com directly, sometimes without attribution, and are potential targets for different kinds of automated and manual analysis

We are also applying plagiarism-analysis algorithms to investigate what websites, social media accounts, and other outlets share the same talking points, with a particular focus on seeing who reuses text directly from Russian official and semi-official propaganda outlets - especially without attribution. Searches across social networks, YouTube, and other platforms can often yield interesting results as well, and we are starting to explore them.

Our team of volunteers are automating this process, integrating commercially-available analytics services, and building out an infrastructure capable of mapping and analyzing the spread of Russian propaganda across the major online-media platforms, and measuring its reach into U.S. audiences. We would ideally like to help lay the groundwork for rigorous academically-publishable research in this regard, and we encourage others to develop their own approaches to replicating our findings.

Following a Specific Story: The Tale of the Painted Jets

Besides using automated analysis, manual analysis, and prior reporting to identify new outlets and accounts as echoing, repeating, and referring their audience to Russian propaganda, we also use similar approaches to track particular stories and analyze their audiences over time.

One example is a remarkable fake-news story about US military aircraft being repainted (in order to attack Syria while pretending to be Russia, naturally) that went completely viral, even though it was essentially debunked before it even got started. This is one example of how fake-news propaganda outlets can amplify a story that advances Russian strategic narratives, and integrate with official Russian state-owned media like Russia Today to push a story to US audiences through multiple channels. Thanks to its specificity, this is a story we can get something of a handle on.

On October 6th, a Canadian journalist, Christian Borys, took pictures of US military aircraft in pseudo-Russian colors, noting that it is "standard training, but interesting nonetheless", and [posted the photos on Twitter](#):



[A veritable army of Pro-Russian Twitter accounts](#) picked it up immediately, asserting that this was preparation for some larger "false flag" operation, in which the US would presumably attack some civilian target and then blame it on Russia. Over the next few days, Mr. Borys repeatedly complained that the "U.S uses "aggressor units" to train pilots. The paint schemes make fighters similar to Russian counterparts. Stop with the conspiracies", but that didn't help:



His attempts at rebuttals did not stop the rumor-mongering. Pro-Russian and Russian-speaking Twitter accounts exploded with this nonsense, like [this gray-market currency systems developer](#), [pro-Russian "Ukrainian"](#), and [pro-Russian Dutch fascist](#), among others. This rattled around the Twittersphere, and the Russian state-controlled social network VK, for a few days.

On October 7th, a notable US-facing Russian propaganda outlet, moonofalabama.org, [posted an article with the same pro-Russian conspiratorial spin as the above-mentioned pro-Russian Twitter accounts](#), ignoring all Mr. Borys' attempts to debunk it:



[Moon of Alabama echoing "false-flag" rumors and tying in larger nefarious motives](#)

A wide range of other outlets that consistently echo, repeat, and redirect their audiences to Russian propaganda immediately ran with and reposted Moon of Alabama's post:

The screenshot shows the Global Research website interface. At the top, there is a navigation bar with links for About, Contact, Membership, Store, and Donate, along with regional links for USA, Canada, Latin America, Africa, Middle East, Europe, Russia & FSU, Asia, and Oceania. The main header features the Global Research logo and search bars. The article title is "Syria: Is the U.S. Preparing a False Flag Bombing?" by Moon of Alabama, dated October 08, 2016. A quote from the article reads: "There is a curious coincidence of a remark Secretary of State Kerry made to Syrian opposition activists and a new paint scheme applied to some U.S. military jets." Below the quote is a photo of John Kerry speaking at a podium. The article is categorized under "War Crimes" and "Militaryization".

[Global Research echoing Moon of Alabama](#), on October 8th (<2k shares, but 77 linking domains)

The screenshot shows the Conspiracy Cafe website. The main heading is "Conspiracy Cafe" with a sub-header "Conspiracy, alternative news, history, intelligence agencies". The article title is "SYRIA - IS THE U.S. PREPARING A 'FALSE FLAG' BOMBING? (U.S. JETS PAINTED IN RUSSIAN COLORS!)" by George Freund, dated October 8, 2016 at 8:10 AM. The article includes a photo of military jets on a tarmac. A quote from the article reads: "Originally appeared at MoonOfAlabama. There is a curious coincidence of a remark Secretary of State Kerry made to Syrian opposition activists and a new paint scheme applied to some U.S. military jets." The website has a sidebar with navigation links and a categories list.

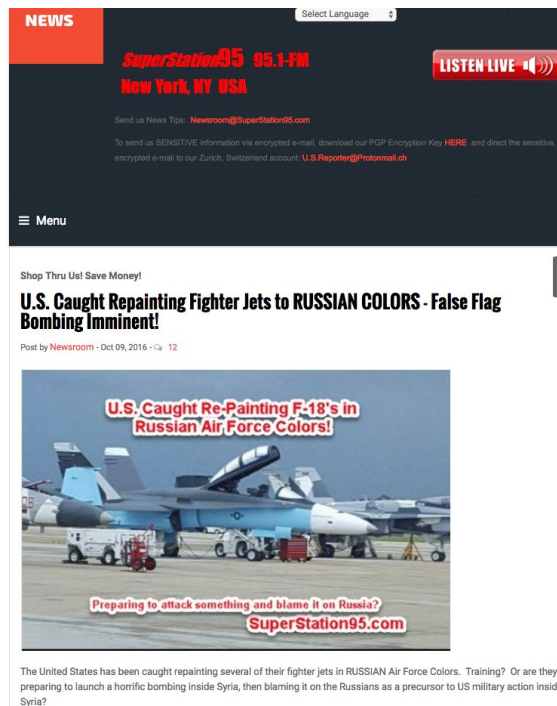
[Conspiracy Cafe echoing Moon of Alabama on October 8th](#)

Over the next several days, other consistently pro-Russian sites repeated their own variations of the same theme, racking up an increasing amount of views and social media engagements, reaching an ever-larger number of people, and boosting the story's search engine visibility.

Also on October 8th, a consistently pro-Russian account pushed it to Reddit:



[Reddit post of the same story](#) on October 8th




[SuperStation95 echoing the story further](#), on October 9th (garnering more than >38,000 Facebook engagements, and getting links from 49 separate domains!)

Public Intelligence Blog The truth at any cost lowers all other costs

HOME ABOUT BLOG BOOKS ESPAÑOL LINKS REVIEWS WHO

Oct 10 **Mongoose: US Painting Fighters with Russian Colors — False Flag Attack in Syria Possible?**

Categories: IO Deeds of War



Syria: Is the U.S. Preparing a False Flag Bombing?

A Canadian journalist based in Eastern/Central Europe, Christian Borys [tweeted](#) yesterday:

Christian Borys @IsBorysThe U.S is painting their F/A-18's to match the paint schemes of Russian jets in #Syria. Standard training, but interesting nonetheless. [pic.twitter.com/FVN6M2Zj](#)

Subscribe Free No Ads

Email Address

Subscribe

Donate If You Can!

Donate

Each donor receives a personal thank you email from Robert Steele that opens a conversation.


Fixing a Rigged System

NO terror

MENU

IS OBAMA PLANNING DRASTIC 'FALSE FLAG' ATTACK IN SYRIA?

not3 | 12 October 2016 | News | No Comments




Western elite exploitation of 'false flag' attacks is well known. The most notorious in Syria have involved the use of poison gas by 'rebels' which have then been blamed on government forces. More recently, Western media outlets are concentrating on trying to build public support for intervention to save the terrorists pinned down in eastern Aleppo, with fake news widely used to try to demonise government forces striving to liberate the whole of the city. Here's a particularly blatant example:

[The "Public Intelligence Blog" echoing the story further, on October 10th](#)

[NoTerror.eu echoing the same story on October 12th](#)

Various obscure and frequently pro-Russian YouTube accounts started pushing out badly-made video content about it. [This one alone](#) got over 11,000 views, and it is exceptionally terrible and content-free:

YouTube Search Upload Sign in



!!BOOM!! USA Caught Repainting Fighter Jets to RUSSIAN COLORS!!!

A Entertainment

Subscribe 18,280

11,614 views

Up next

Autoplay

Funny Comparison American Jets Vs

The Joint Forces Channel

2,136,731 views

6:29

163 68

On October 10th, Snopes, the famous fact-checkers, picked it up and comprehensively rebutted the whole thing. That didn't stop it:



Fact Check › Politics › Conspiracy Theories

False Colors

A rumor circulating among conspiracy theorists holds that the U.S. repainted some of its fighter jets to look like Russian planes in preparation for a "false flag" attack on Syria.

David Emery
Oct 10, 2016

SHARE **944**



CLAIM: The United States was caught repainting some of their fighter jets in Russian air force colors for a false flag bombing.



[Snopes rebuts the "painted jets" rumor-mongering](#), October 10th (<1k shares, 16 linking domains)

Then, on October 11th, the day after the Snopes rebuttal, Russia Today picked up the rumors, with a story focused on reporting the rumors, and their piece got an immense amount of coverage. Russia Today did not include and still does not include a link to the Snopes analysis debunking the rumor:



Home / Viral /

Aggressor squadron? Pics of US jets painted in Russian colors spark Syria false flag conspiracy

Published time: 11 Oct, 2016 07:05
 Edited time: 11 Oct, 2016 15:44

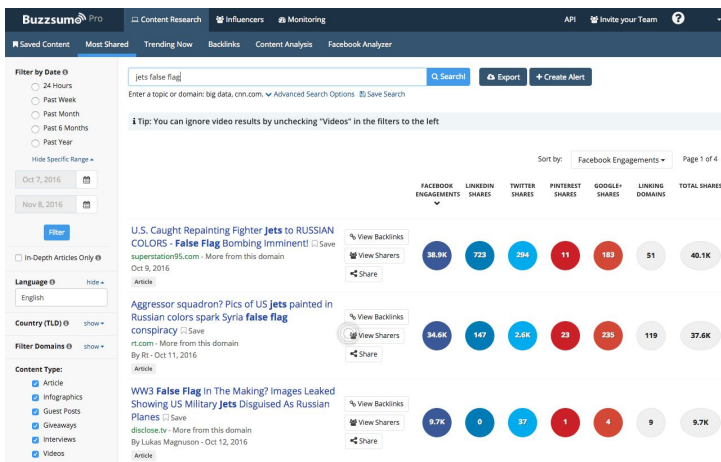


© AiirSource Military / YouTube

Photos showing US jets being painted Russian colors have triggered debates and conspiracy theories online, with many saying Washington plans to conduct false flag attacks in Syria and blame them on Moscow.

[Russia Today stokes the rumor-mongering, after it was debunked by Snopes, October 11th \(garnering 34,600 engagements on Facebook, many more views, and 117 linking domains!\)](#)

We invite the other researchers to explore this story and others like it, using Buzzsumo, Google, Trendalizer, etc. The engagement and linking domain data comes from Buzzsumo, [starting here](#):



To review, the story was preemptively debunked by the originator, but echoed and repeated and referred to by a wide array of pro-Russian social media accounts and websites that consistently echo, repeat, and refer their audiences to each other, and to Russian state-owned media - even after it had been roundly debunked by Snopes. It was false from start to finish, yet garnered over 100,000 likes, comments, and shares on

Facebook alone, and was linked to by scores of separate websites.

Following a Specific Story: The Tale Hillary Clinton's "Parkinson's"

On Aug 22, 2016 a particularly intense spate of Hillary Clinton health rumors, which greatly increased that narrative's exposure in the context of the campaign, were sparked by this story, from a relatively-obscure but typically pro-Russian propaganda outlet, TruePundit.com:



A wide range of outlets, but especially Russian propaganda outlets, had been discussing Hillary's health previously, but this assertion cited Wikileaks, and [then got cited by by a more-significant pro-Russian outlet \(ThePoliticalInsider.com\)](#). It really took off, garnering over 74,000 Facebook engagements and being linked to by over 154 separate domains. The rest of the fake-news echo chamber network, notably including angrypatriotmovement.com, americasfreedomfighters.com, beforeitsnews.com, and wearechange.org, immediately picked it up and started rebroadcasting it: Over the next few days it got over 90,000 Facebook engagements and over 8m views, through the at least 152 separate domains that linked to it.

[The next day the Daily Beast nicely rebutted it](#), in an article that got [around 1,700 Facebook engagements](#) and over 30k views through the over 62 separate domains that referred to it.

The rebuttal helped, but wasn't enough. It appears to have had well over an order of magnitude less engagement than what it was trying to rebut.

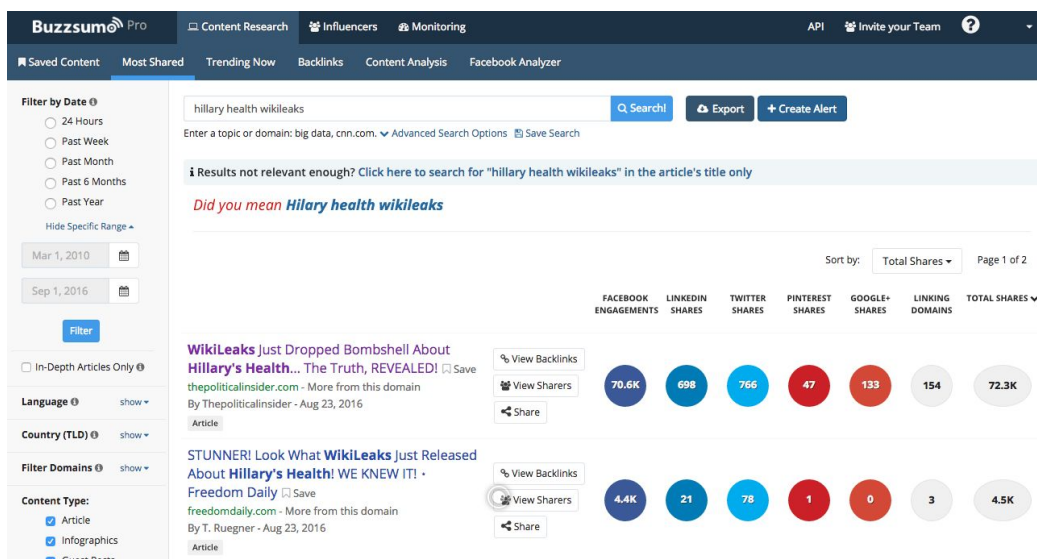
This case is particularly interesting because, while a wide range of other media (including noted Russian propaganda outlets, as rebutted by [pieces like this](#)) had been discussing Hillary's health for some time, this particular narrative was sparked by a groundless assertion based on Wikileaks, picked up by a typically Kremlin-echoing site, and then amplified by the rest of the noise machine, which domestic American sites

picked up a bit as well... but not nearly as significantly.

Our research shows that all the non-propaganda outlets which covered the story, including foxnews.com, toprightnews.com, chicksontheright.com, and youngcons.com, when combined, had less than 8k Facebook engagements and 900k views through the fewer than 10 separate domains that referred to them. That is an order of magnitude less engagement than the pro-Russian echo-chamber propaganda network got out of the story, and several times more than the rebuttal got.

To review, the story started with a consistently pro-Russian propaganda outlet, TruePundit.com, citing a Russian cyberespionage/influence operation, Wikileaks, to add a bogus "data point" to an existing narrative, which had previously been extensively hyped by other types of media but especially Russian propaganda. Non-propaganda media also ran with it, but their effect on the story pales in comparison to that of the Russian propaganda network. The rebuttal, while scathing and comprehensive, was essentially insignificant in comparison.

We invite the other researchers to explore this story and others like it, using Buzzsumo, Google, Trendalizer, etc. The engagement and linking domain data comes from Buzzsumo, [starting here](#):



[Buzzsumo "hillary health wikileaks" story overview](#), sorted by Facebook engagement

Following a Specific Story: Ourselves!

In the early stages of our project, we developed a number of hypotheses about what would happen as our efforts became increasingly well-known. We like to test things, and while rigorously-controlled experimental testing with "in the wild" social media environments is often difficult for projects like ours, we sought to make some predictions about what would happen, and use the resulting coverage to discover new outlets worthy of follow-up review and analysis. Among other things, we expected that:

- 1) The core Russian propaganda outlets (like Russia Today, Sputnik, The Russophile, Southfront, Russia Insider, etc) would be predictably outraged.
- 2) The more-deniable Russian outlets that we identified, along with the Russian comment-troll farms and social-media botnets, would quickly follow suit, in ways that mirrored the core outlets.
- 3) The primary focus of their messaging would be to distract public discourse away from the actual content of the story. They would find whatever else they could to talk about *other* than whether the websites we highlighted actually echoed, repeated, or referred their audiences to Russian propaganda.
- 4) We would be able to divide the resulting commentary into two general categories: *Engagers* and *subject-changers*. The former would engage with the material, attempting to analyze it on its own terms, in historical context, and in light of other research. The latter would be led by the core Russian propaganda outlets, and do everything they could to change the subject.

We are still collecting data on this, but thus far have not been disappointed. Will be releasing our analysis of this over the coming days in order to contribute to the conversation.

Using Google Trends to Measure Larger-Scale Effects

Another line of effort at PropOrNot is attempting to measure the effects of Russian propaganda on the public discourse generally. This is a subtle task, but there are interesting angles from which we can approach it, and we encourage others to experiment in ways that go beyond our findings. We are confident that data scientists at major tech firms and universities will be able to shed significantly more light than we can.

One simple and interesting but decidedly less-than-rigorous example follows from the way that Russian propaganda has long used "globalism" and "globalists" as derogatory scare-words instead of "globalization", in an attempt to demonize what has been largely seen in the West as a relatively secular process resulting from increasingly efficient global communications and transportation. [The New York Times did a great backgrounder on how it has recently been used by Trump et al](#), but did not mention how, almost exclusively, Russia and Russian-aligned actors in the West have been using it for over a decade.

For example, here's [Russia Today, in 2005, highlighting the credentials of one of their talking heads](#), who was the "Chairman of the Public Chamber Commission on Questions of *Globalism* and National Strategy Development, Moscow".

Here's [Russia Today, in 2009, interviewing Kremlin-aligned neo-fascist British politician Nick Griffin](#): "The UK is being broken by internationalism and globalism and needs a nationalist response, says Nick Griffin, leader of the far-right British National Party."

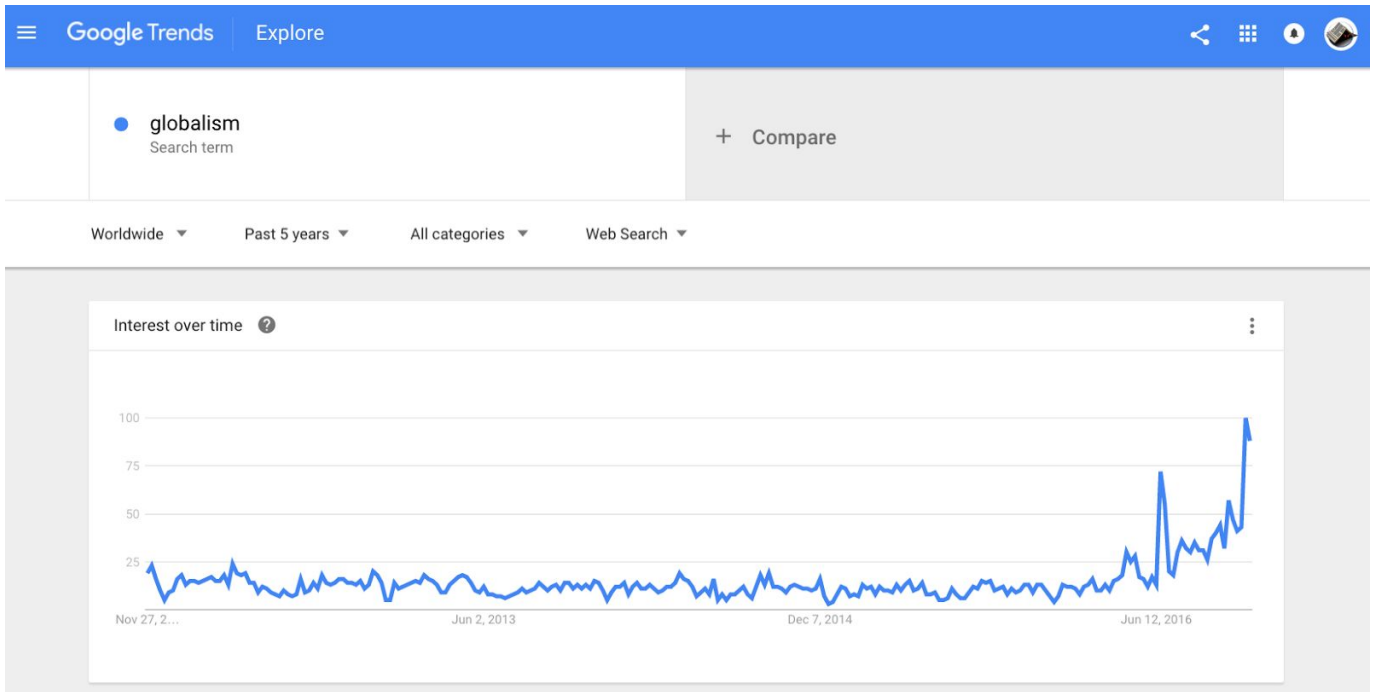
Here's [Russia Today, in 2012, interviewing a Kremlin-aligned neo-fascist French EU MP politician](#), Bruno Gollnisch, about it: "Europe should have been protected against the side effects of *globalism*..."

[Here's Russia Today, in 2013, giving a platform to Rand Paul](#) as he accuses Obama of plotting with 'anti-American *globalists*' to grab guns.

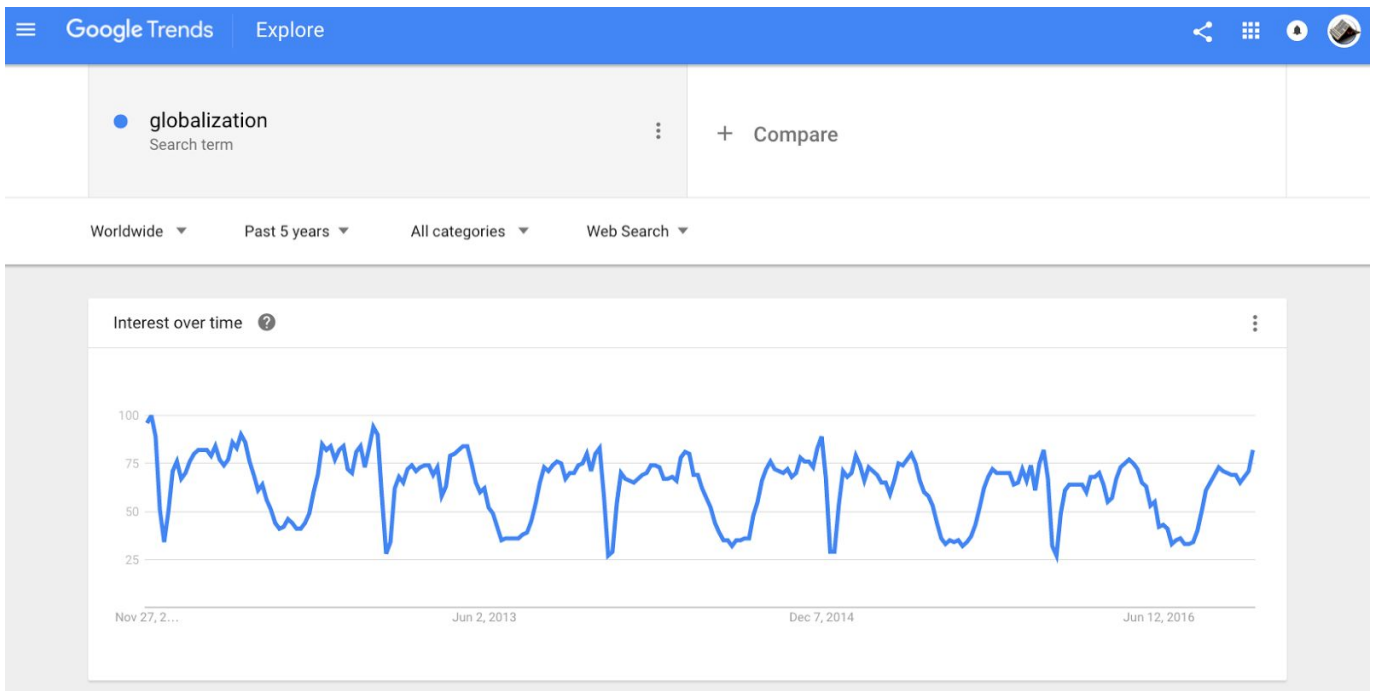
Here's [Russia Today, in 2015, with an editorial from a pro-Russian Yemeni](#) echoing the standard Kremlin line, including this: "We have now entered the uncharted territories of a US-run supra-national police state system, where *globalism* rhymes with authoritarianism."

And here's [Russia Today again, in 2016, decrying "globalism" in all kinds of ways and highlighting Putin as the answer to it](#): "So while I understand westerners who – rightly disillusioned by their own countries – choose to see Putin as a lone hero fighting a rear-guard action against globalism, I don't exactly share their sentiments. One can't help but have a twinge of envy when looking at Russia's Putin..."

[We used Google Trends to evaluate the utilization of the term "globalism"](#), which has historically almost exclusively occurred on Russian propaganda outlets and been used by pro-Kremlin actors, over the past five years. It looks like this:

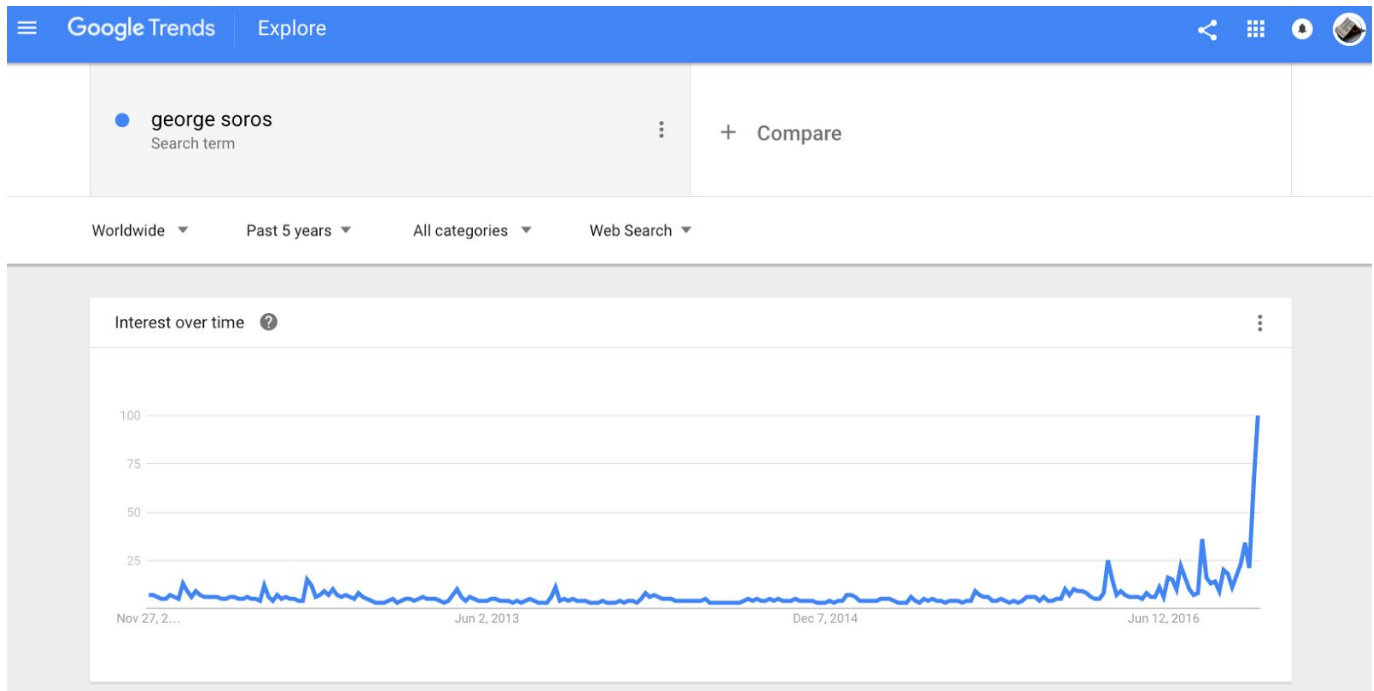


In contrast, [the utilization of the term "globalization" fluctuates seasonally](#), apparently in line with the academic calendar:



For comparison purposes, note that the Kremlin and its allies everywhere *strongly* dislike George Soros. He's one of their major boogiemens, [primarily due to his successful efforts promoting human rights and democratization in Eastern Europe and elsewhere](#), and their propaganda demonizes him constantly.

Bearing that in mind, compare the [Google Trends for "globalism"](#) to the [Google Trends for "George Soros"](#):



Preliminary Conclusions

Thus far we at PropOrNot have identified well over 200 distinct website domains which qualify as Russian propaganda outlets according to our criteria, and target audiences in the United States. We estimate the regular U.S. audiences of these sites to number in the tens of millions. We are gathering data to measure that more precisely, but we are confident that it includes at least 15 million Americans. We estimate that stories planted or promoted by these were viewed over 213 million times, across various social media platforms and directly. We have yet to analyze at least a couple hundred more websites, along with many more YouTube channels, Facebook pages, and Twitter accounts.

We assess that this overall Russian effort is at least semi-centralized, with multiple Russian projects and influence operations working in parallel to manage the direct and outsourced production of propaganda across a wide range of outlets. It is data-driven, and rewards effective entrepreneurship and innovation with increased funding and other resources. There are varying degrees of involvement in it, and awareness of involvement. Some people involved seem genuinely unaware that they are being used by Russia to produce propaganda, but many others seem to know full well.

This Russian propaganda effort resembles a viral marketing effort, with roughly a dozen individual outlets ("sources") actually producing large amounts of original propaganda content. That content is echoed, extended, and amplified through an immense number of other sites, YouTube channels, Facebook pages, social-media botnets, etc. ("repeaters"), and there are both source and repeater outlets targeting different audiences: U.S. military veterans, Wall St. insiders and finance specialists, natural-food and health enthusiasts, racists, homophobes, peace activists, and politically-active Americans on both the right and left.

Next Steps

We are building out our website, and expect to be online in the next day or so. We intend to launch in conjunction with a concerted effort to make the [YYYcampaignYYY](#) go viral, begin crowdsourcing the resulting investigation, and start an informed and perhaps even humorous national conversation about Russian propaganda. It might be too much to hope that such a conversation will be conducted in a calm, sober, or minimally reasonable fashion, but we will do our best to start it off in good spirits.

We are also constantly improving our analytic systems, and expect to have publicly-available and peer-reviewable data available in the near future. However, we are loathe to go public with all our sources and methods for the time being.

While there are a number of long-term possibilities for this nascent initiative, we are keenly aware of the urgency of the story in a larger context. We are working hard to build our systems and launch in a timely fashion, but we request the assistance of professional journalists and other researchers in a few areas:

- **Increase public awareness of the fact that that Russian disinformation is bigger than hacked e-mails** - Russian hacking and selective leaking is accompanied by large-scale, long-term, and remarkably effective efforts to build online propaganda outlets targeting U.S. audiences. Sites with U.S. audiences estimated in the millions echo Russian state-owned propaganda consistently and relentlessly attack actual journalism. However, media coverage of Russian disinformation regarding the election has focused on the hacking of e-mails leaving the average voter with no understanding of the concerted effort to influence their thinking regarding Russian interests and ultimately affect their vote.
- **Give this story the systematic and incisive coverage it deserves** - We have brought together a range of concerned citizens with relevant experience and expertise to follow breadcrumbs and connect dots in an effort to identify propaganda targeting a U.S. audience. We want to prevent foreign disinformation aimed at Americans from distorting U.S. political and policy discussions. Instead, we want to strengthen our cultural immune systems against hostile influence, while hopefully improving public discourse generally. In order to get from this point, where we've identified a significant network of disinformation, to our ultimate goal, we need the community of journalism professionals throughout the U.S. to follow up. We need actual journalists addressing this issue, asking the tough questions, and providing citizens with the objective analysis that makes the fourth estate such an invaluable part of the democratic process that is currently under assault. We're eager to help inform those journalistic efforts as best we can.
- **Help answer the following questions**, via questions to official spokespeople and other tools of traditional reporting, in light of the larger circumstances which lend them urgency:
 - **Does the U.S. government have any information about Russian propaganda efforts to build or use fake-"media" online gray and black disinformation outlets, which conceal their association with Russia, to influence U.S. public opinion?**

- **What information is the government able to share** with the American people now that they've cast their votes in the November election?
- **What does the U.S. government assess that Russian propoganda and influence operations in the U.S. include?** What are their target audiences, objectives, and funding and control methods? How successful have they been?
- **Does the U.S. government asses that any particular fake-"media" propoganda outlets targeting U.S. audiences are under direct or indirect Russian influence or control?** If so, which ones?
- **Has Russia been using these propoganda outlets in an attempt to influence the U.S. election?** If so, in support of which candidate? Did it work? Isn't that the sort of information the U.S. government should tell the American people about?
- **Is the U.S. government constrained by constitutional press freedoms** when considering how to address fake-"media" propoganda claiming to conduct actual journalism?
- **Are such constraints preventing the U.S. government from alerting the American people** to disinformation efforts intended to manipulate them, especially as they exercise their right to vote?
- **Was the U.S. government concealing related information from the public in order to avoid interfering in the domestic U.S. political process,** and/or leaving propoganda channels operating in order to monitor and analyze them?
- **By seeking to avoid interfering in the domestic U.S. political process itself, did the U.S. government allow Russia to manipulate the U.S. domestic political process,** through the use of online propoganda along with other methods, in favor of one political candidate over another?
- **By allowing Russian attempts to influence the U.S. election through online propoganda to proceed unhindered, and not alerting the American people to the full extent of ongoing disinformation activity, has the U.S. government withheld pertinent information from the American people directly related to the election?**

Thank you very much for taking the time to review this report, and thank you in advance for whatever following and contributions you might have. We look forward to continuing the conversation.

Sincerely,

-- The PropOrNot Team

propornot@gmail.com

November 25th, 2016