

Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019

RENÉE DIRESTA AND SHELBY GROSSMAN





Stanford | Internet Observatory

Cyber Policy Center

Encina Hall
616 Jane Stanford Way Mall C100
Stanford University
Stanford, CA 94305-6055

io.stanford.edu

Statements and views expressed in this report are solely those of the authors and
do not imply endorsement by the Stanford Cyber Policy Center.

Cover photo by Gregor Sailer from the series *The Potemkin Village*, Carson City, Vårgårda, Sweden, 2016

© Copyright 2019, Stanford Internet Observatory

TABLE OF CONTENTS

1. Document Purpose	3
2. Background and Context	5
3. Key Takeaways	7
4. Summary Statistics and Description of Contents	9
5. Operational Clusters	17
5.1 Fake Personas, Think Tanks, and Media Outlets	17
Fake Personas	17
Suspect Think Tanks and Media Outlets	26
Inside Syria Media Center	27
Crna Gora News Agency	32
Nbenegroup.com	38
The Informer	41
World News Observer	42
Victory for Peace and InfoRos	43
5.2 Operations Targeting Ukraine	51
Committee of Soldiers' Mothers of Ukraine Комитет солдатских матерей Украины	52
For an Exit from Ukraine За вихід з України	55
5.3 Operations Targeting the United States	57
Race	57
Michael Brown Memorial	57
Baltimore is Everywhere	59
Geopolitical Issues	62
White House Griller	62
Kuril Islands	64
5.4 Hack and Leak Operations	70
DCLeaks	72
Fancy Bears	75
Foul Play	80
Southern Front Южный Фронт and Cyber Berkut	83
6. Closing Notes and Future Threats	91
6.1 Assessments Related to Prior Data Sets	91
6.2 Research Limitations	93
7. Appendix	95
7.1 Minor Operation: Antimaidan ukraine [sic]	95
7.2 Residual Pages	96
Endnotes	99



1. DOCUMENT PURPOSE

Upon request by the United States Senate Select Committee on Intelligence (SSCI), researchers reviewed a data set of social media posts that Facebook provided to SSCI. Facebook attributed the material to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (Главное управление Генерального штаба Вооружённых сил Российской Федерации), known as the GU, or by its prior abbreviation GRU, which we will use throughout this document. The data set was provided to SSCI in response to a Committee inquiry about GRU activities on Facebook.

Facebook attributed this collection of 28 folders of data, each consisting of the contents of at least one unique Facebook Page, to the GRU. This report quantifies and contextualizes the material in that data set. It includes a background overview of GRU tactics and methods, a collection of summary statistics, and a set of key takeaways about several distinct operational clusters that are then discussed in detail later in the document. These clusters include the creation of fake personas, publications, and organizations to aid in the dissemination of Russian government narratives; operations targeting Ukraine; operations targeting the United States; and hack-and-leak operations. We discuss these clusters and their component Pages in detail in Section 5: Operational Clusters.

The Pages in this data set were taken down in (or before) 2018 in accordance with Facebook's policy on inauthentic activity and are no longer visible to the public. While some content related to a few of these operations has been unearthed by investigative journalists, we are releasing this report to provide a more thorough view of GRU activities across the broader information environment – media as well as social media.¹

This publication and its conclusions are in part based on the analysis of social media content that was provided to the authors by the Senate Select Committee on Intelligence under the auspices of the Committee's Technical Advisory Group, whose Members serve to provide substantive technical and expert advice on topics of importance to ongoing Committee activity and oversight. The findings, interpretations, and conclusions presented herein are those of the authors, and do not necessarily represent the views of the Senate Select Committee on Intelligence or its Membership.



2. BACKGROUND AND CONTEXT

Colloquially known as the GRU, the Main Directorate of the General Staff of the Armed Forces is the military intelligence agency of the Russian Federation.² The GRU reports to the Russian Minister of Defence, who in turn reports to the President of Russia, the Commander-in-Chief of the armed forces. Consisting of several directorates organized by region and capability, the GRU has human intelligence, signals intelligence, analysis, psychological operations, cyber operations, and kinetic operations (Spetsnaz, or Special Forces) abilities; the GRU's psychological/influence operation and cyber intrusion capabilities are the two that are relevant to this report. The GRU's influence operations capabilities overlap with several other Russia-attributed entities, including the Internet Research Agency (IRA)—a nominally independent social media firm owned by Yevgeny Prigozhin, an oligarch with close ties to Russian President Vladimir Putin.³

The first tactic, the spreading of disinformation, is a well-established Russian tactic for information warfare, part of a series of influence mechanisms called “active measures” [активные мероприятия]. The influence operations in the GRU data set largely follow an established tactical pattern known as narrative laundering, or information laundering, in which a story is planted or created and then legitimized through repetition or a citation chain across other media entities. Notable past examples targeting the US include fake stories attributing the creation of AIDS to the CIA,⁴ and a campaign with fake documents insinuating that the US government supported apartheid.⁵ A related tactic to narrative laundering is boosterism, in which repetitive content is created and disseminated to reinforce the perception that a given position represents a popular point of view; one historical example was the 1970s KGB operation to create thousands of articles bolstering then Prime Minister Indira Gandhi.⁶ This data set illuminates how those strategies have been updated for the digital age with the creation of online sock puppets who serve as authors, “independent media” front websites, byline placement in independently-run politically aligned outlets, and dissemination and amplification via social networks.

The extent of coordination between the various entities with influence operations capabilities—in this case, the GRU and the IRA—is an open question, particularly following the release of the Special Counsel’s Report (colloquially known as the Mueller Report).⁷ The US Department of Justice investigation into Russian interference in the US 2016 presidential election resulted in distinct sets of indictments for GRU officers and IRA employees. The Special Counsel’s report attributed the 2016 US Democratic National Committee and Clinton campaign hacks to GRU Unit 26165 and Unit 74455.⁸ The report includes a citation to cybersecurity firm CrowdStrike, which conducted an early investigation into the DNC systems following the breach, and identified operational signatures of a Russian cyber espionage group linked to the GRU by many different cybersecurity researchers and governments: APT 28, also known as Fancy Bear.⁹ Prior research into the IRA data sets, conducted by New Knowledge,¹⁰ Graphika, and Oxford Internet Institute,¹¹ on behalf of SSCI, enumerated themes present in this GRU data set, including IRA troll accounts boosting hashtags and content related to the GRU hack, some of which were set up shortly before GRU dumps. As yet, however, there has been no concrete evidence of collaboration between the two entities.

In the second tactical function, hack-and-leak capabilities, GRU operations similarly overlap with other Russian intelligence agencies such as the KGB successor agencies—the internally focused Federal Security Service (Федеральная служба безопасности Российской Федерации, or FSB) and the outwardly focused Foreign Intelligence Service (Служба внешней разведки

Российской Федерации, or SVR). Russian media have remarked upon these overlaps, noting that the delineation between GRU and SVR responsibilities “seems to be perceptible only to those inside the two agencies.”¹² Cybersecurity researchers have posited that the entities operate in competition with each other, rather than in coordination or cooperation, and point to instances where one agency inadvertently exposed the activities and presence of the other while hacking the same target.¹³ The Facebook-provided data set does not include attribution evidence related to the hacks themselves, but does provide a view into dissemination pathways for releasing hacked information to the public.

We hope that this analysis of GRU-attributed operations on social platforms and the comparison to previously-released IRA assessments help to inform policymakers and the public about the scope and evolution of information warfare tactics executed by this state actor.

3. KEY TAKEAWAYS

Our analysis has produced three main takeaways.

3.1 Narrative Laundering Updated for the Modern Era

First and foremost, this collection of influence operations has roots in a well-established, decades-old Soviet propaganda strategy of laundering a narrative through aligned publications, “useful idiots,” and, perhaps, unwitting participants. The operations were primarily focused on creating long-form state-aligned propaganda content and seeding it for distribution within other media properties, including authentic media in the local ecosystem. This is distinct from the social-media-first strategy of the International Research Agency (IRA) Pages¹⁴ which focused primarily on memetic propaganda with high virality potential to attract the like-minded and facilitate tribalism.

The GRU narrative strategy also involved the creation of think tanks and “alternative news” sites to serve as initial content drops, from which the content was syndicated or republished on other sites. These think tanks and media sites relied on personas¹⁶—fake online identities that persist over time, or across multiple platforms, and attempt to create a perception that the person behind the identity is real—who served as both bylined authors for the GRU’s own fabricated media properties and “freelancers” who could inject the narrative into other publications under the guise of contributing authors. The content-creator personas served as both authors and amplifiers, often cross-promoting each other’s articles. In addition, we found a network of highly suspicious, likely fabricated accounts who were involved in the *distribution* of the content on other social platforms, including Twitter and Reddit. Upon further investigation, some of those distributors of content related to the Facebook-attributed Pages turned out to be bylined authors of articles unrelated to the Facebook data set, but which we believe are likely related to other GRU operations. We describe the network in detail in this white paper.

3.2 Influence: Narrative vs Memetic Propaganda

Second, when viewed as a *social media operation*, the collection of disinformation campaigns described in this document appear to be largely a failure, or perhaps a half-hearted experiment in new methods. Whereas the IRA expended significant effort building up social pages and engagement, the GRU appears not to have done even the bare minimum to achieve peer-to-peer virality, with the exception of some Twitter networking, despite its sustained presence on Facebook. While GRU-attributed Facebook posts spanned a period from 2014 to 2018—a time when the IRA was operational and actively spending money and effort on audience engagement—only one of the GRU-attributed Pages bought ads. There is evidence of one Page, Inside Syria Media Center (ISM), attempting basic social media marketing techniques to grow audiences and engage with potential amplifiers, but that activity happened on Twitter. The lack of resources and time invested in these Pages and the scant engagement they received suggest that the GRU was either inexpert in the methods used by the IRA or simply not focused on social distribution.

Viewed as a *narrative propaganda operation* to exploit the media environment, however, the campaigns were successful at placing stories from multiple fake personas throughout the alternative media ecosystem. Articles achieved placement in at least 142 alternative outlets and were occasionally amplified by large state media entities as well. While social network engagement (Likes, Shares) is one of the most quantifiable measures of reach, securing article placement delivers the attention of those publications' audiences; a piece of content with minimal engagement on Facebook that nevertheless ends up quoted on RT (formerly Russia Today, the Russian international media network) has the potential to reach an audience of millions. A narrative that is repeated, on multiple sites, in a subsection of a media ecosystem with heavy audience overlap is more likely to achieve a measure of influence within that segment. Understanding the dynamics of narrative laundering through the alternative media ecosystem and its entanglement with state-sponsored overt propaganda properties is critical to assessing modern influence operations.

3.3 Media Coverage of Hack-and-Leak Operations

Third, the data set provides a unique view into the dissemination process that is a necessary part of hack-and-leak operations. Of the multiple forms of Russian interference in the U.S. 2016 election, for example, the GRU hack-and-leak attack on the DNC arguably had the most significant impact, in substantial part due to the resulting media coverage of the obtained materials, not GRU-related operations on social media. One of the unique findings in this data set is the extent to which the the GRU-executed attempt at social dissemination on their own Pages was weak; Wikileaks and direct outreach to press, followed by subsequent mainstream US media coverage, significantly contributed to making the operation effective. This data set helps illuminate the extent to which they were dependent on *media*, not *social media*, to pick up their material and amplify it. This is one explanation for the GRU's lack of investment in audience engagement, in contrast to the IRA: it could reliably depend on other media to publicize the results of its work, rather than having to gin up audience interest on its own. In this data set, we observe several distinct operations (not all US-focused) in which the GRU used social media primarily as a tool for dropping a collection of hacked documents (including, per the responses from targets, edited or fabricated documents). We are able to assess their social Page engagement for the first time, across a number of hack-and-leak operations, to observe the extent to which their social distribution efforts flopped, but media attention (including by RT) led to widespread coverage nonetheless.

4. SUMMARY STATISTICS AND DESCRIPTION OF CONTENTS

The data set provided by Facebook to SSCI consists of 28 top-level folders representing 33 distinct Facebook Pages; several of the folders contain subfolders with similarly named Pages with different account identifiers.

- Page data was divided into subfolders with PDFs consisting of information on Shares, Status Updates, Photos, Linked Media, Ads, and Videos. A majority of the Pages had either Status Updates (posts made to the account by the account holder) or Shares (anything that the account holder has shared, by way of clicking the “share” button on pre-existing content, or posting a link to their page). Several had Photos or Videos (uploaded by the account owner to the Page). One Page ran ads.
- There were 5543 Shares and 1576 Status Updates in the data set. Additionally, several of the data sets contained a small collection of photos or videos related to the posts.
- Engagement was minimal. Across all posts, there were 4,830 Likes, 5,469 reactions, 3,432 shares, and 902 comments.
 - The vast majority of the Facebook posts— 81% of the Status Updates and 78% of the Shares— had 0 engagements.
 - The Pages related to Fancy Bears (primarily sports-focused hack-and-leak operations) had the highest engagement.

Page Name	# of Posts and Shares	Date of first Post or Share	Date of Last Post or Share	Average # of Likes	Average # of All Reactions	Average # of Shares	Average # of Comments	Total Engagement
All Pages	7,315	2012-03-05	2018-08-17	0.7	0.7	0.5	0.1	14,633
Inside Syria Media Center	5,367	2016-10-06	2018-08-15	0.1	0.1	0.2	0.01	1,855
Crna Gora News Agency	1,530	2016-08-29	2017-03-16	0.6	0.6	0.9	0.02	3,232
The Informer	68	2017-08-29	2017-10-19	0.4	0.6	0.01	0.04	73
Южный Фронт (Southern Front)	64	2018-04-13	2018-08-17	0.1	0.2	0.3	0	39
Fancy Bears	56	2016-09-12	2017-08-25	47.9	56.2	15.4	13.2	7,427
Michael Brown Memorial	56	2015-01-27	2016-04-08	0.5	0.5	0.3	0.2	81
Baltimore Is Everywhere	38	2017-05-10	2017-06-01	0.8	0.8	1.1	0.4	120
Victory for Peace	27	2015-03-24	2015-08-04	11.1	11.1	1	0.3	632
DCleaks	22	2016-06-08	2016-09-30	9.6	12.7	12.6	3.0	834
White House Griller	20	2015-04-20	2015-08-05	0.4	0.4	0	0.05	15
World News Observer	19	2016-07-15	2016-07-20	0	0	0.7	0	13
Russian Kuril Islands	14	2014-02-02	2014-10-16	1.1	1.1	0.5	0	37
За вихід з України (For an Exit from Ukraine)	13	2017-06-02	2017-06-30	10.1	10.5	0.2	0.3	274
Sadam Al wahdi	5	2017-02-08	2017-03-14	0	0	0.2	0	1
Polite People of the Capital of Culture	4	2015-08-21	2015-08-21	0	0	0	0	0
Conflict Zone	3	2015-11-25	2015-11-25	0	0	0	0	0
Foul Play	2	2016-10-21	2016-10-21	0	0	0	0	0
Комитет солдатских матерей Украины (Committee of Soldiers' Mothers of Ukraine)	2	2017-03-24	2017-03-24	0	0	0	0	0
Anal	1	2015-06-18	2015-06-18	0	0	0	0	0
Babygone	1	2015-06-17	2015-06-17	0	0	0	0	0
FozNews'	1	2016-10-04	2016-10-04	0	0	0	0	0
Mycompany	1	2012-03-05	2012-03-05	0	0	0	0	0
nbenegroup.com	1	2014-02-03	2014-02-03	0	0	0	0	0

Table 1. Summary statistics for Facebook accounts. Several Facebook accounts had no content in them and are not included in this table. These include Andrew Kolkovich true to life, Antimaidan ukraine, Fdfxc, Music and Company, and Sdf. Spelling corresponds precisely to account name spelling. Total engagements = Likes + Reactions + Shares + comments.

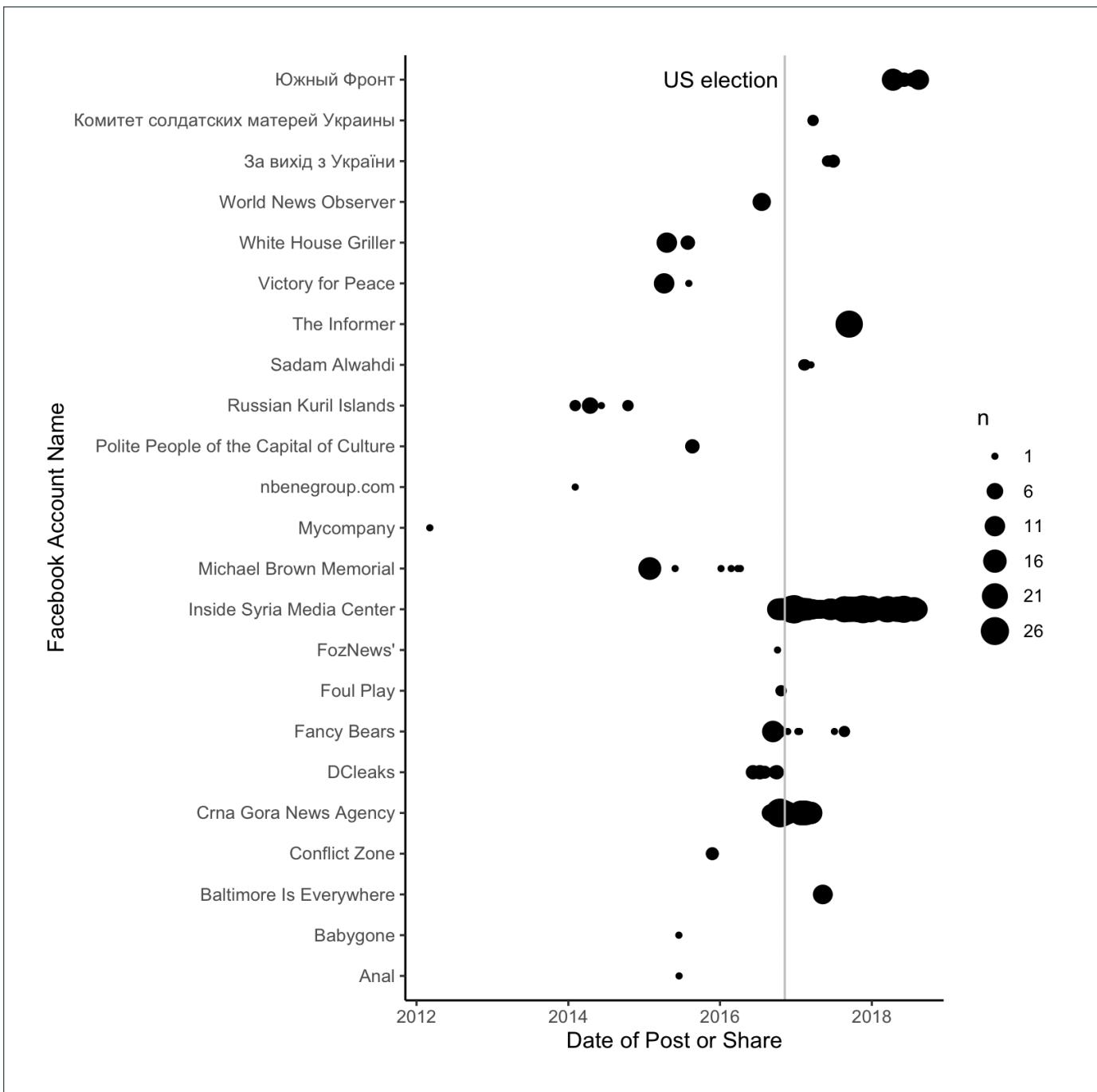


Figure 1. Number of Facebook account posts by date. Inside Syria Media Center and Crna Gora News Agency show the largest number of posts.

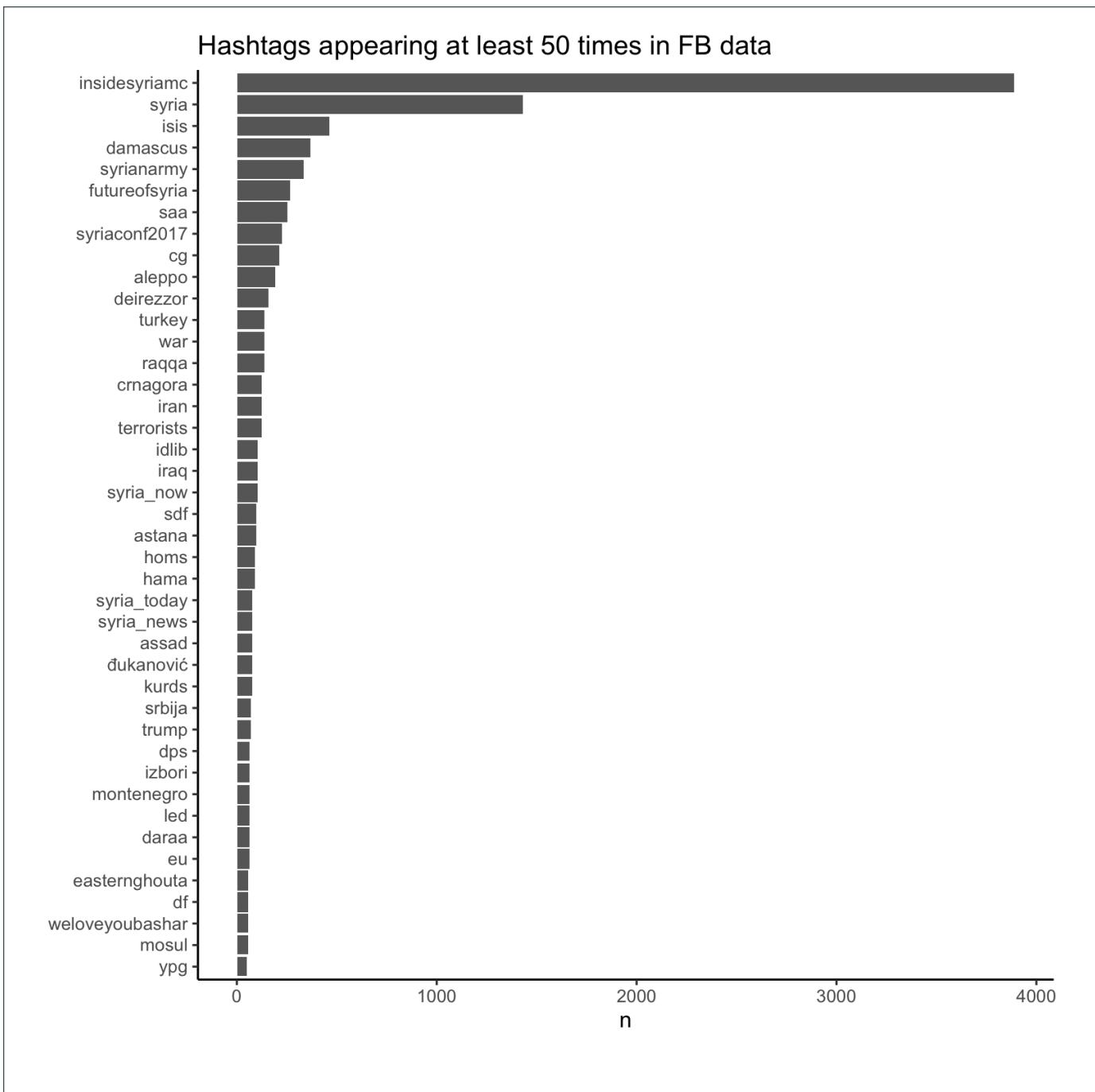


Figure 2. English hashtags that appeared 50 or more times in the Facebook page data. The vast majority relate to the Syria content. #SAA stands for Syrian Arab Army. #CG stands for Crna Gora ("Montenegro" in Montenegrin).

Analyses Performed:

Noting that the data provided was already attributed to the GRU by Facebook, researchers:

- evaluated the content within the folders (within Pages)
- investigated relationships across folders (between Pages)
- evaluated the content, and closely-related content, as it appeared elsewhere on the internet and on other social networks, assessing narrative, authorship, and distribution patterns
- evaluated the content against the previously-provided SSCI IRA data set, to ascertain the extent to which there were thematic, temporal, metadata, or collateral-based similarities between the operations (*this process is ongoing and will be addressed further in subsequent papers*).

4.1 Operational Observations

- The largest collection of posts by topic volume in the GRU data set was concerned with Syria. Inside Syria Media Center (ISMC) had 3,853 Shares (70% of total) and 1,511 Status Updates (96% of total); put another way, it had 5,367 posts, comprising 73% of total overall types of content. Facebook posts primarily linked to the ISMC website, which hosted original, pro-Assad stories in both Arabic and English.
- The second largest collection of posts came from the Crna Gora (Montenegro) News Agency (CGNA), which had 1,530 posts (21% of total). This Page shared content from three different versions of the CGNA website, which had original articles in Bosnian and English in the months before and after Montenegro's October 2016 elections. The articles largely aimed to undermine now-President Milo Dukonović, who has been pro-NATO and pro-EU.
- This data set contained evidence of operations targeting a range of countries, featuring issues related to Ukraine, Syria, Iran, Japan, the United States, the Balkans, Estonia, Germany, and Russia. The IRA-attributed data set provided to SSCI primarily encompassed online operations targeting the United States and Ukraine; this GRU-attributed data is geographically broader in scope, which reinforces existing assessments¹⁷ that Russia uses strategic deception, narrative laundering, and active measures far beyond its targeting of US society and politics.
- Several of the Facebook data set Pages were interlinked. For example, Andrew Kolkovich: true to life bore the name of a fake author persona, purportedly a journalist or analyst, who wrote the articles featured on Russian Kuril Islands.
- Many sites associated with these Pages seemed designed to play on distrust of mainstream media. For example, ISMC's About Page said, "We are going to distinguish between the truth and blatant lies about the situation in Syria."
- Despite the minimal engagement on Facebook, activity related to the GRU Facebook Pages appears to exist on other social platforms including Reddit, YouTube, Instagram, and Twitter. Activity spanning a multitude of popular social networks was similarly observed in the IRA data set; the broad presence allows fake media properties to bolster their legitimacy.
- In addition to social networks, the presence of content bylined by fake and suspicious personas, and conversational commenting activity, appears on Quora, LiveLeak, and Medium as well as a number of message boards. These environments, which blur the lines between social media and publishing, are likely to play an important role in future narrative laundering.

4.2 Commonality between IRA and GRU data sets

- The GRU-attributed Facebook Pages link to 75 unique domains.
 - They link to 19 domains more than once.
 - They link to seven domains more than 10 times. Four of these domains were websites associated with the Pages:
 - (en.)insidesyriamc.com (5,355 links)
 - cgna.info/cgna.me/crnagoranews.wordpress.com (1,525 links)
 - theinformer.life (37 links)
 - fancybear.net (18 links)
 - Because they have identical media property names and Facebook Page names, these domains were likely operated by the same people as the Facebook Pages; thus, the domains are likely attributable to the GRU.
- Of these 75 domains, 55 were also linked to in Twitter posts by accounts that Twitter attributed (in the first data set) to the IRA. However, these domains include mainstream news sites and platforms such as YouTube.
- In the data sets provided to SSCI, GRU Facebook Pages and IRA Twitter accounts shared 597 mutual hashtags. The most common hashtags used in both data sets are almost exclusively centered around the Syrian Civil War: #syria, #isis, #damascus, #syrianarmy, #futureofsyria, #saa, #syriacn2017, and #aleppo. These are thematically significant but not particularly unique or linguistically anomalous. #syriacn2017 was related to a 2017 conference “Supporting the future of Syria and the region,” held in Brussels in April 2017.
- We assess that despite being operationally active during the same period of time, and with some topical overlap, the IRA and GRU were using largely separate collections of assets; IRA accounts on Instagram, Facebook, and Twitter did participate in some of the same hashtags as the GRU accounts, but only at a significant level in relation to Syria. *An assessment of the extent to which there was coordination is ongoing.*

Domain	Frequency in Facebook Data Set	Frequency in January 2019 Russia Twitter Data Set	Frequency in IRA-attributed Twitter Data Set
En.insidesyriamc.com	3,091	2,209	5
Insidesyriamc.com	2,264	1,705	1
Dcleaks.com	7	4	4
Youtube.com	5	3,718	42,803
Cyber-berkut.org	4	1	17
Nydailynews.com	2	100	7,542
Telesurtv.net	2	13	44
Usatoday.com	2	138	1,908
Fancybear.net	18	0	1

Table 2. Frequency of domains across data sets. In the course of investigating the distribution patterns for this Facebook data set, we looked at Twitter accounts from the IRA-attributed data set (delivered to SSCI as well as released publicly), as well as a second public data set that Twitter released in January 2019, attributed to “Russia,” but which the company assessed as distinct from IRA-attributed activity. We will discuss these two Twitter data sets and their possible relationship to GRU activity in Section 6 of this paper. This table shows URLs that appeared at least twice in the Facebook data set, and at least once in the Twitter data sets, in addition to fancybear.net. (Total posts in the Facebook data = 7,315; total tweets in Russia file = 765,246; total tweets in IRA file = 8,768,633.)



5. OPERATIONAL CLUSTERS

The 28 top-level folders in the data set reflected a collection of operations that we assessed in terms of targets and tactics. Major operations are grouped into four clusters. Two are **tactical**: operations involving the creation of fake personas, think tanks, and front media properties, and hack-and-leak operations. The other two are **regional**: a cluster targeting Ukraine, and a cluster targeting the United States. There is also a small collection of isolated content, largely undeveloped and containing only one or two posts, addressed in the appendix to this report.

5.1 Potemkin Personas, Think Tanks, and Media Outlets

Several GRU Pages reveal attempts to port Russia's traditional narrative laundering strategies to an online environment by creating inauthentic media properties and front entities. In this section we will first review fake personas created to author and distribute state-aligned narratives, then assess think tanks and media properties, many of which relied on those personas.

Fake Personas

The creation of personas by intelligence entities for the purposes of socializing or disseminating information is not new. Nevertheless, the process has been updated for the social media era; in many ways it's easier today in online environments where pseudonymity, anonymity, and aliases are accepted social norms. The proliferation of millions of real citizen journalists and independent online media outlets worldwide has led to a bigger crowd in which to hide, as well as more value-aligned authentic media entities within which to distribute malign content.

The GRU-attributed data set reveals what we believe to be fake personas leveraged for two distinct lines of effort: (1) the creation of narrative propaganda, and (2) the distribution of content on social platforms. Most of the personas in the table below *created* content for sites associated with Pages in the data set, as well as for other independent media sites on the internet. Other personas served primarily as *distributors*, or amplifiers, for the sites in the data set, sharing their content on social networks. However, several of the distributors additionally wrote for other sites outside the data set. In the table that follows we present examples of these personas, and outline our criteria for assessing whether an identity is a likely persona, as well as observed evidence for each.

Name Social Platform Presence	Wrote for attributed GRU outlet?	Stolen profile photo?	Disseminated GRU media outlet content?	Social media platform removed account?	Other evidence
Mariam Al-Hijab    	Inside Syria Media Center	Yes	Yes		Media exposé
Said Al-Khalaki  	Inside Syria Media Center	Yes	Yes Also disseminated information about a 2013 hack .	Facebook profile is down; Facebook Group he administered is down.	
Alice Donovan  	Plagiarized Inside Syria Media Center content, amplified DC Leaks content	Unknown; used an Instagram image	Yes	Twitter and Facebook removed profile	Media exposé, Mueller report, FBI assessment
Mehmet Ersoy	Inside Syria Media Center	No known profile photo (or social profile) anywhere			
Anna Jaunger 	Inside Syria Media Center	Yes	Yes	Twitter removed profile	Media exposé
Sophia Mangal    	Inside Syria Media Center (co-editor)	Yes	Yes	Twitter removed profile	Media exposé
Firas Samuri    	Inside Syria Media Center	Two known photos, wearing same shirt		Twitter removed profile	
Jonivan Jones 	The Informer (Chief Editor)				First emerged on Medium to write defenses of Russia related to the Skripal poisoning
Jelena Rakocevic	No; produced Kremlin-aligned writing elsewhere	Yes, from a real person's VK account	Yes, shared Crna Gora News Agency content repeatedly	None appear to exist; only photo was on a press page	Phone number provided to a journalist profile links to a Mercedes-Benz dealership
Milko Pejovic   	No; produced Kremlin-aligned writing elsewhere	Yes	Yes, shared Crna Gora News Agency and Inside Syria Media Center	Facebook removed profile	
Andrew Kolkovich    	Had a Facebook Page named for him, his content used on Russian Kuril Islands Page.	No known profile photo anywhere	Yes	Facebook removed Page named for him	No evidence of an Andrew Kolkovich working at University of Oregon, as he claims in Quora
Adomas Abromaitis    	No, but co-authored with Jelena Rakocevic	One known photo. Cover photo on Facebook is a stock photo		Medium froze account	Targeted communities on Reddit and other forums flagged him as a Kremlin troll; Facebook friends with many stub profiles with Russian model profile photos

Table 3: Examples of personas and criteria for assessing whether an identity is a likely persona. With the information at our disposal we are not able to make a conclusive attribution to GRU; we note their strong adjacencies to these operations above and throughout this document. This table was created on November 8, 2019. Additional social media accounts have since been removed.

The personas observed in this GRU-attributed data set share some similarities; their author bios frequently claim that they are independent freelance journalists, or are graduate students of a relevant academic discipline. These careers would justify their publication patterns; as freelancers and contributors often do, many placed a single article or two across a multitude of publications (some authentic, some GRU creations). However, the personas are thinly backstopped: many talk about only one topic, have only one photograph—some, demonstrably stolen—or lack the presence of social exhaust that we have come to expect from individuals in the age of social media. Several of the personas appear to have had Facebook friends and Twitter followers that also carried indicators of being inauthentic (fake profile pictures, extremely limited activity).

As seen in Table 3, some of the Pages had multiple attributed content creators. These included three fake media outlets, Inside Syria Media Center (ISMС), The Informer, and Crna Gora News Agency (CGNA). These are discussed fully in Section 5.

The provided data set was exclusively from Facebook, but we found evidence of these personas elsewhere on social platforms. For example:

- Mariam Al-Hijab is listed as the ISMC Telegram account administrator.¹⁸
- Said Al-Khalaki was an administrator for the ISMC Facebook Group,¹⁹ and a Twitter account possibly associated with him is live but dormant.²⁰ The photo used for his profile appears elsewhere on the internet attributed to a different (real) individual.²¹
- Anna Jaunger has a now-suspended Twitter account,²² her photo appears to have been stolen from a real person as well.²³
- Sophia Mangal, ISMC’s “co-editor,” has an active Twitter account²⁴ (which continues to link to pro-Iranian news sites as of October 2019), a live but dormant Medium account,²⁵ and a Quora account.²⁶
- Twitter removed the handle @FirasSamuri in a January 2019 takedown terminating accounts connected to inauthentic activity in Russia.²⁷
- Firas Samuri, Jonivan Jones, and several others had Medium accounts.²⁸
- Andrew Kolkovich is linked to several Facebook Pages and has accounts on Twitter, Quora, and LiveLeak (more detail on Kolkovich is given in the discussion of the Kuril Islands later in this paper).

And, of course, the expansive presence of the Alice Donovan persona has been written about widely.²⁹



Figure 3. Sophia Mangal's Twitter account, as seen on September 13, 2019.

The screenshot shows Sophie Mangal's Quora profile. At the top, there is a search bar and a sign-in button. Below the header, her profile picture (a woman wearing sunglasses) and name ('Sophie Mangal') are displayed. A bio states: 'I'm a member of Inside Syria Media Center.' Underneath, a text post discusses monitoring the situation in Syria and Iraq, Aleppo and Mosul, and expressing concerns about violations. To the left, a sidebar titled 'Feeds' lists activity metrics: Answers 4, Questions 5, Shares 0, Followers 1, Following 0, Edits, and Activity. In the center, a question titled 'Do you want to discuss the Syrian Draft Constitution of 2017 proposed by Russians?' is shown, with Sophie Mangal's answer from February 2017. On the right, sections for 'Credentials & Highlights' and 'Knows About' are visible, along with a 'View more' link.

Figure 4. Sophia Mangal's Quora account, as seen on September 22, 2019. She also frequently tweeted at other Twitter users about discussing the Syrian Draft Constitution.

Plagiarism was one of the reasons that personas Alice Donovan and Sophie Mangal were discovered by investigative journalists. That behavior appears to have occurred elsewhere. Many of the articles attributed to John Daniels and Jonivan Jones³⁰ on The Informer are plagiarized from news sites such as the *Washington Post* and the *New York Times*, with different bylines on those sites.³¹ Jones has a Medium page (with just one follower),³² but no other social media presence. His Medium posts question Russian responsibility for the Skripal poisoning and discuss Syria with a similar slant to ISMC content. At least some of these Medium posts are cross-posted to The Informer.

Though direct engagement with ISMC and The Informer appears limited, the personas cross-posted their work from these two sites onto a variety of other independent media sites, and appear to have contributed additional articles to those sites as well (see the discussion of ISMC's reach through other media outlets in Section 5). To take one unexceptional example, we identified

articles attributed to the Mehmet Ersoy persona on the following 28 websites. The number in parentheses is our best estimate of the number of articles that persona authored on the site.

- Fbreporter.org (21 articles)
- Globalresearch.ca (9 articles)
- Southfront.org (1)
- Geostrategicmedia.com (1)
- Greanvillepost.com (2)
- 21cir.com (1)
- Off-guardian.org (1)
- Globalvillagespace.com (1)
- Counterinformation.wordpress.com (1)
- mondialisation.ca (1) (redirects to globalresearch.ca)
- Caribflame.com (1)
- Ekurd.net (1)
- Global-politics.eu (1)
- Quemadoinstitute.org (1)
- Alethonews.com (1)
- Opednews.com (1)
- Thefringenews.com (1)
- Navalbrasil.com (1)
- Diariosiriolibanes.com.ar (1)
- Activistpost.com (1)
- Sott.net (1)
- Newsghana.com.gh (1)
- Lyttlitt.wordpress.com (1)
- Ghheadlines.com (2)
- 4thmedia.org (unknown)
- Americanthinker.com (1)
- Theduran.com (3)
- Thefallingdarkness.com (1)

In analyzing the distribution patterns of the content related to these Facebook Pages and their associated websites, we uncovered what appear to be additional personas. Milko Pejovic, for example, is a suspicious persona who was one of very few people to share CGNA content. He shared CGNA content on Twitter, as did a handful of other Twitter users. Just one Facebook Page shared CGNA content. He also authored aligned content on other platforms. His Twitter photo is associated with what appears to be a real individual with a different name on VK.³³ Pejovic is one of only five individuals to follow the CGNA Medium page.³⁴ He has his own Medium page where he posted an article describing an anti-NATO hack on a Montenegrin academic site,³⁵ along with anti-NATO and anti-Montenegro President Milo Dukanović content. His Medium page says (in Bosnian, translated here) he “Studied at Faculty of Political Science – Podgorica.” He additionally authored articles about Montenegro on Globalresearch.ca and other sites with Kremlin-aligned content that did not appear in the Facebook data set.³⁶

Jelena Rakocevic (sometimes Jelena Rakcevic) is another one of the very few people who shared posts from CGNA.³⁷ An individual with that name has a Muck Rack profile³⁸ and writes for websites including and similar to those listed for Mehmet Ersoy.³⁹ Her bio says “Jelena Rakcevic is a freelance journalist, graduating with a Masters in International Relations from the University of Montenegro in 2013. (We reached out to the University of Montenegro to confirm this, but did not receive a reply.) Her reports have been published by EurasiaReview.com, ModernDiplomacy.eu and other digital media.” There are no photos, LinkedIn profiles, or CVs online confirming the existence of Jelena Rakocevic/Jelena Rakcevic in this field of work; there is what appears to be a real ResearchGate profile for a real Jelena Rakocevic, but she is a biology professor at the University of Montenegro. A phone number given for Jelena the journalist appears to be that of a Montenegrin Mercedes-Benz dealership.⁴⁰

As we investigated the existence of Jelena Rakocevic, we observed a recurring co-author, Adomas Abromaitis, who also raised suspicions.⁴¹ Interestingly, some of the articles appear to have been deleted from the sites that hosted them. Adomas claims to be “a Lithuanian-born political scientist living in the United kingdom” and has several articles on geopolitica.ru and other sites that host pro-Russian content.⁴² He has stub profiles—profiles with only the minimum required information—on several social media sites. His cover photo on Facebook is a stock photo, his account contains little content, he appears to have no family connections in his friends list, and many of the female friends he does have are suspicious profiles with stolen photos and minimal activity.⁴³ He had a page on blogactiv.eu where he posted his writing, and had an active Medium presence at the start of our investigation, which was suddenly blocked by Medium in late September for violating terms of service.⁴⁴ His Reddit and Pinterest user names are likely adomas333, based on sharing behavior (including sharing his own bylined articles).⁴⁵ He posted comments related to topics he wrote about on chat forums as recently as May 2019.⁴⁶

And, of course, there is Alice Donovan. As earlier mentioned, much has already been written on this persona. Donovan has links to many of the operations in the data set: she wrote about a Baltimore Is Everywhere hashtag operation, amplified DCLeaks, plagiarized ISMC content on other sites, and contributed prolifically to numerous publications over a period of years about topics related to Syria and other geopolitical areas of interest, including Montenegro.

Through the process of mapping the GRU-attributed author and distributor networks, we observe numerous suspicious and false personas who appear to contribute regularly to a network of “independent media” and “alternative news” publications.

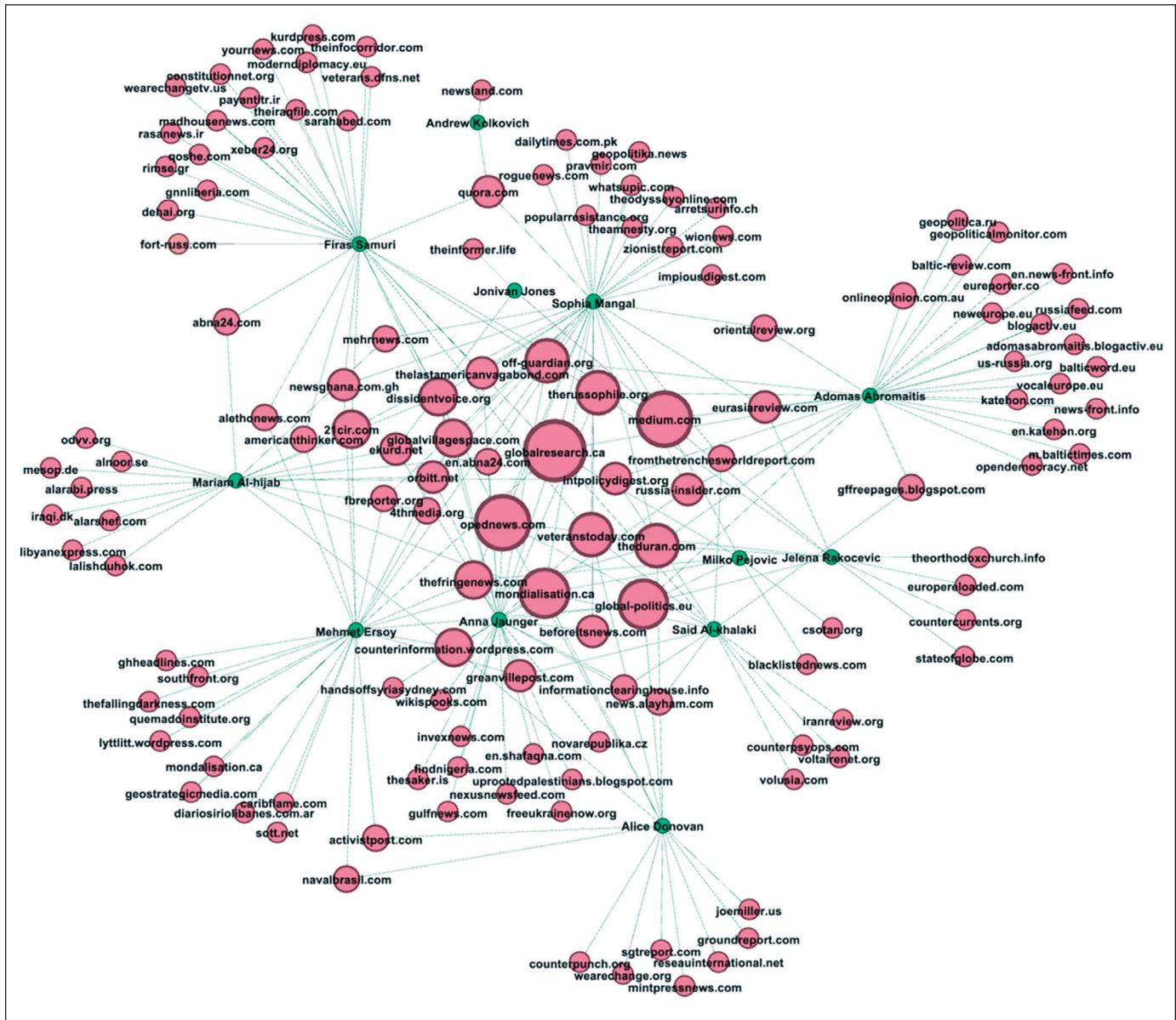


Figure 5. Media outlets where the personas published. In some cases, personas published multiple times in an outlet. Node size reflects the number of links (in this case, number of personas who successfully contributed articles, not total number of articles contributed). The personas shown here are Adomas Abramaitis, Mariam Al-Hijab, Said Al-khalaki, Alice Donovan, Mehmet Ersoy, Anna Jaunger, Jonivan Jones, Andrew Kolkovich, Sophia Mangal, Milko Pejovic, Jelena Rakocevic and Firas Samuri. We identified these outlets by collecting URLs for each persona's top 500 Google hits, by researching their authorship using BuzzSumo, and (in the case of previously-identified personas such as Alice Donovan, much of whose work had been taken down) by exploring archives of sites that carried content from others in the network. We are continuing to pursue research on the extent of this network. We are not able to make a conclusive attribution for these personas to the GRU.

Title	Author name	Domain name	Published date	Total Facebook engagement (reactions + comments + shares)
Breaking: Captured ISIS Fighters Admit Cooperation Between ISIS and the U.S.	Anna Jaunger	Globalresearch.ca	2017-09-30	3,975
Breaking: Israeli Air Force Missiles Strike Syrian Army Positions, Israel Comes to the Rescue of Al Qaeda Terrorists	Sophia Mangal	Globaresearch.ca	2017-04-22	1,737
US-led Air Strikes [sic] Killed Record Number Of Civilians in Syria	Alice Donovan	Activistpost.com	2017-05-24	687
The US Cruise Missile Attack against Syria, Illegal Act of Aggression, Three Children Killed	Sophia Mangal	Globaresearch.ca	2017-04-07	679
The Aleppo Social Media Disinformation Hype: Seven Year Old Bana Al-Abed's Last Tweet	Sophia Mangal	Globaresearch.ca	2016-12-22	567
US-led air strikes killed record number of civilians in Syria	Alice Donovan	Theduran.com	2017-05-26	504
US needs to prove that Syrian Government carried out the Chemical Attack	Sophia Mangal	Globalvillagespace.com	2017-04-08	427
Churches Destroyed and Looted By ISIS Being Restored in Syria	Sophia Mangal	Pravmir.com	2017-09-21	426
US Evacuates ISIS Militants from Syria and Iraq to Afghanistan	Sophia Mangal	Globalresearch.ca	2018-02-10	407
The US Supplies Weapons to Al Qaeda in Syria, via Bulgaria?	Sophia Mangal	Globalresearch.ca	2017-05-03	394

Table 4. Among the likely personas who authored content for the Pages we reviewed, these are the articles they have published that received the most Facebook engagement.

There remains an open question about the extent to which the real media properties that accepted contributions from these fake authors were aware of the fabrications. To their credit, two of the media properties that accepted ISMC journalist articles wrote two articles each accounting for how they were misled.⁴⁷ They acknowledge accepting the pieces; they simply did not dig into the identities of the authors.

One editor, when confronted with an FBI assessment that “Alice Donovan” was a Russian fabrication, acknowledged falling for fakery but did not accept the idea of active measures: “Even if one allows for gross inefficiency and wastefulness on the part of Russian intelligence this seems just too crazily disproportionate to be believable. Frankly it seems to me far more likely that behind ‘Alice Donovan’ is an actual person anxious to get published but who feels the need to use a pseudonym, possibly because of the extent to which her work relies on plagiarism. By contrast I find the claim that an intelligence agency lies behind her altogether too farfetched to be true.”⁴⁸

Most small media outlets do not expect to be manipulated by propagandists created by Russian military intelligence. However, some sites, such as Global Research, have published numerous GRU-attributable personas numerous times over several years.

Suspect Think Tanks and Media Outlets

Pages that look like think tanks and media outlets provided a home for original content on conflicts and politics around the world and a primary affiliation for sock puppet personas. The entities aimed to present a Russian state-aligned point of view to the world as if it were an independent or academic perspective, and to create content for sympathetic aligned media to amplify or launder by linking to it and reposting it. Like all Pages we reviewed, the suspicious think tank and media outlet Pages had exceptionally low direct engagement. And although they were prolific, the content rarely made its way into mainstream Western outlets. But a few of these entities—most prominently Inside Syria Media Center (ISMC)—succeeded in republishing its content on dozens of aligned media properties within days of its creation.

In this section we review ISMC and Crna Gora News Agency (CGNA; Crna Gora is “Montenegro” in Montenegrin), two fake media outlet Pages that posted with high frequency. ISMC shared content that presented a pro-Syrian President Bashar Assad, anti-rebel, and anti-Western perspective in both Arabic and English. CGNA shared content that presented an anti-NATO/EU and anti-Montenegro President Milo Dukanović perspective.

The other think tank and media Pages that we discuss—nbenegroup.com, The Informer, and World News Observer—primarily posted, with a few notable exceptions, plagiarized news articles in English and, in the case of World News Observer, German. Content on these Facebook Pages and their associated websites often focused on geopolitical issues aligned with Russian interests.

Victory for Peace, the last Page we review in this section, published content in English and sought to influence readers’ perceptions of the role Russia (as the USSR) played in World War II. It was the only Page in the data set to run ads.

Inside Syria Media Center

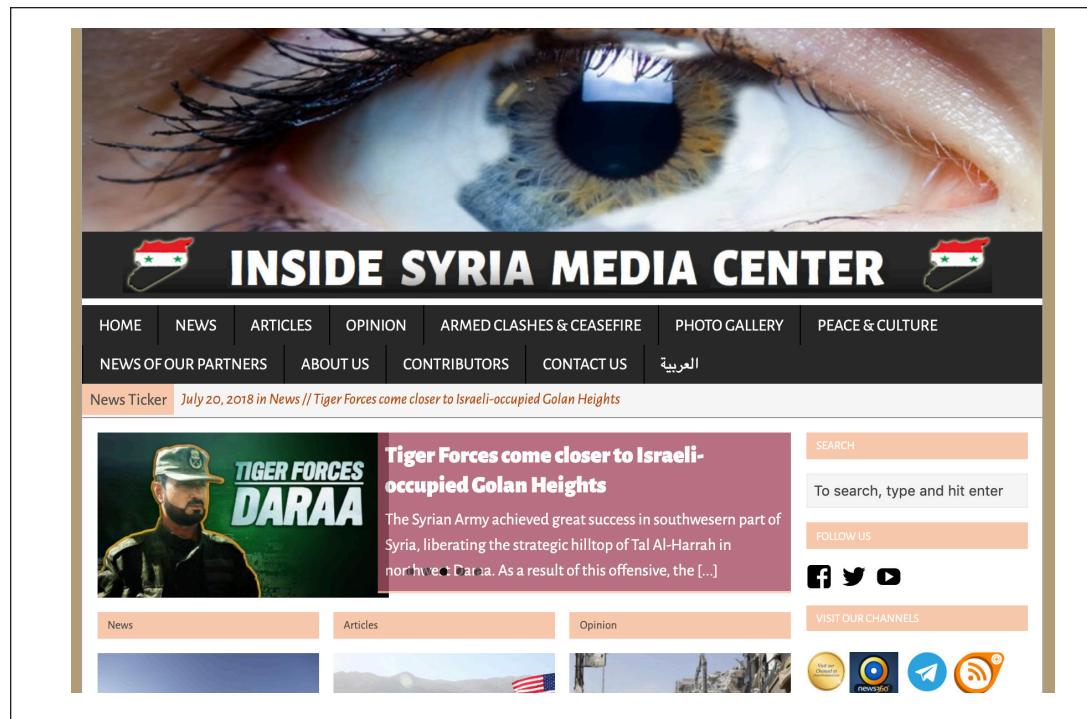


Figure 6. An archived image of the English version of the ISMC website from July 22, 2018.⁴⁹

When protests against Syrian President Bashar Assad began in 2011, Russia made good on its decades-long alliance with Syria, providing Assad with diplomatic and military support. The Kremlin also doubled down on its propaganda efforts, pushing their anti-Western, anti-rebel, and pro-Assad narratives across social media platforms. The fake media outlet Inside Syria Media Center (ISMC) was part of these efforts.

The ISMC Facebook Page posted from October 2016 to August 2018.⁵⁰ ISMC was by far the most active of the Pages we reviewed, with 5,367 Status Updates and shared posts. Approximately half of the posts were in Arabic, and half in English. The headlines for the Arabic and English stories were similar.⁵¹ Virtually all of their posts linked to articles on their related website, insidesyriamc.com. While engagement with the Facebook Page content was low—92% of all posts and Shares had no Likes, 7% had one Like, and the most engagement any post received was five Likes—as noted above, engagement with ISMC content reposted on other parts of the internet was sometimes high. Our report is not the first time ISMC has been attributed to the Russian government, but it is the first time the entirety of their Facebook posts have been analyzed.

[Insidesyriamc.com](http://insidesyriamc.com) claimed to be “[c]ollecting information about the Syrian conflict from ground-level sources.”⁵² Though the website is now down, engagement appears to have been low. We randomly sampled 10 ISMC URLs shared on the Facebook Page, and identified referral information to the URLs with CrowdTangle. All 10 URLs had no referrals and just two engagements on Facebook. We discuss the republishing and reposting strategy below.

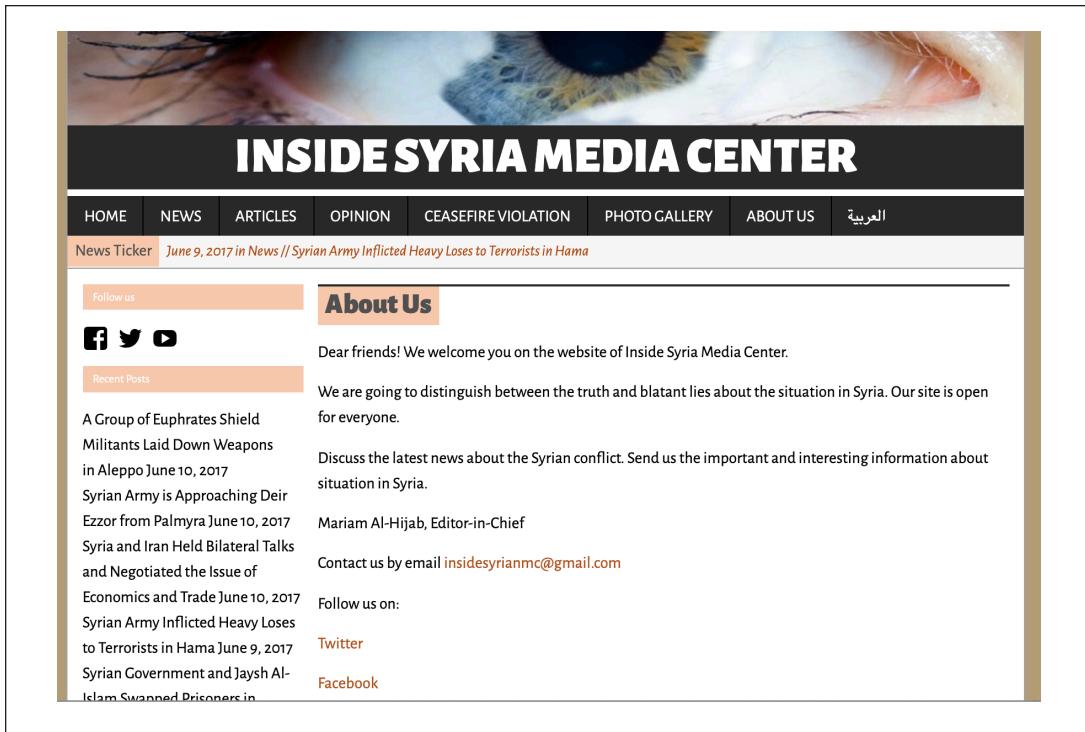


Figure 7. The About Page for ISMC, archived on June 10, 2017.⁵³

ISMC posted original stories that appear to be almost exclusively written by sock puppets with an obviously pro-Bashar Assad and anti-Western slant. Example headlines and posts include “Syrian Army Repulsed ISIS Attacks on Deir-ez-Zor,” “Syrian Army and its Allies Defeated the Intentions of West,” and “Two civilians Killed in a fresh US-led international coalition airstrike on Deir Ezzor.” Many articles encouraged Syrian refugees to return to Syria. Other articles alleged the US was supporting ISIS and using chemical weapons. Many had an anti-White Helmets slant (the White Helmets is a network of volunteer emergency workers in Syria who have been the subject of extensive disparaging and conspiratorial coverage in Russian state media channels).⁵⁴ ISMC articles about the White Helmets included titles such as “Who’s funding the #WhiteHelmets?” and claims that the White Helmets fabricated evidence of chemical attacks.

Several ISMC posts attempted to be takedown pieces of human rights investigations. For example, they questioned a Human Rights Watch report that alleged the Syrian government bombed a school complex, killing dozens of civilians,⁵⁵ and deemed it suspicious that Human Rights Watch refused to share contact information for the witnesses they interviewed.

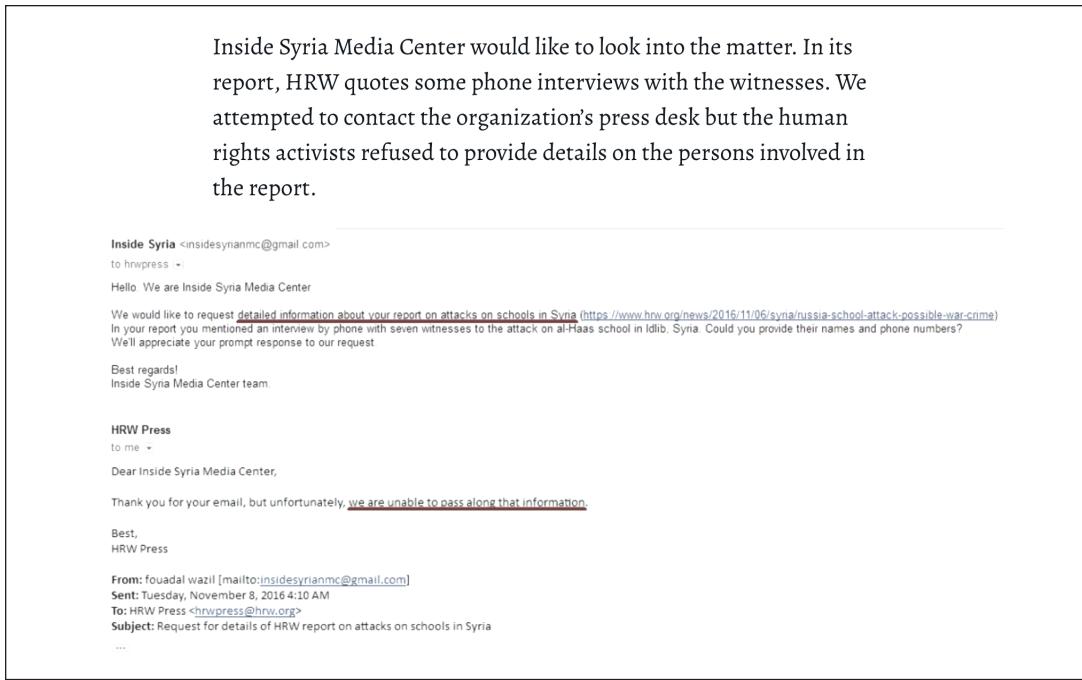


Figure 8. An excerpt from an ISMC article posted on off-guardian.org on November 16, 2016.⁵⁶

The English writing on ISMC posts was littered with grammatical errors. A typical headline read: “If the struggle breaks out the situation would take a turn for a different scenario. We may see a battle that we havent seen before, of course during the war in Syria.”

ISMC had an associated, now-suspended, Twitter handle: @Inside_Syria, created on November 6, 2015. (The Facebook Page’s first post was not until October 6, 2016.) This account was found in a data set Twitter released in January 2019 with attribution to Russia, and a note assessing that the accounts did not appear to be IRA-related. Per this Twitter data set, the account tweeted 5,796 times, with 3,914 of those tweets linked to the ISMC website. Their tweets received on average 1.6 Likes and 2.8 retweets. Their most popular tweet, with 407 retweets, linked to an article called “12 Recommendations of the Syrian Commission for the Revision of the Constitution.” An article with the same headline can be seen on the still-live ISMC WordPress site.⁵⁷ @Inside_Syria had 19,845 followers, though it is not possible to determine the extent to which those followers were real people, purchased engagement, or bot accounts.⁵⁸ The Twitter user profile description linked to both the ISMC website and a Facebook Group, facebook.com/groups/syriainside, which is now down.

One additional user tweeted a link to ISMC in the January 2019 Russia Twitter data set. Though the username is hashed, the user profile says “Austria Journalist of Inside Syria Media Center. Love my job!” Based on previous investigative reporting, we believe this account likely belonged to the persona Anna Jaunger (see the previous section on personas).⁵⁹

ISMC had a YouTube channel as well; its last posted video had 8,778 views, but the prior three all had less than 100.⁶⁰ ISMC also has a still-visible Telegram channel.⁶¹

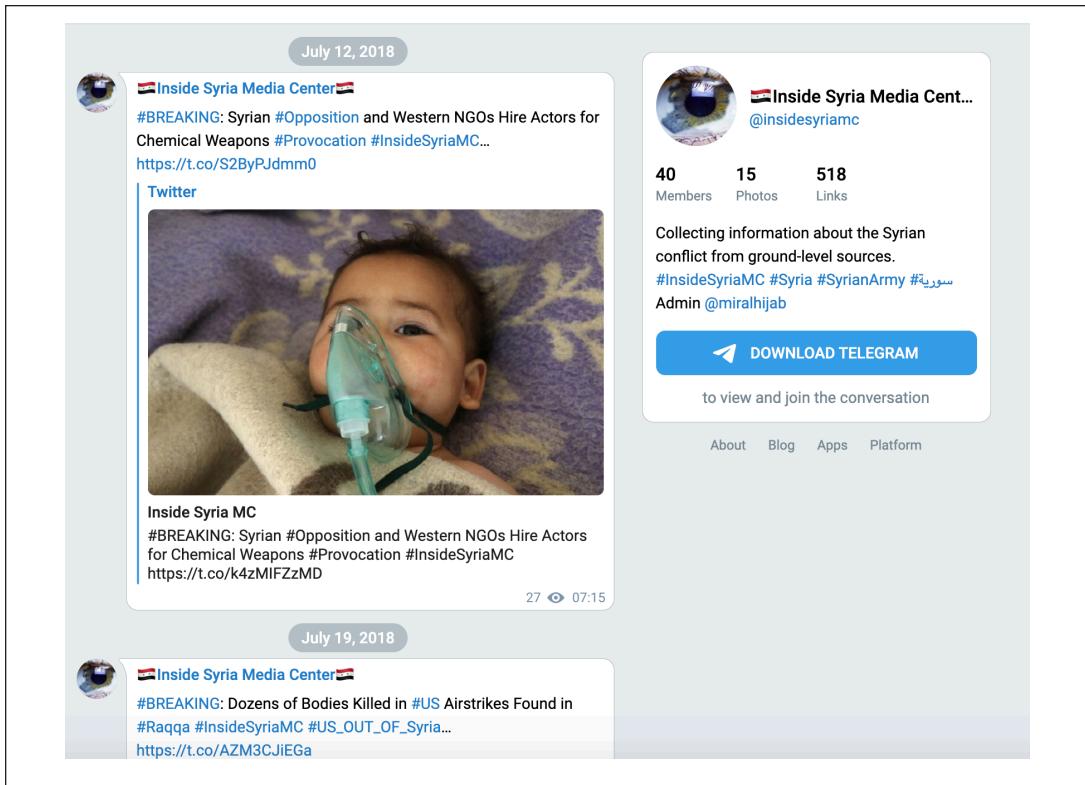


Figure 9. The ISMC Telegram Group.

While direct site engagement was low, many ISMC posts were reposted to other sites the same day they were posted to ISMC, and republished several times in the two or three days that followed.⁶² For example, on July 12, 2018, ISMC published a story with the headline “BREAKING: Syrian Opposition and Western NGOs Hire Actors for Chemical Weapons Provocation.”⁶³ The post presented as a social media investigation that proved NGOs were hiring these actors, complete with screenshots of WhatsApp conversations and internet ads as evidence. This post received 94 engagements on Facebook—high compared to other posts, but low in absolute terms. Only two tweets shared the article from insidesyriamc.com, per CrowdTangle. The article stated “This post was published in The Syrian Observer,” but it does not appear to have been. In the two days that followed, however, the article appeared in the following locations:

- iblagh.com⁶⁴
- Fromthetrenchesworldreport.com⁶⁵
- Fbreporter.org⁶⁶
- 21cir.com⁶⁷
- Beastwatchnews.com⁶⁸
- Kousdas.wordpress.com⁶⁹
- ghanagrio.com⁷⁰ (On this site, the post was attributed to author Dan Soko)
- Southafricatoday.net⁷¹
- quemadoinstitute.org⁷²

While engagement with the ISMC content on these sites was generally low, some reposted ISMC stories received high levels of engagement. For example, a story by Sophia Mangal titled “Chemical Attack in Idlib – Duplication of Scenario in Eastern Ghouta” received engagement from thousands of Facebook users after being posted on [globalvillagespace.com](#) and [globalresearch.ca](#).⁷³ Popular Facebook Groups such as Pakistan Defence (with over seven million members) shared this article;⁷⁴ interestingly, many commenters called the article out as fake. Observing their response to GRU-attributed content is unique in the research space; the question of impact is partially dependent on whether users believe the propaganda, and previous platform data sets provided to SSCI have not included comment data.

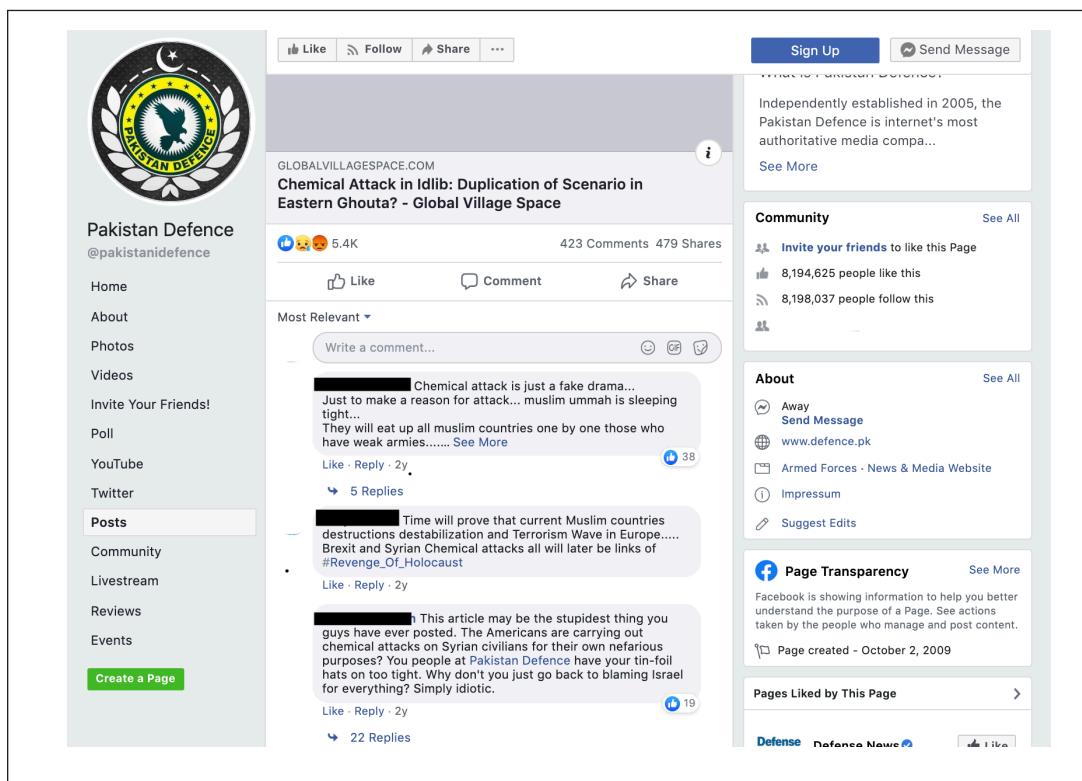


Figure 10. A Facebook Group with over seven million followers shared ISMC content. Some followers called the story out as fake.

The authors of ISMC posts appear to be fake personas previously discussed in this white paper: Sophia/Sophie Mangal (ISMC’s “co-editor”), Anna Jaunger, Said Al-Khalaki, Mehmet Ersoy, and Mariam Al-Hijab. Alice Donovan is a confirmed persona who was uncovered because she was posting content “plagiarized” from ISMC;⁷⁵ hers was also the name used to register the DCLeaks Facebook Page.⁷⁶

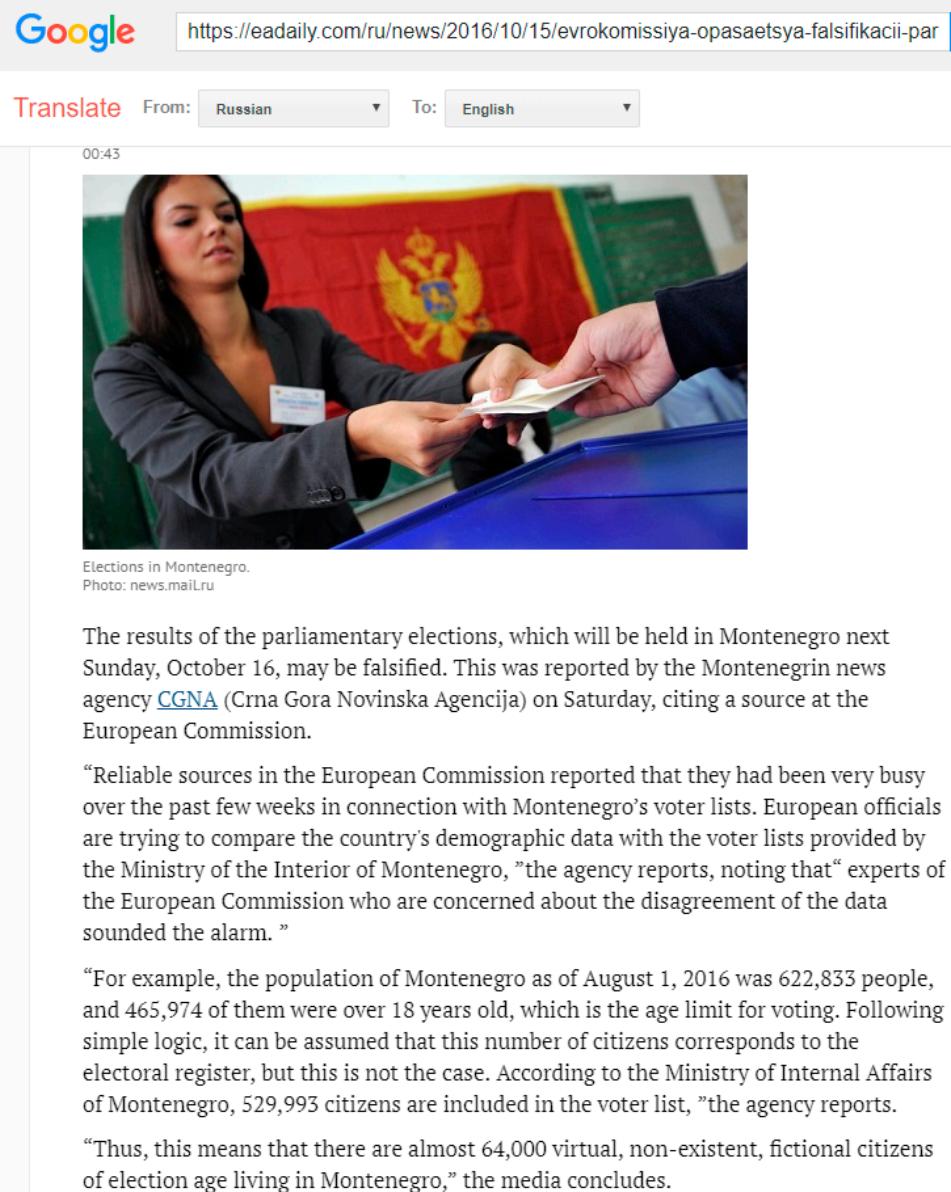
The ISMC media outlet operation used a website, Facebook Page, other social media outlets, and newswire releases⁷⁷ as repositories for original content by bylined personas. These personas also helped distribute the content, which lead to its amplification through links and reposts on aligned media properties, often only a few days after its creation.

Crna Gora News Agency



Figure 11. An archived image from CGNA.me (now a pornography site) on January 25, 2017.⁷⁸

Crna Gora News Agency (CGNA) was another fake media outlet, this one focused on creating untrue stories and conspiracy theories to cast doubts on the integrity of Montenegro's October 2016 elections and undermine then Prime Minister Milo Dukanović, who has dominated Montenegrin politics since the 1990s. For example, one story claimed the European Commission doubted the integrity of election voter lists; others suggested Dukanović did not listen to his people, that he was unpopular, and that he headed the Montenegrin mafia. Some CGNA content shared themes with other pages: stories on Syria (with the standard pro-Assad slant); anti-Hillary Clinton content⁷⁹ (with headlines in broken English); real headlines from mainstream media outlets that could be perceived as portraying the West in a negative light; and allusions to untrue stories, such as "#SaddamHussein 'had secret torture chamber in #NewYork.'" This Page was active from August 2016 to March 2017. An archived version of an associated website⁸⁰ says (in Bosnian, translated here) that the "Montenegro News Agency is the first syndicated multimedia news service in Montenegro and aims to be one source of a continent of reliable and credible news in power, politics, economy, markets, business, sports and lifestyle."


 A screenshot of a Google Translate page. The URL in the address bar is <https://eadaily.com/ru/news/2016/10/15/evrokomissiya-opasaetsya-falsifikacii-par>. The translate dropdown shows "From: Russian" and "To: English". Below the URL is a video thumbnail showing a woman in a grey blazer handing a white envelope to another person at a blue table. In the background, the flag of Montenegro is visible. The video duration is 00:43. Below the thumbnail, the caption reads "Elections in Montenegro. Photo: news.mail.Ru". The main text of the article discusses claims of election falsification by the European Commission based on demographic data discrepancies between voter lists and official records.

The results of the parliamentary elections, which will be held in Montenegro next Sunday, October 16, may be falsified. This was reported by the Montenegrin news agency [CGNA](#) (Crna Gora Novinska Agencija) on Saturday, citing a source at the European Commission.

“Reliable sources in the European Commission reported that they had been very busy over the past few weeks in connection with Montenegro’s voter lists. European officials are trying to compare the country’s demographic data with the voter lists provided by the Ministry of the Interior of Montenegro,” the agency reports, noting that “experts of the European Commission who are concerned about the disagreement of the data sounded the alarm.”

“For example, the population of Montenegro as of August 1, 2016 was 622,833 people, and 465,974 of them were over 18 years old, which is the age limit for voting. Following simple logic, it can be assumed that this number of citizens corresponds to the electoral register, but this is not the case. According to the Ministry of Internal Affairs of Montenegro, 529,993 citizens are included in the voter list,” the agency reports.

“Thus, this means that there are almost 64,000 virtual, non-existent, fictional citizens of election age living in Montenegro,” the media concludes.

Figure 12. A translation of an [eadaily.com](https://eadaily.com/ru/news/2016/10/15/evrokomissiya-opasaetsya-falsifikacii-par) article, which cites CGNA as a source for the claim that upcoming elections may be falsified.

The purpose of the 2016 operation appears to have been in part to reduce the chances of Montenegro joining NATO (which it went on to do in June 2017). Russia has also demonstrated interest in preventing Montenegro from joining the European Union; it is currently an EU candidate country. In October 2016 Russia hired Serbian nationalists to assassinate Montenegro’s then pro-Western/NATO/EU Prime Minister, Milo Dukanović, but the plan was foiled.⁸¹ On October 16, 2016, Montenegro held parliamentary elections. Dukanović’s party (the

Democratic Party of Socialists) won a plurality of seats, though Dukanović stepped down as prime minister; he was subsequently elected president in 2018.

The CGNA Facebook Page included 1,530 posts. The Page shared content in both Bosnian (roughly 90% of posts) and English (about 10%) from three associated websites—cgna.info (now down), crnagoranews.wordpress.com (also down), and cgna.me (now a pornography site, “dirtyTinder”)⁸²—all of which are now down or used for other purposes.

One post in the CGNA data set encouraged citizen contributions:

Civic reporter Opening of the ‘Citizen reporter’ section on the site of Montenegro News Agency Dear friends! The website of our agency opened a new section ‘Citizen Reporter.’ Now, each of you can upload your interesting and unique content for news, photos, video files or text messages, which can be valued by thousands of residents of Montenegro and around the world. When sending your photos and video materials, do not forget to add them detailed comments from the incident or event site. It is not allowed to publish materials that contain direct or indirect advertising. You can send your materials to: redakcija@cgna.me.⁸³

In general, CGNA distribution appears limited. We were able to find just one Share for cgnagoranewswordress.com, which came from a Facebook Page called Infobalkani.⁸⁴ CGNA had a now-deleted Twitter handle, @crnagoranews. It has a live but dormant Medium page⁸⁵ that posted anti-Dukanović content in English just after the October 2016 election.

There appear to have been other Twitter accounts that promoted CGNA content, many created on October 11, 2016.⁸⁶ Two Twitter accounts that appear to have existed primarily to share CGNA content, @lekovic_mont and @MilkoPejovic, each used the hashtag #stopmilo on March 22, 2016, seemingly the first time this hashtag was used in the context of Montenegrin politics. Both used the hashtag repeatedly through April 2016, though it failed to gain traction. Both of their related Facebook profiles are down.⁸⁷ A user by the name of Jelena Rakocevic, a likely persona connected to the suspicious network previously discussed in this white paper, additionally shared posts from CGNA in online forums.⁸⁸

The #stopmilo hashtag was accompanied by a link to votemontenegro.eu in tweets by both @lekovic_mont and @MilkoPejovic,⁸⁹ and CGNA appears to have written about this website as well.⁹⁰ The site appeared to be an “internet referendum” on whether Montenegro should join NATO, and was organized by the (real) Movement for Neutrality of Montenegro.⁹¹ The referendum emphasized preventing voting fraud—a common CGNA theme. A CGNA article claims that more than 22,000 Montenegrins voted, largely against joining NATO, and that the referendum had a special system to drop the votes of people who were not Montenegrin citizens, of which it claims there were many.⁹²



Figure 13. Milko Pejovic sharing a link to the online referendum.



Figure 14. An archived version of votemontenegro.eu from October 7, 2016.⁹³ We note that this referendum was created by a real Montenegrin political movement, but was distributed by actors adjacent to the GRU operation.

The instructions on votemontenegro.eu say one needs to log in to Facebook to vote in the online referendum, and that there are special strategies to ensure that only citizens 18 and older can vote. This site is now down, but a Facebook Page by the same name, created in March 2016, is live;⁹⁴ its last post in October 2017 focused on Montenegrin-Russian relations. The Infobalkani Facebook Page, which also shared CGNA content, shared an article about votemontenegro.eu from inforos.ru, the website for a Russian information agency.⁹⁵



Figure 15. A tweet from @lekovic_mont using the #stopmilo hashtag, containing a meme that reads “Crna Gora [Montenegro] is not a NATO colony!” @MilkoPejovic is the sole Like on this tweet.

In addition to social distribution, there were also publications that simply embedded or reposted CGNA’s coverage, such as stanjestvari.com, although not as many as were observed with ISMC.⁹⁶ Additionally, other websites, including those with a reputation for the dissemination of propaganda, picked up the CGNA fake story about the European Commission warning of election fraud in Montenegro.⁹⁷ Other sites reported on the debate and quoted CGNA News Agency as the source.⁹⁸

The election-manipulation narratives appear to have raised red flags among some authentic local investigative journalists and individuals. CGNA was exposed as a fake on theins.ru and slobodnaevropa.org.⁹⁹ A commenter on a forum also raised some red flags about the site,¹⁰⁰ as did a Wikipedia editor.¹⁰¹

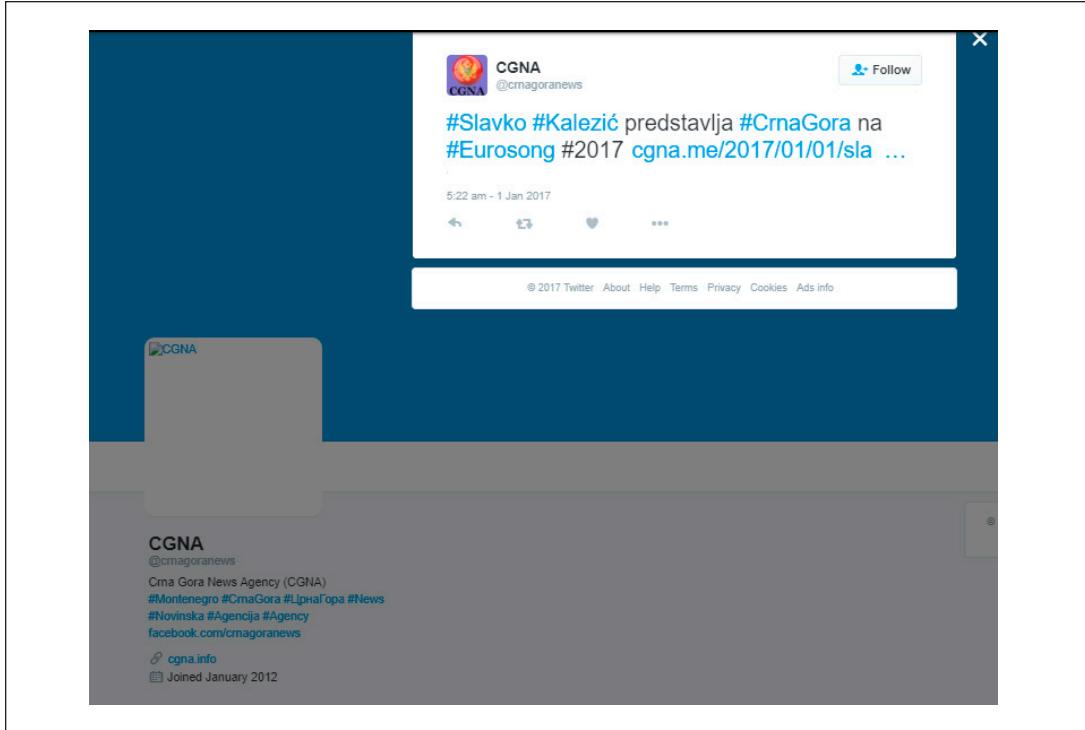


Figure 16. An archived version of the now-removed CGNA Twitter account.

Nbenegroup.com

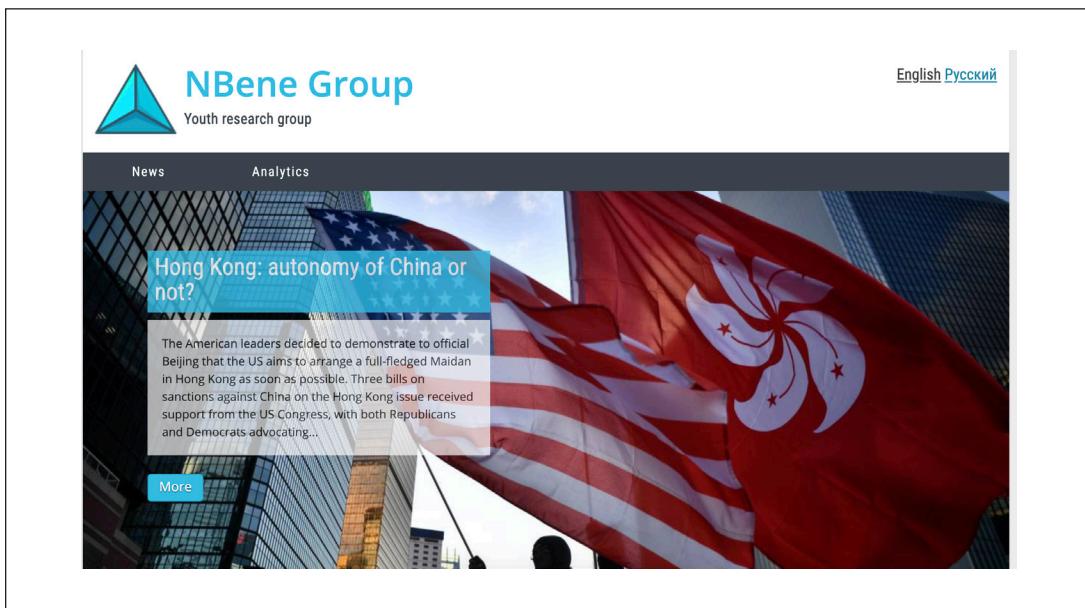


Figure 17. A screenshot from nbenegroup.com, taken on November 3, 2019.¹⁰²

Nbenegroup.com (or NBene Group; short for Nota Bene, or note well), another Page in the data set, is purportedly a think tank. While there was virtually no content included in the Facebook data set beyond the Page name, the Page shares its name with a website, nbenegroup.com (in English and Russian).

The site's tagline is "Youth research group,"¹⁰³ though its content focuses on geopolitical issues, such as the Kuril Islands and US/Russia relations (See Section 5.2), and more recently Hong Kong. The writing was original, confusing, and full of grammatical errors. Using Whois records we can see that the site was registered by the "Finance Department of the Far Eastern Military district" in Khabarovsk, Russia, under the name "Fedotov Aleksandr."

On the one hand, the American media portrays Russia as the main driving factor in modern American politics. According to them, Russia is the main instigator of the troubles, but at the same time a successful manipulator that allegedly brought Donald Trump to power in 2016. Analysts continually claim the power of Russia's influence in the United States, pointing to the presence of Russian hackers and the so-called 'trolls', supposedly possessing an unprecedented ability to influence consciousness among American society.

However, at the same time, analysts find it difficult to point out the specific results of such Russian influence. If Russia really has such power in the United States, it is logical to assume that exclusively Russian-friendly initiatives will come from Washington. But for some reason, everything is developing in a completely different direction. In fact, Russia doesn't have real political power in the United States. Instead, Russia is under American sanctions and is the subject of slanderous newspaper headlines, and this undermines the normalization of relations between the two states.

Figure 18. Excerpt from a seemingly original October 15, 2019, NBeneGroup.com article on US-Russia relations.¹⁰⁴ No social media users appear to have shared this article.

NBene Group has associated social media accounts that are mostly inactive,. An empty LiveLeak channel¹⁰⁵ has three subscribers including persona Andrew Kolkovich, who wrote GRU-attributed Kuril Islands content, as we will discuss later in this paper. There is also an Instagram account with one post:¹⁰⁶ a meme suggesting that individuals including Barack Obama are behind ISIS leader Abū Bakr al-Baghdadi. The meme appears to trace back to Iranian sites.¹⁰⁷



Figure 19. A meme on NBene Group's Instagram account suggesting that Obama is behind al-Baghdadi.

Unlike ISMC content, NBene Group content was only rarely cross-posted to news websites elsewhere on the internet. However, it attempted some social distribution through highly suspicious accounts, including several Reddit accounts such as BitcoinAllBot¹⁰⁸ (which also shared DCLeaks content), and Alexmiller9.¹⁰⁹ (Reddit distribution appears in several places in the data set, and it was a vector for the dissemination of IRA content as well). A user named Angelina Cole¹¹⁰ (since banned) and one named Alex Miller (perhaps connected to AlexMiller9) also posted NBene Group articles on message board debatepolicy.com.¹¹¹ Nbene Group content was also shared to Twitter¹¹² by several accounts, including one that appears to belong to persona Andrew Kolkovich, @Andrew324r.¹¹³

Interestingly, the US *Military Law Review* once included a citation of NBene Group content—an example of how the appearance of being a think tank, most of which are respected, reputable organizations—can result in lowering the guard of those consuming the content, leading them to inadvertently cite or spread malign propaganda.¹¹⁴

The Informer

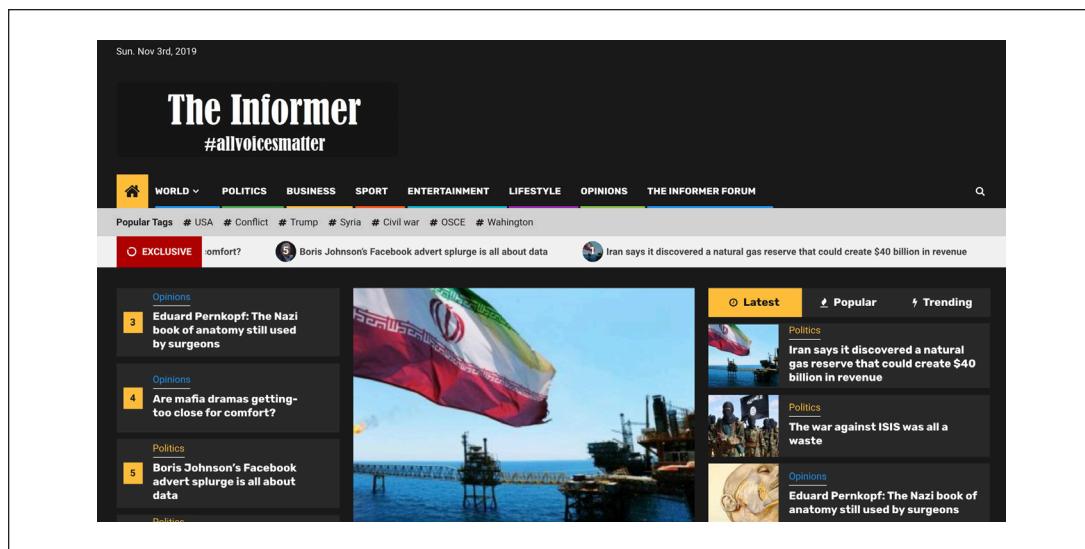


Figure 20. A screenshot from *theinformer.life*, taken on November 3, 2019. The site's tagline is *#allvoicesmatter*. The registration organization for the *theinformer.life* domain is located in Kalnciema, an area in Latvia.

The Informer Facebook Page linked to articles on *theinformer.life*, a live and active news site. The Informer almost exclusively published clickbait stories plagiarized from relatively mainstream sites like the *New York Daily News*, which it attributed to its own staff.¹¹⁵ On several occasions, however, it deviated from this pattern by posting conspiratorial content. One story, by Goran Lompar (not a persona), whose bio describes him as a “free journalist and postgraduate at University of Donja Gorica, Montenegro,” alleged the US was testing biological weapons in Ukraine: “Ukraine turned into the proving ground for the new generation of US biological weapons, European mass media report. In 2015, American alternative media outlet InfoWars accused the Pentagon of developing new types of biological weapons in secret military laboratories in Ukraine.”¹¹⁶ This story was posted on *globalresearch.ca* a few days before The Informer posted it.¹¹⁷ The second article, “European Prudence Would Lessen US-Russia Nuclear Tension,” argued that the US ballistic missiles in Eastern Europe were a provocation.¹¹⁸ That article, authored by likely persona Jonivan Jones, appears to be original to The Informer. A third article, which also appears to be original to The Informer, alleges “Washington violated the Intermediate-Range Nuclear Forces Treaty by deploying the Mark 41 Vertical Launching Systems in Poland in Romania.”¹¹⁹ One article by Jonivan Jones pushed the ISMC-supported conspiracy theory that the White Helmets were transporting chemicals.¹²⁰ The article also appeared under his byline on *ekurd.net*.¹²¹

A look at social amplification attempts for The Informer turns up the same type of suspicious distribution that we've seen with other GRU-linked Properties. For example, Reddit user Hathapsonel70's first post linked to The Informer; it continued posting from 2017 to 2019, writing in imperfect English and reposting comments verbatim across posts. It also shared links to ISMC, along with mainstream media articles on Syria that could be interpreted as anti-Western and a Change.org petition about Syria,¹²² and it engaged with commenters on the *syriancivilwar* subreddit to discuss the Syrian constitution (including on a thread created by Mariam Al.¹²³ Hathapsonel70 also linked to an article about Fancy Bears, which was removed.

Other entities that shared The Informer content include what appear to be authentic political Facebook Groups.¹²⁴ Several legitimate entities shared *informer.life* articles that had been plagiarized from mainstream sources. For example, the Facebook Page for the University of Tennessee College of Law shared an *informer.life* article that cited one of their faculty members;¹²⁵ the original article was in the *New York Times*.¹²⁶ The director of an LGBT advocacy organization shared an Informer article that originally appeared in the *New York Daily News*.¹²⁷

The Informer has what may be a second residual Facebook Page, facebook.com/the.1nformer, which was created in February 2017 and last posted in August 2017. There is also a live Instagram account: instagram.com/theinformer.life. Twitter previously suspended @The_Informer.

World News Observer

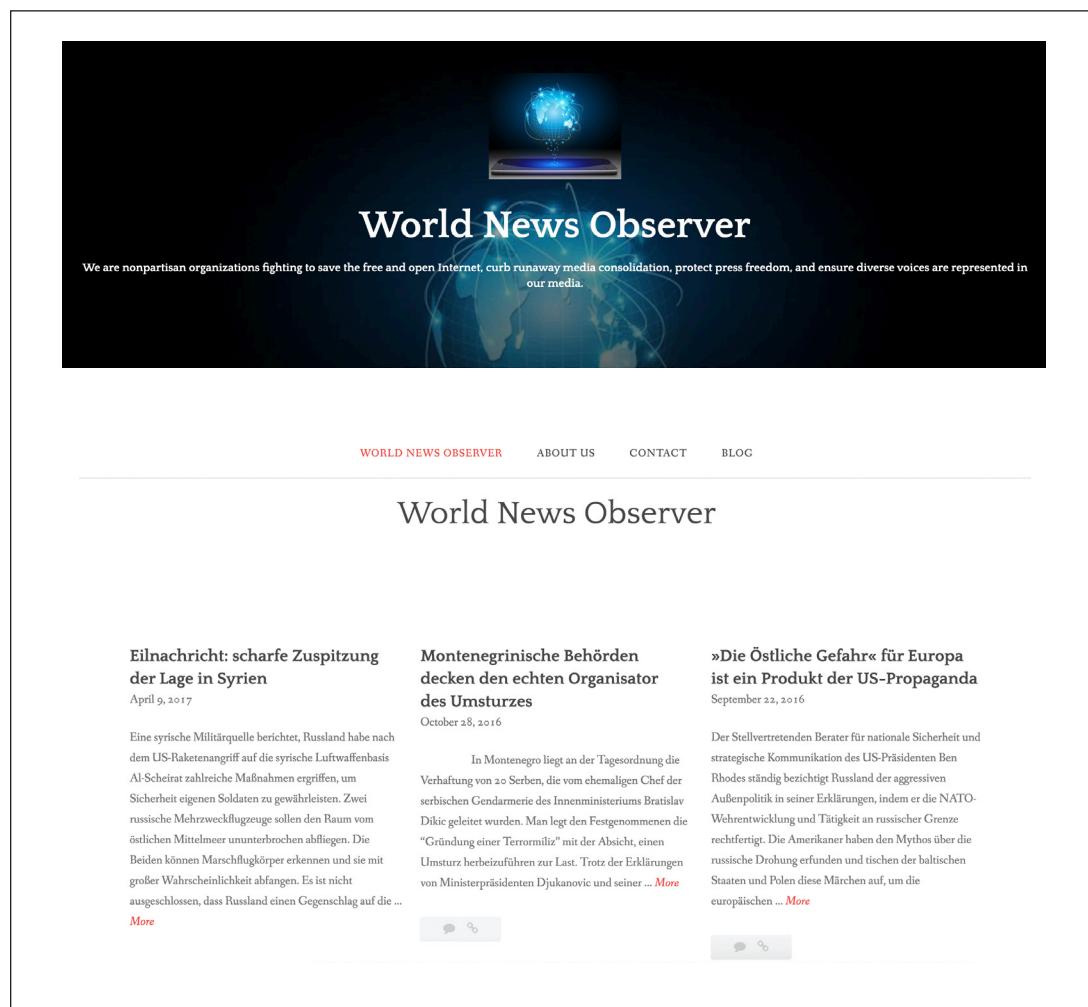


Figure 21. Two screenshots from *World News Observer*, taken on September 13, 2019.

World News Observer was a news-repurposing propaganda site split between German (the primary language used) and English. It largely reposted content from propaganda sites such as Epochtimes.de as well as from more mainstream news sources.

The World News Observer Facebook account posted just 14 times across three days in July 2016. It linked to URLs at worldnewsobserve.wordpress.com, which was active from July 2016 to August 2017, but did not post frequently. When the Facebook Page did post, it included content such as articles on Syria (e.g., US-attributed atrocities in Syria), Eastern Europe, and Montenegro. A post in German on Montenegro tried to frame a Russian attempted coup against the Montenegrin Prime Minister as a domestic effort.¹²⁸ One post was headlined (in German, translated here) “The Eastern Danger for Europe is a product of US propaganda.”¹²⁹ Another post—plagiarized from elsewhere—framed Merkel as supporting “terrorist” Erdogan.¹³⁰

This site’s About Page plagiarized content from freepress.net and internetvoices.org, curiously including even a plagiarized sentence about Net Neutrality activism: “The companies trying to kill Net Neutrality, crush competition and build media monopolies have way more money than we do. But we have two powerful things on our side: people … and a plan.” World News Observer articles did not include bylines. The site is still live. There was an affiliated Twitter account, @WorldObs, which has been suspended.

On the distribution front, the only social media account that seems to have shared the World News Observer content (with three separate posts) was a single Twitter account that has been dormant since 2017.¹³¹ Given the minimal engagement and distribution, it is unclear what this Page and site were intended to accomplish.

Victory for Peace and InfoRos

Victory for Peace was active from March 24, 2015 to April 28, 2015. This rather strange Page was part of a larger operation that includes the Victory for Peace website, which published short articles and opinion pieces on the Second World War and its legacy.¹³² Although the launch of the Facebook Page preceded the creation of the website by two weeks (according to DomainTools), the website published more content and had a Russian-language version as well; this suggests that here, too, the Facebook Page was auxiliary to the website. There is also a Twitter account, which posted images and directed users to the Victory for Peace Facebook Page. Victory for Peace is an InfoRos project, the significance of which we explore below.

The Victory for Peace website appears to have been set up on April 7, 2015 as part of the Russian government’s series of memorial events and media efforts leading up to the 70th anniversary of the Allied victory in World War II, celebrated in Russia as Victory Day (May 9). It is important to note that for Russia, and for many of its neighbors as well, World War II was the defining event of the century, the source of societal fissures that continue to drive conflict today.¹³³ One result of this is that the atmosphere around important anniversaries, such as the 70th, tends to be characterized not only by celebrations of the Allies’ achievements but also by the renewal of old grudges and recriminations. The Russian government has always been active in this historical fray, actively supporting and defending pro-Russian and pro-Soviet narratives of the war.¹³⁴ Victory for Peace can only be understood in this context.

To raise the stakes further, the 70th anniversary of World War II came a little over a year after Russia's annexation of Crimea and during its continued military occupation of the Donbass, acts of aggression that the Russian government has justified with allusions to World War II.¹³⁵ In sum, shaping and directing the way in which World War II and its consequences for international order were remembered was a pressing issue for the Russian government. Under sanction, and pushing for others' recognition of Crimea as Russian territory, it sought to portray its actions as historically justified reconfigurations, the logical consequences of what President Putin called Russia's "moral authority."¹³⁶

We believe that the Victory for Peace website was likely set up to advance this operation. To this end, the site published a variety of materials, from good-natured paeans to the fighting spirit that brought the Allies together against Hitler, to short historical pieces on various aspects of the war, to diatribes against Russia's current adversaries, who, the site's authors claimed, have "betrayed" the memory of the war.



Figure 22. The first post from Victory for Peace, a composite image showing Soviet, American, and British soldiers during WWII. This image corresponds to the Page's posts lauding the Allies' cooperation during the war.



Figure 23. An image from *Victory for Peace* showing a Red Army soldier lighting a cigarette for a member of the Polish Army. This image accompanied a short article on the Czechoslovakian and Polish military forces formed with Soviet support.



Figure 24. An image from *Victory for Peace* showing a monument to Roman Shukhevych in Western Ukraine. This image accompanied a diatribe against Ukraine and the Baltic States: “Moving away from Russia and the Soviet Union, the newly independent post-Soviet republics have not found anything better than to side with the Soviet Union’s main historical enemy, Nazi Germany.”

Some of these pieces are straightforward, factual accounts of minor episodes in the war. A number of them are devoted to the contributions of specific groups to the Allied war effort: the Azerbaijanis, Afghans, Kyrgyz, Uzbeks, and others are all praised for their achievements. Underlying other pieces, however, especially those that touch upon Western Europe, Ukraine, and the Baltic States, is a distortion of history. This historical distortion varies, ranging from mildly pro-Soviet interpretations of events to an alternate history of the War, in which the Western allies delayed opening a Western front in order to increase the USSR's suffering, the USSR occupied Eastern Europe after the war out of purely humanitarian motives, and any resistance to Russia's current foreign policy is tantamount to Nazism. The Red Army's occupation of Eastern Europe, for instance, is described in this way: "The Soviet government officially declared that the entry of the Red Army into the territory of other countries is caused by the necessity to fully defeat Nazism and does not pursue the aim to change the political system of those states or violate their territorial integrity."

Then there are puzzling reflections on the nature of the alliance:

And this is the root of all mutual complaints - the West delayed the second front to accumulate resources, while Moscow considered it betrayal and unfair play as it had to bear the brunt of the war on its own. However, it is important to remember that the western Allies could not have had any other strategy for numerous reasons, starting from the poor shape of their armed forces at the beginning of the war and the system of political decision-making.

In all, the content on Victory for Peace represents an attempt by the Russian government to convince readers of its narrative. In some cases this seems like a simple desire to assert Russia's "right to claim leadership among the winning countries"—to tell their side of the story. In other places, it is more concrete, such as the story of how Crimea and Sevastopol "returned to its historical motherland."¹³⁷

The latter angle perhaps provides a window into why this Page was created. After all, claiming the title of "leader among the winning countries" may not have an impact on global politics. But reframing the results of the Second World War—emphasizing how hard Moscow fought for Sevastopol and the Crimean Peninsula—is a subtle way to rationalize Russia's annexation of Crimea. This is also true for countries like Poland and Ukraine, which, Victory for Peace implies, do not show enough gratitude for what the USSR did for them. Considered as a whole, then, Victory for Peace is of a piece with Russia's larger effort to portray all of Eastern Europe as its backyard and a region in which it has special prerogative.

Compared to the other Pages reviewed in this data set, Victory for Peace was an above-board operation. Although it published pieces in English, it made no effort to hide its origins. Its Twitter account follows 30 accounts, all official Russian news agencies. This distinguishes it from influence operations like Inside Syria Media Center, for which fake authors were created, and positions it closer to official outlets like RT and InfoRos.

Victory for Peace was the only Page in the data provided by Facebook that was advertised across the platform. The Page's managers created and purchased six advertisements, all featuring an image of three soldiers—American, Soviet, and British—celebrating V-J Day:



Figure 25. The image featured in all 12 Victory for Peace advertisements. In each case the image linked to the Victory for Peace Facebook Page.

Six additional ads, also featuring this image, were not purchased but were included in the data collected by Facebook. The purchased ads were aimed at different audiences and appear to have had varying results. The most effective ad, in terms of engagement, was one purchased for 3000.00 rubles aimed at Facebook users in Belgium, Bulgaria, the Czech Republic, Denmark, Finland, France, the United Kingdom, Greece, Hungary, Israel, Norway, Poland, Romania, and Serbia—and at users characterized by an interest in “Peace, History, War, World War II or Politics and social issues.”¹³⁸ This ad attracted 1,206 clicks and generated 94,910 impressions. Other, nearly identical ads were aimed specifically at Facebook users in the USA, the UK, France, and Russia. Overall, Victory for Peace’s six purchased ads generated 212,936 impressions and 2,032 clicks at a cost of 18,000 rubles (approximately \$280), or roughly 9 rubles (\$0.14) per click.

Date	Spend	Impressions	Clicks	Engagement Stats	Countries	Interests
2015-04-10 14:42:23 UTC	3,000.00₽	3960	162	CPC: 18.5₽ CTR: 4.1%	USA	Peace, History, Veterans or World War II
2015-04-10 14:52:29 UTC	3,000.00₽	94,910	1,206	CPC: 2.5₽ CTR: 1.2%	Belgium, Bulgaria, Czech Republic, Denmark, Finland, France, United Kingdom, Greece, Hungary, Israel, Norway, Poland, Romania, Serbia	Peace, History, War, World War II or Politics and social issues
2015-04-10 14:53:49 UTC	6,000.00₽	103,586	524	CPC: 11.5₽ CTR: 0.5%	Belgium, Czech Republic, Denmark, France, United Kingdom, Greece, Hungary, Israel, Luxembourg, Netherlands, Norway, Poland, Serbia, Russia	Peace, History, War, World War II or Politics and social issues
2015-04-15 16:55:47 UTC	2,000.00₽	2,192	62	CPC: 32.2₽ CTR: 2.8%	UK	n/a
2015-04-15 16:58:45 UTC	2,000.00₽	5,170	44	CPC: 45.5₽ CTR: 0.8%	Russia	n/a
2015-04-15 17:01:54 UTC	2,000.00₽	3,118	34	CPC: 58.8₽ CTR: 1.1%	France	n/a
Totals	18,000₽	212,936	2,032			

Table 5. Engagement statistics for Victory for Peace paid advertising including cost-per-click (CPC) and clickthrough rate (CTR).

The ads were designed to appeal to users in a neutral way and funnel them toward more strongly ideological content. Even without the specific interests stipulated by the ads' buyers, the V-J Day image's connotations of goodwill and the Allied spirit would potentially draw in any user with an interest in the history of World War II, regardless of their political alignment. After users clicked on the ad and visited the Victory for Peace Page, they were shown other, more pro-Russian, content. A tweet from the Victory for Peace Twitter account used the same V-J Day image, and while we cannot assume that it featured exactly the same language as the ad, it suggests the direction the ad buyers might have taken:



Figure 26. A tweet from the Victory for Peace Twitter account featuring the same image used in the Facebook Page's advertisements.

Second, the USA, the UK, France, and Russia were singled out for ads, while a large set of other European countries were lumped together. In effect, more money was spent targeting users in the first set of countries, while the second, larger, set was allotted a sum spread out among those countries. Setting aside Russia, this suggests that the GRU saw Victory for Peace primarily as an operation in the Cold War context. This would be in accord with the notion, common in Russian propaganda, that the USSR, and Russia by extension, has never received the respect it deserves. The desire to remedy this was perhaps one of the more abstract considerations motivating Victory for Peace.

It is also potentially significant that Victory for Peace is associated with InfoRos.



Figure 27. Footer crediting InfoRos on victoryforpeace.ru.

Home > Whois Lookup > VictoryForPeace.ru

Whois Record for VictoryForPeace.ru

Domain Profile

Registrant Org	InfoRos Co., Ltd
Registrar	RU-CENTER-RU IANA ID: – URL: https://www.nic.ru/whois Whois Server: –
Registrar Status	REGISTERED, DELEGATED, VERIFIED
Dates	1,624 days old Created on 2015-04-07 Expires on 2020-04-07
Name Servers	NS1.INFOROS.RU. (has 824 domains) NS2.INFOROS.RU. (has 824 domains)
Tech Contact	–
IP Address	91.109.201.210 - 451 other sites hosted on this server
IP Location	- Moskva - Moscow - Okay-telecom Ltd.
ASN	AS199669 ATLEX-AS, RU (registered Oct 12, 2012)
Hosting History	3 changes on 3 unique name servers over 4 years

Website

Website Title	1945: Our common victory
Server Type	nginx/1.15.6
Response Code	200
Terms	236 (Unique: 132, Linked: 10)
Images	5 (Alt tags missing: 2)
Links	10 (Internal: 9, Outbound: 1)

Whois Record (last updated on 2019-09-17)

Figure 28. Whois records showing Victory for Peace's use of InfoRos name servers.

InfoRos is a Russian information agency “dedicated to a wide range of topical issues of political, economic and socio-cultural life of Russia and CIS countries.”¹³⁹ It is registered with Russia’s Ministry of Digital Development, Communications and Mass Media of the Russian Federation and has many of the hallmarks of state media: it does not identify an editorial staff and frequently reposts content from other sources with no byline.¹⁴⁰ Its main site, inforus.ru, publishes news and opinions in English and Russian, as well as resources for visitors looking to find out more about Russian businesses in certain industries. InfoRos also runs Twitter, Facebook, and VK accounts of varying influence; its English-language Facebook page, for instance, has close to 40,000 followers, while its (dormant) Twitter account has 86.

More importantly, InfoRos has been previously linked to GRU Unit 54777 as part of an operation aimed at Russian expatriates.¹⁴¹ Facebook’s attribution of a Victory for Peace Page to the GRU might indicate that Russian state media and the security services are more closely intertwined than it seems. Many observers have speculated on the connection between these two branches of the government, but evidence is scarce because there would be no need to establish tangible links,¹⁴² as the cases of Fancy Bear and CyberBerkut, described below, show, state media networks can publish the results of the GRU’s operations without actually working with it. Using state media directly in a narrative-laundering operation, however, is another matter; the connection between Victory for Peace and InfoRos merits further investigation and suggests that the GRU does not rely only on the creation of fake think tanks and the like—it can enlist above-board state media as well.

These six GRU-affiliated media front pages—Inside Syria Media Center, Crna Gora News Agency, Nbenegroup.com, The Informer, World News Observer, and Victory for Peace—and the associated network of personas provide a look at how Russia has updated their well-established influence mechanisms of narrative laundering for a digital age. In addition, the data set appears to reveal the GRU’s initial attempts to insert its narratives into the social media environment. However, those attempts for the most part failed; instead, their success largely came in the form of placement in and amplification from alternative outlets and via large state media entities, allowing the Russia-aligned narratives to reach a larger audience. Regionally-focused operations, including those targeting Ukraine and the US, followed a similar pattern.

5.2 Operations Targeting Ukraine

Background

Although efforts by the Russian government to influence its neighbor to the west are neither new nor unexpected, they took on a new intensity during, and especially after, the Euromaidan protests of 2013–2014. Because the GRU-attributed Pages targeting Ukrainian users are focused on the characteristics and consequences of Euromaidan, we include a summary of the pro-Western Ukrainian revolution of 2014 and the standard narratives used by the Russian government to frame opposition to it.

In November 2013, the protest movement that came to be known as Euromaidan began in central Kyiv. The proximate cause of the protests was then President Viktor Yanukovych’s decision to back away from the Association Agreement between Ukraine and the European Union that had been under negotiation since 2012.¹⁴³ But the conflict between Yanukovych’s government and the students and activists who gathered in Kyiv’s central square was also a new flare-up in the much deeper, long-standing conflict afflicting Ukrainian society, which had experienced the Orange

Revolution only nine years before.¹⁴⁴ In general, the Western part of the country, largely Ukrainian-speaking and with historical ties to Poland and the Austro-Hungarian Empire, sought closer ties with the EU; the East, home to large Russian-speaking populations and for centuries part of the Russian Empire, wanted Ukraine to remain closely tied to Russia.¹⁴⁵ This internal tension was not simply a matter of domestic affairs; the Russian government has historically exploited this divide to exercise influence over Ukrainian politics.¹⁴⁶ When Euromaidan culminated in February 2014—after days of street fighting in Kyiv that left more than 100 dead and government control over parts of Western Ukraine had effectively ceased—Yanukovych fled to Russia and a new government was installed in Kyiv. This revolution was seen by one side as a rejection of the widespread corruption of the Yanukovych government and Russia's undue influence over Ukrainian politics, and by the other as the usurpation of a lawfully elected government.

The Russian government had a lot to lose in this struggle, and it did not sit idly by as the Ukrainian government began its turn to the West.¹⁴⁷ Its use of force, including the annexation of Crimea and military intervention in the Donbass region, played out for all the world to see. It also fought an ideological narrative battle. From the beginning, the Russian state media sought to discredit Euromaidan as a coup d'état fomented by the US in cooperation with fascist Ukrainian nationalists. This was the Russian government's "open" narrative, the one that it sowed at home and abroad with the help of its domestic and international news outlets and its Ministry of Foreign Affairs.¹⁴⁸ In addition to this narrative, which could be followed on state news channels each evening, the Russian government undertook a covert influence operation consisting of fabricated social media pages and hack-and-leak attacks.¹⁴⁹ The aims of this influence operation were twofold: to turn international opinion against the pro-Western government in Kyiv and to weaken Ukraine from within by exacerbating existing tensions between East and West.

Committee of Soldiers' Mothers of Ukraine | Комитет солдатских матерей Украины

One GRU-attributed Facebook Page targeting Ukraine appears to have purported to represent the Committee of Soldiers' Mothers of Ukraine (CSMU). This organization is modeled after a Russian NGO, the Committee of Soldiers' Mothers [Комитет солдатских матерей] (CSM), which uncovers abuses in the Russian military and advocates on behalf of soldiers. It is worth noting, given the outline of the Russian government's influence operations in Ukraine, that CSM has historically been a source of problems for the Russian government, especially with regard to its military operations.¹⁵⁰ Facebook's attribution of a Page for the CSMU to the GRU may suggest that the Russian government saw in the CSMU an opportunity to create similar problems for the Ukrainian military effort.¹⁵¹ In this report we do not make a firm assessment regarding the legitimacy of the CSMU; it is quite possible that the GRU simply created a Facebook Page for an otherwise authentic organization.

The CSMU became active in September 2014, five months after the beginning of the armed conflict in the Donbass. The group maintains a website on which it regularly posts appeals to the Ukrainian government, reports of corruption in the armed forces, and accounts of soldiers' plights in the war in the Donbass.¹⁵² A recent post, for example, details the fate of a Ukrainian soldier driven to suicide by hazing in the ranks and attacks the Ministry of Defense for its tendency to "close its eyes rather than investigate non-combat deaths." The group also maintains a Page on VK (entirely in Russian) that has been updated more recently, and there is a CSMU Facebook Group, dormant since 2015, that is mostly pro-Russian in tone and content, although it links to the

CSMU website.¹⁵³ This Group was most active, posting nearly every day, from January to March 2015. It appears to have been overrun by suspicious pro-Russian accounts — one example is Olga Gromova, below — and then abandoned.

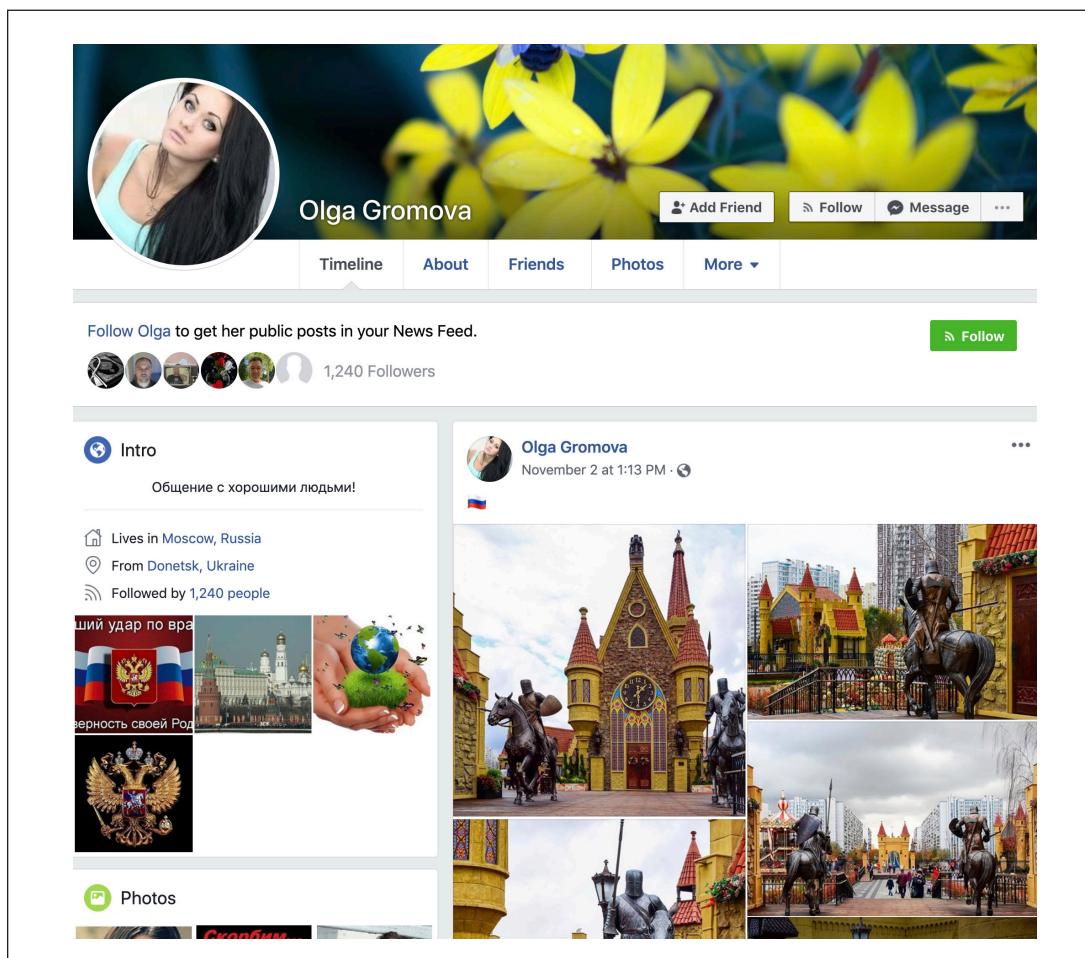


Figure 29. The Facebook Profile for Olga Gromova, one of the accounts that joined a Facebook Group associated with CSMU and converted it into a channel for anti-Kyiv content. Gromova's profile picture and some of the photos purporting to be her were taken from other social network profiles (several are popular on Pinterest). The Gromova profile has been active since July 2014, and its publication pattern suggests that it has been used for different purposes over that period.¹⁵⁴ We are not able to make a conclusive attribution of this account to the GRU.

Interestingly, the CSMU website features Like buttons that link to both the Facebook and VK communities—despite the fact that, in contrast to the VK page, the Facebook Group never posted any CSMU content, instead featuring pro-Russian videos and articles. It is curious that the official CSMU website came to feature a link to this Facebook Group, which never posted any content relevant to it, and that this link stayed up after the Group was overrun by pro-Russian accounts (at least one of them a likely persona).

The GRU-attributed Facebook Page for CSMU appears to have been active for only one day: March 24, 2017, when it posted profile images identical to CSMU's VK page and similar to the image that

appears in the header for CSMU’s website. This date falls between activity on CSMU’s other pages, which show activity on March 16, 2017, and April 5, 2017.

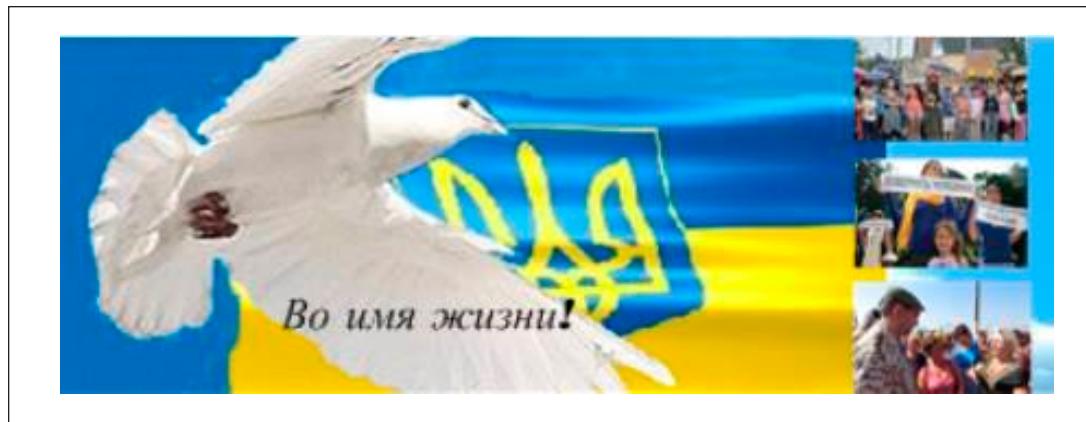


Figure 30. An image from the Facebook Page for the Committee of Soldiers’ Mothers of Ukraine. The inset Russian text reads “In the name of life!”

Because it posted almost nothing, the GRU-attributed CSMU Page is not a useful source of information about how the GRU may have sought to use the CSMU to further Russian narratives about the conflict in Ukraine. It is clear, however, that the CSMU would have presented a good opportunity to the Russian government: a domestic NGO, with a well-regarded analog in Russia, that created problems for the Ukrainian military and frequently questioned the need to fight against the rebels in the East. It is unclear to what extent, if any, the CSMU acted in concert with the Russian government—the answer might be not at all—but it certainly furthers Russian interests in its attacks on the Ukrainian Ministry of Defense and its exposés of abuse in the armed forces, potentially undermining citizens’ confidence. It is true that the group has been accused by Ukrainian journalists of employing crisis actors to stir up indignation, of spreading fake news about the Ukrainian military, and of collaborating with Antimaidan activists, but it is difficult to verify these claims. Regardless, boosting organizations centered around divisive issues was one of the core tactics of the disinformation campaign executed by the IRA—which created social-media accounts with names identical to those of real decentralized social groups such as Cop Block, for example—and the GRU’s attempt to exploit CSMU in this context does not indicate anything about the organization’s legitimacy. The wider activity of CSMU may merit further investigation by Ukrainian journalists.

CSMU appears to demonstrate a GRU tactic of inserting inauthentic Facebook Pages into legitimate pro-Russian networks and groups to support and enhance pro-Russian messages. (See appendix for a strategically similar Page, Antimaidan ukraine.) Another Ukraine-focused Page, For an Exit from Ukraine, might have attempted the same tactic but took on a different domestic-Ukraine focus to appeal to a pro-Western audience.

For an Exit from Ukraine | За вихід з України

This GRU-attributed Facebook Page departed from the Russian government's "general line" on Ukraine-related matters. For an Exit from Ukraine targeted Ukrainians living in Western Ukraine, and in Lviv in particular. Because anti-Russian sentiment and support for Euromaidan was very high in this part of Ukraine, it was likely necessary to take a different approach to this audience.¹⁵⁵ The strident anti-Euromaidan and anti-EU message sounded daily by Russian state media outlets and social media accounts would not have gained much traction here. Thus, if the objective was societal division in Ukraine, it was necessary that the GRU create a new, non-Russian persona, and a different narrative.

The GRU-attributed For an Exit from Ukraine Facebook Page represents one approach to accomplishing the goal. Although there is no evidence that it was successful—it was active for less than a month, from June 2 to June 30, 2017, and most of its posts received no engagement at all—it suggests another strategy within the Russian government's influence operations in Ukraine. This strategy had four components:

- Stoking anti-government sentiment among Leopolitans by appealing to Lviv's historical status as a Polish city.¹⁵⁶
- Sharing content from other Facebook Pages and groups dedicated to helping Ukrainians and Russians emigrate to and find work in Poland.
- Sharing news and articles related to visa-free travel between Ukraine and EU countries, and to Ukrainian emigration to the EU.
- Criticizing the Ukrainian government for creating conditions in which it would be impossible to stay and live in Ukraine.
- All of these components were wrapped up in an anti-Ukrainian narrative implying that Western Ukrainians would be better off leaving their country. Thus, although For an Exit from Ukraine pushed in a different direction than other GRU-attributed pages, it was aligned with the same larger goal to pull Ukrainian society apart.

The For an Exit from Ukraine Facebook Page was so small and short-lived that it is difficult to draw many conclusions. Outside of a few shared articles and a single photoshopped image, very little time appears to have been spent on it. A narrator of sorts was created, but only the penultimate post on the Page gives any indication of what kind of narrator this was: a status update, written in English, lamenting Ukraine's lack of a future and expressing a great desire to emigrate to Poland.¹⁵⁷ The Page briefly tapped into Lviv- and Poland-centered groups and then disappeared. There is also no evidence that anything was done to amplify the Page's content on other social platforms or to extend its reach, and thus it was essentially a Page in a vacuum.



Figure 31. An image from For an Exit from Ukraine showing Lviv's Old Town, with a Polish flag photoshopped onto City Hall Tower.

Because of this, For an Exit from Ukraine is primarily interesting as an indication of an alternative direction in Russian influence operations in Ukraine and of the GRU's adoption of social media tactics associated with the IRA. Although the creators of the For an Exit from Ukraine Page did not use the IRA's playbook for increasing audience and engagement, they did attempt to create a persona that could credibly appear to be Ukrainian and advance a certain domestic point of view. This is something of a departure from the GRU tactics targeting Ukraine observed in the rest of the data set, and thus worthy of note. In some respects For an Exit from Ukraine resembles another embryonic effort to achieve what the IRA accomplished: create content that successfully pitted opposing sides of the political spectrum against each other and develop online hotbeds for inflammatory rhetoric around domestic issues.

5.3 Operations Targeting the United States

Perhaps the most well-known recent GRU activity targeting the United States has been the Fancy Bear (also referred to by cybersecurity professionals as APT 28) hacks of the Democratic National Committee and the Hillary Clinton presidential campaign in 2016. Data provided by Facebook related to Fancy Bear and DCLeaks are discussed in detail in the hack-and-leak section of this white paper. However, the data set also revealed a series of smaller GRU-attributed operations targeting Americans on racial and geopolitical topics, including a curious fan page for a reporter with a State Department beat.

Race

Michael Brown Memorial

Much like the well-documented IRA activity related to race and the Black Lives Matter movement,¹⁵⁸ the GRU-attributed Facebook Page Michael Brown Memorial aimed to stoke racial animus. The GRU activity overlapped in time with the IRA-run operation: GRU creators began to post on January 27, 2015, and posted several times a day until March 3, 2015. Following this spate of activity, the GRU Page went largely dormant until January 6, 2016, when it posted once per month from January through April 2016, and then ceased operations. The content was almost exclusively Shares of news articles and videos, 56 in total, featuring stories of officer-involved violence. Most focused on high-profile instances of Black men killed by police in the US. There was no editorializing over the posted articles; the Shares included a snippet or the title, and nothing else.

Despite sharing a common theme, the content did not identically overlap with IRA content posted during the same time frame. However, there were a handful of memes in the data set visually similar in form and structure to those used by the IRA; one came from a page that the IRA also drew material from.



Linked Media File: linked_media_photos_2478059554.jpg

Id 2478059554

Title Our country and our society are sick. It's not normal that we afraid both criminals and police although the rest must protect us from the first. They behave similarly. Meeting to both of them can bring sad outcomes. But there is the difference. Criminals act like that because they want ur money and belongings. Police do it because they have extra rights and power. It looks like sadism! So what's worse?

Uploaded 2015-02-25 07:46:14 UTC

Comments Count 0

Share Count 1

Likes Count 4

Reactions Count 4



Figure 32: Memes on the Michael Brown Memorial Page.

This GRU-run Page was markedly different from the closely related IRA pages in that it had extremely low engagement and no indication that it was attempting to purchase or drive traffic to grow any meaningful audience. The Michael Brown Memorial Page provides one of the starker examples of the differences in social media execution between the two disinformation actors on an identical topic. It was not substantially interlinked into either the broader real Black media ecosystem or the GRU's other Pages. (There was a single Status Update featuring a link to another Facebook Page, Justice for Jerame Reid,¹⁵⁹ which is down) By contrast, the IRA executed on both types of interlinking strategies with its own Black community-targeted efforts.

Baltimore is Everywhere

The second race-related Page in the data set, Baltimore is Everywhere, appeared well after the Michael Brown Memorial Page stopped posting. It was active for one month only, from May 10 to June 1, 2017, and appeared to post, or make repeated edits to posts (this is not always clear from the data set) multiple times per day. This Page appears to have created posts mere minutes apart from each other.



Figure 33. The Baltimore is Everywhere Facebook Page banner.

Like the Michael Brown Memorial Page, Baltimore is Everywhere focused on officer-involved shootings and police violence, and the majority of the content was Shares of real news stories. Domains ranged from Alternet to *The Nation* to the *New York Times*, with local and international press mixed in. The Page content expanded the focus on police brutality to include other countries and other forms of brutality; one story was about police brutality against dogs.¹⁶⁰ One post, from May 15, 2017, reposted a July 2016 announcement of the creation of an organization called the National Association Against Police Brutality (NAAPB) with slight wording changes and no link.

Please click share and share this with people.

The National Association Against Police Brutality (NAAPB)

www.facebook.com/naapb is building a network of passionate and committed volunteers, attorneys, and affiliated service organizations to collaborate with to reform our criminal justice system and end police brutality.

NAAPB will refer incidents to local attorneys and community organizations to offer a legal, spiritual, and wellness services to victims and their families. Our online platform will receive misconduct complaints from citizens in all 50 states. Each referral is reviewed for accurate contact information by a law student or a trained volunteer and then forwarded to an attorney and the requested service organization.

NAAPB can help local community organizations with awareness and coordination of direct actions. Our collective effort is better than our individual strength. I encourage people and organizations of conscious to participate.

Interested parties can inquire about being a part of this network and vital civil rights issue at:

Attorneys

<http://membership.naapb.org/inquiry/attorney>

Individuals

<http://membership.naapb.org/inquiry/individual>

Community Service Organizations

<http://membership.naapb.org/inquiry/organization>



35

1 Comment 55 Shares

Figure 34. A post announcing the creation of the NAAPB, which Baltimore is Everywhere reposted.

Because two posts both use imperfect English (distinct from the fluent English in the news site reshares), they may have been written by the Page owner directly. Both posts directed readers to listen to two online radio stations, HumpDayRadio and Black On Black Network. Several other radio programs were also included as links, but it is unclear why these two programs were selected for more direct promotion. They appear to be legitimate media run by real people living in the US.

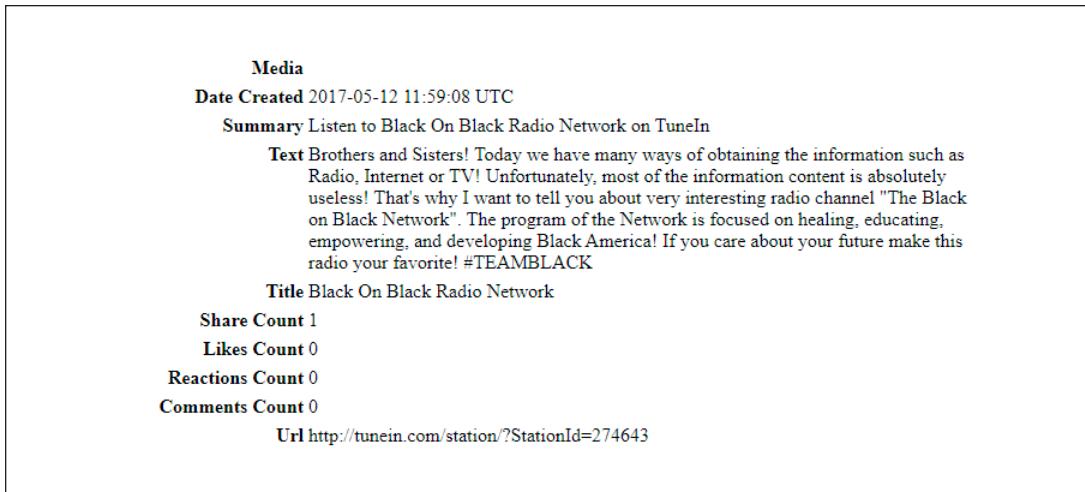


Figure 35. *Baltimore is Everywhere posted a link to online radio station Black On Black Radio Network.*

Interestingly, a May 2017 Baltimore is Everywhere post linked to Black Lives Matter Media,¹⁶¹ which was later revealed by Vox Media to be a fake Black Lives Matter website run by an Australian man with economic motivations. There is no indication that the GRU chose that site strategically, and it only appears once.¹⁶²

More details on Baltimore is Everywhere, including screenshots, can be found in an assessment conducted by the Atlantic Council's Digital Forensics Research Lab, which aggregated data about the account after its first public mention in the DOJ's indictment of GRU operatives. The operation had a Twitter account, @BaltimoreIsWhr, which attempted to start a Twitter hashtag #BlacksAgainstHillary; it largely failed, picked up primarily by other accounts that appear to have been bots, likely owned or operated by the GRU.¹⁶³ This explicitly partisan aspect of the operation is not reflected in the Baltimore is Everywhere Facebook posts. The operation also had a Facebook Group with 4,000 members, and at least one persona that reached out to authentic Black American activists, suggesting that infiltrating communities was not solely the purview of the IRA. The data from the Facebook Group was not provided to SSCI for outside research.

The race-focused Pages targeting the US both aimed to fan the flames of racial dissension in the US, and both primarily shared real long-form news stories of police violence. The Baltimore is Everywhere operation, with its larger (though still small) social media reach, more closely resembled IRA tactics.

Geopolitical Issues

White House Griller

One rather unique US-focused Page in the data set was dedicated to AP Journalist Matt Lee. The title, White House Griller, alludes to a nickname bestowed upon Lee by RT interviewer Gayane Chichakyan.

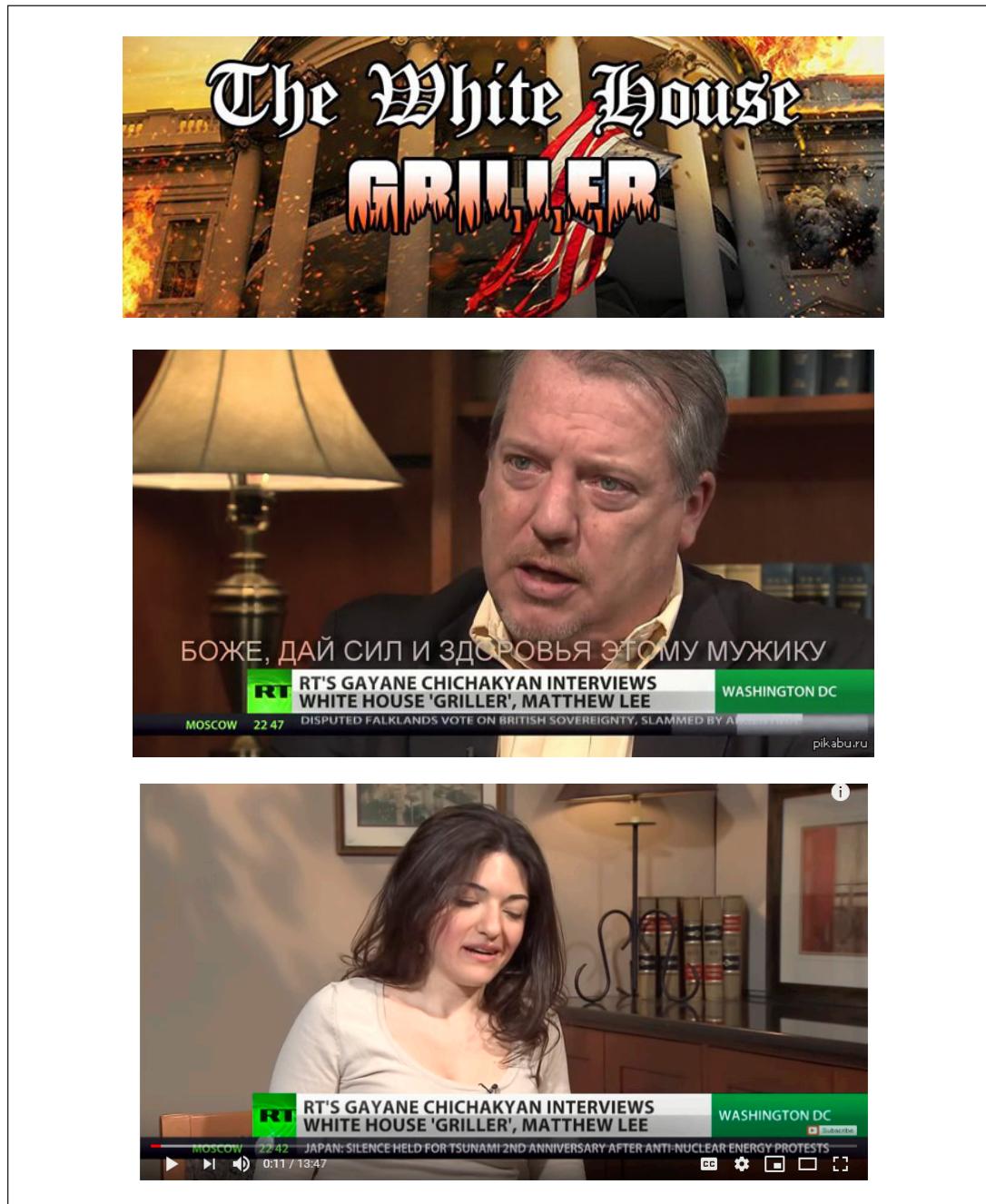


Figure 36. The White House Griller Page header and screenshots of an RT interview with Matthew Lee, known as the “Griller.”

The Page, started on April 20, 2015, is somewhat unique in that it features memes rather than long-form content. The memes were primarily mocking President Barack Obama and trolling other public figures, including former White House deputy press secretary Jen Psaki. Ms. Psaki was serving as a spokesperson for the US Department of State at the time the Page was operational, and videos on the Page feature press conferences in which she comments about human rights abuses by Russian separatists in Ukraine. The Page features videos of Mike Lee questioning Psaki about conflict between Russia and Ukraine, seeming to push back against the idea that Russia intended to commit abuses, which led to a discussion of whether bad actions were committed by both sides. One of the videos is by RT, which wrote derisive articles, including one on June 1, 2015, about Ms. Psaki's "most embarrassing fails, most entertaining grillings."¹⁶⁴ US press coverage at the time the White House Griller Page was active noted the Russian media's "obsession" with Jen Psaki,¹⁶⁵ which extended to state TV creating a recurring comedy news program targeting her, and bloggers and Twitter accounts¹⁶⁶ extensively mocking an orthopedic boot¹⁶⁷ she wore following an injury. Lee's comprehensive questioning of Ms. Psaki appears to have won him favor more broadly. This is one of several examples in the data set of Russian state media (RT) and Russian military intelligence executing similar messaging.



Figure 37. Memes posted on White House Griller, mocking White House deputy press secretary Jen Psaki.

Kuril Islands

A second geopolitical operation targeting the United States aimed to spread propaganda about the Kuril Islands, the ownership of which Russia and Japan (a US ally) have long disputed.¹⁶⁸ By date—2014—this operation appears to be one of the earliest attempts at online narrative laundering with the creation of a fake online identity, Andrew (or Andrei) Kolkovich, who authored articles for one fake research group and shared content from another (Nbene Group). The persona was less developed than those of subsequent operations, and leveraged a smaller cluster of sites.

This Kuril Islands operation was revealed through multi-Page analysis. The data set contained a folder indicating the existence of a Page called Andrew Kolkovich true to life, which our research discovered is likely connected to two other Pages and three other social network accounts.

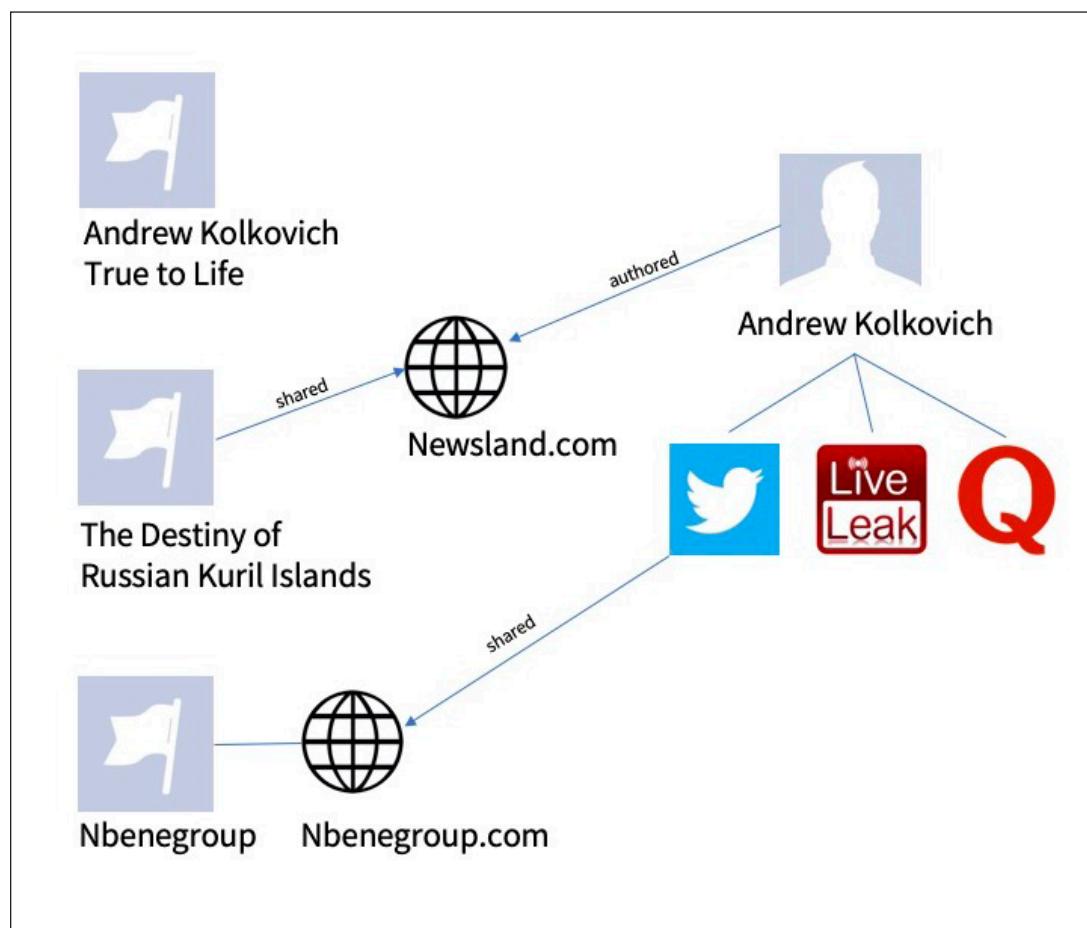


Figure 38. An illustration of the three Facebook Page operations (denoted by the Page flag icon used by Facebook) connected to the Andrew Kolkovich persona. Kolkovich had at least four social profiles: Facebook, Twitter, Quora, and LiveLeak. Via Twitter, he shared content from the nbene-group.com website. He authored content on Newsland.com, which was shared by the Destiny of Russian Kuril Islands page. The third Page appears to have had no activity, but bears his name.

The Andrew Kolkovich true to life Page contained no shares, photos, videos, or ads. Searching Facebook revealed a stub of a user profile by that name with no profile picture, containing one post from July 16, 2015, about Japanese Prime Minister Shinzo Abe.¹⁶⁹ Investigation on other social networks uncovered a Twitter account for an Andrew Kolkovich, whom we first discussed in the personas section of this white paper, with the handle @Andrew324r, created in December 2011 and with the bio “interested in policy and relations between Russia and other countries.....believe in world peace.”¹⁷⁰ The Twitter profile is particularly interested in Japan, US, and Russian relations, with its earliest tweets from December 2011, a time of significant tension around ownership of the Kuril Islands, asking why Japan would not sign a peace treaty with Russia and expressing concerns about the Kuril Islands.

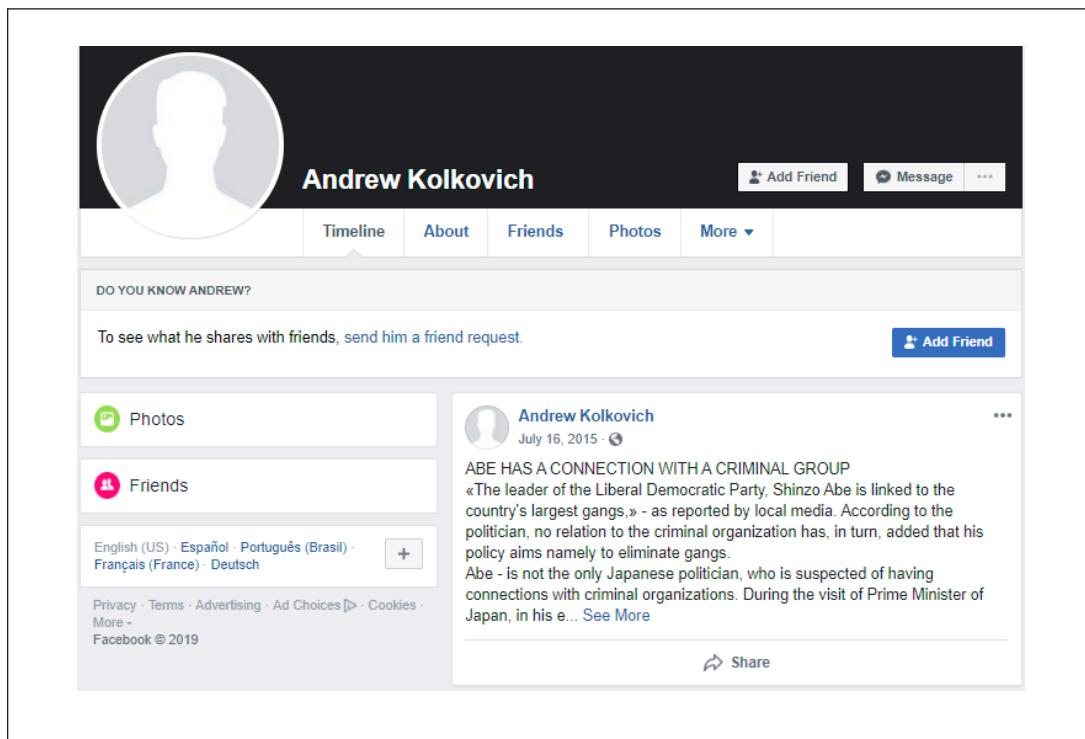


Figure 39. Stub Facebook profile of Andrew Kolkovich.

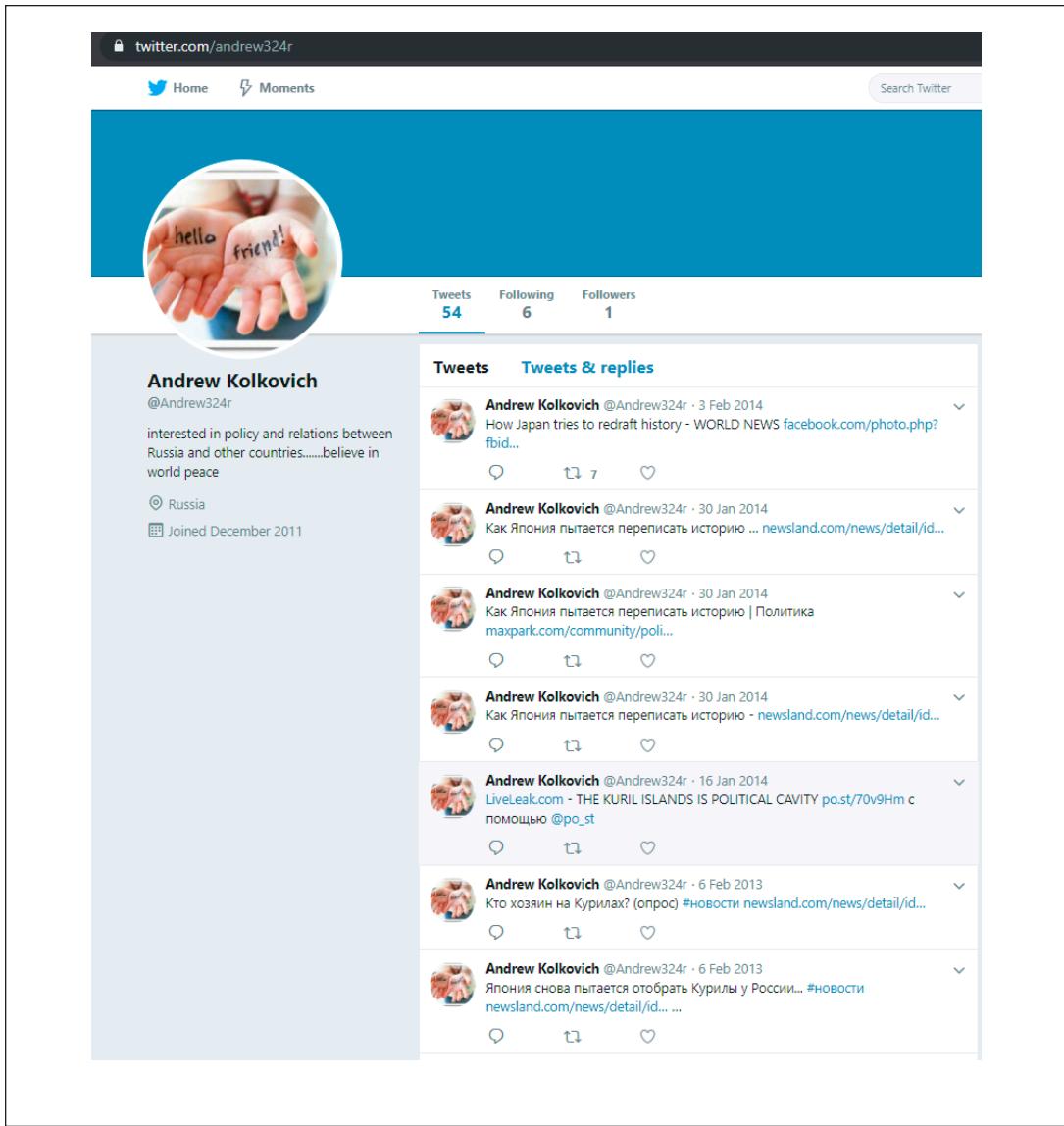


Figure 40. Twitter profile of Andrew Kolkovich.

The Kolkovich Twitter account is older than the Facebook Page; it tweeted repeatedly in December 2011 and then a few times a year thereafter until Feb 3, 2014. The tweets also contain links to a number of articles from Newsland.com and Maxpark.com bearing Kolkovich's byline, sometimes as Andrei Kolkovich.¹⁷¹ The written content includes articles related to the Kuril Islands issue, but also includes posts critical of the US, attempts to erode NATO and Asia Pacific alliances, and claims that the US was creating an "Indian Reservation Policy"¹⁷² of dividing the world up into areas it could control.

The Kolkovich Twitter account additionally shared URLs including dozens of InfoRos articles (using the shortener clck.ru) and an analysis by purported think tank NBene Group. Nbenegroup.com, per our earlier analysis, was the title of another folder in the GRU-attributed data set, indicating that the Kuril operation spanned multiple pages. In addition to Nbenegroup.com, Kolkovich is

linked to a data set folder for a Page named The Destiny of Russian Kuril Islands, which featured a collection of memes mocking Japan and articles attempting to undermine the US-Japan and Russia-Japan relationships. The article content, posted to the Page around a photo, appears to be translations of the original content bylined Andrew Kolkovich. The Destiny of Russian Kuril Islands Facebook Page appears to be the earliest cohesive operational content in the data set,¹⁷³ with a first post to the Page on February 3, 2014; the only post to the Facebook Page for Nbenegroup.com was made on the same date, one hour later. The content of both posts was the text “123.” The Destiny of Russian Kuril Islands Page ceased activity in October 2014.

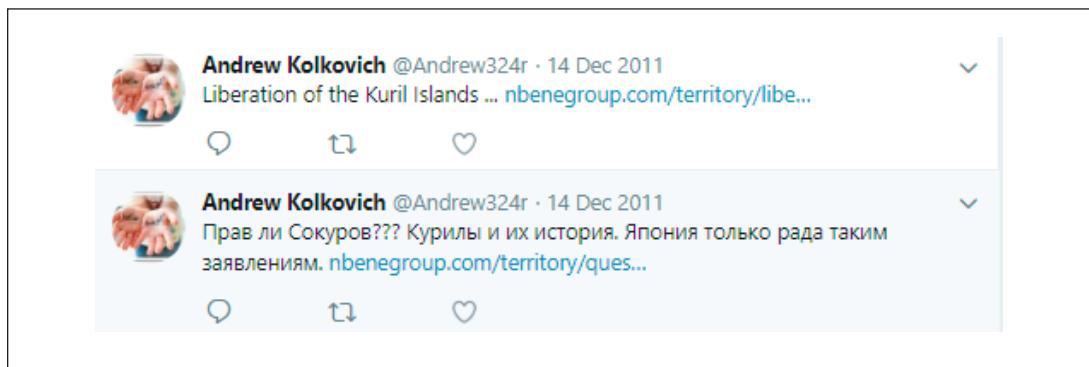


Figure 41. Tweets by Andrew Kolkovich linking to NBGroup.com articles.

Content for Andrew Kolkovich across the broader internet reveals him to be a frequent commenter on Russian news portals, as well as the creator of a LiveLeak channel that was operational from 2014 to 2015 (now down) and focused on the US, Japan, and Russian relationship.¹⁷⁴ There is also an Andrew Kolkovich account on Quora that answered one question: “Do you think Americans are right to hate the Japanese for Pearl Harbor?” Kolkovich responds in the affirmative.¹⁷⁵

The image shows a screenshot of a Quora profile page for Andrew Kolkovich. The profile picture is a dark circular image with some glowing orange and yellow elements. The name 'Andrew Kolkovich' is displayed above the bio. The bio section includes 'Credentials & Highlights' and 'More' buttons, with entries for 'Works at University of Oregon', 'Studied at Southern Federal University', and 'Lives in Eugene, OR'. Below the bio, there are sections for 'Feeds', 'Answers 1', 'Questions 0', 'Shares 0', 'Followers 1', 'Following 0', 'Edits', and 'Activity'. The 'Answers 1' section shows a single answer to the question 'Do you think Americans are right to hate the Japanese for Pearl Harbor?'. The answer text reads: 'Of course they DOI Japanese killed many innocent people in that attack. America didn't even want to participate in that war. Japan made it do it. And there were lots of casualties. Today we have less and less people that can tell you the true story. Japanese attack was truly a sneaky one, not that of 'brave, honorfull' japanese mojo. Americans can truly hate Japan for doing that. And Hiroshima was truly justified!' It also notes '134 views'. At the top of the page, the URL 'quora.com/profile/Andrew-Kolkovich' is visible in the address bar, along with the Quora logo and search bar.

Figure 42. Andrew Kolkovich’s answer to a question on Quora. Kolkovich is likely a persona.

In his Quora profile Andrew Kolkovich claims to work at the University of Oregon; we pursued an investigation into individuals by that name affiliated with the University or living in the state of Oregon, and found no evidence to bolster that claim. None of the online profiles, bylines, or social media accounts contain a photo of Andrew Kolkovich. We believe that Andrew Kolkovich is a persona in the style of Alice Donovan and the ISMC journalists, as we discussed in Section 5.1.¹⁷⁶

The two Facebook Pages in this operation, nbeneigroup.com and The Destiny of Russian Kuril Islands, only got a few dozen engagements across their entire period of activity. It is unclear why they were so weakly developed. Subsequent folders related to more recent operations showed that the GRU replicated this structure—a fake journalist or graduate student persona, replicated on several social sites, purportedly writing for a dubious think tank or independent media property—repeatedly. This perhaps suggests that the Kolkovich-Kuril Islands activity was a first foray into a strategy that became more fully refined as the GRU continued to execute active measures on social platforms.

The screenshot shows a news article from Newsland.com. At the top, there is a red banner with white text asking if the user wants to enjoy the full version and get unlimited access to all materials. Below the banner, the Newsland logo is displayed in a large, bold, red font. To the right of the logo are navigation links for 'Main topics', 'news', 'Hyde Park', 'Communities', and 'People'. The main title of the article is 'How Japan is trying to rewrite history', written in a large, bold, black font. Below the title, the author's byline is listed as 'andrewkolkovich'. The article content begins with a paragraph about territorial disputes between Russia and Japan, mentioning the Kuril Islands. It then discusses a campaign in Japan called 'Fires of the Northern Territories' where candles were lit in central squares. The article continues with a paragraph about a mass event for children and youth in Matsue, Shimane Prefecture, held as part of a campaign to popularize the northern territories among Japanese schoolchildren. It also mentions an essay competition in Kyoto. A photograph of children in a classroom setting is included on the right side of the article. The bottom of the article contains a continuation of the text, describing another event in Matsue on January 27, 2014, where children learned about the northern territories.

Figure 43. An article from Newsland.com bearing Kolkovich's byline.



Linked Media File: linked_media/photos_817262002.jpg

Id 817262002

Title How Japan tries to redraft history Everybody knows about the territory dispute between Russia and Japan. Each Russian knows that the Kuril Islands are Russian territory. And each Japanese believes that four islands of the Kuril string will become Japanese according to some unbelievable reasons. Each year these Asian fans of Russian Cheburashka try to open debates over the Kuril dispute. They even have established a holiday – “The Day of Northern territories” which is celebrated on the 7th of February. Last year Japanese have conducted the protest action named “The lights of The Northern territories”. As part of it they were lighting candles on the central squares of their cities and ... and just standing together full of hope. May be they were hoping to be snapshoted by Russian satellite. This year they understood that candles wouldn’t help them to take islands back. So, they decided to implant to young heads the idea that the Kurils belong to Japan. According to Japanese daily newspaper “Sankei Shinbun” on the 26th of January in Matsue (prefecture Shimane) there an event was organized for Japanese children and teenagers called “Let’s know about The Northern territories properly” within the framework of program “The school of joy of four islands” aimed to popularize “The Northern territory” problem among Japanese pupils. Children took part in competitions and other games devoted to “Northern territories”. And in Kioto (prefecture Kioto) a composition contest was held under the theme “The Northern territories and we” among pupils of high schools. Pupils of 18 schools took part in it. Organizers underlined the improvement of compositions quality in comparison with last year. As they said the majority of compositions “mirror author’s perception of The Northern territories disputes and contain thoughts about ways of resolving a problem”. It should be noted that Japan Parliament association of returning Northern territories established in 2003 organized all of these events. In that way the Japanese make self-hypnosis and actively impart falsified history to young generation. This is the way of redrafting the history. Ten years later these children will become full-fledged citizens of their country and will be wholly sure that Kuril Islands belong to Japan. Though ... even in that case they will get nothing.

Uploaded 2014-02-03 11:22:36 UTC

Figure 44. A post in The Destiny of Russian Kuril Islands Page that replicates content bylined by Andrew Kolkovich in the Newsland article in Figure 43.



Figure 45. Memes from the *Destiny of the Kuril Islands* Facebook page.

The two regional clusters in the data set, targeting Ukraine and the US, again provide a view into Russia's attempts to port its long-standing propaganda technique of narrative laundering to the online environment. In most cases, the social component of the operations failed to create engagement with the Pages or their related social media accounts. This is interesting in light of the IRA's more substantial success in the same time period.

5.4 Hack and Leak Operations

The Facebook GRU-attributed data set contained several folders related to significant hack-and-leak operations, several of which had previously been attributed to the GRU with varying degrees of confidence; this Facebook attribution can be taken as another point of corroboration from a different angle.

Of note is the fact that direct engagement with Pages in these folders was relatively low; collaboration with WikiLeaks and press outreach played a much larger role in capturing public

attention. In the case of DCLeaks in particular, it becomes increasingly clear that media, not social media, had the most significant impact on amplifying that hack-and-leak operation for the American electorate.

Some of the operations in these Pages are familiar to the public. The first of these was a set of several folders related to the hacking group known as Fancy Bear. Fancy Bear, one of the names associated with cyber espionage group APT 28, has long been believed to be affiliated with the GRU by cybersecurity experts.¹⁷⁷ That attribution was further bolstered by the 2018 US Department of Justice Special Counsel “Report On The Investigation Into Russian Interference In The 2016 Presidential Election,”¹⁷⁸ which we excerpt here to provide background:

At the same time that the IRA operation began to focus on supporting candidate Trump in early 2016, the Russian government employed a second form of interference: cyber intrusions (hacking) and releases of hacked materials damaging to the Clinton Campaign. The Russian intelligence service known as the Main Intelligence Directorate of the General Staff of the Russian Army (GRU) carried out these operations. (p. 4)

Two military units of the GRU carried out the computer intrusions into the Clinton Campaign, DNC, and DCCC: Military Units 26165 and 74455. Military Unit 26165 is a GRU cyber unit dedicated to targeting military, political, governmental, and non-governmental organizations outside of Russia, including in the United States. (p. 36)

Military Unit 74455 is a related GRU unit with multiple departments that engaged in cyber operations. Unit 74455 assisted in the release of documents stolen by Unit 26165, the promotion of those releases, and the publication of anti-Clinton content on social media accounts operated by the GRU. Officers from Unit 74455 separately hacked computers belonging to state boards of elections, secretaries of state, and US companies that supplied software and other technology related to the administration of US elections. (p. 37)

Starting in June 2016, the GRU posted stolen documents onto the website dcleaks.com, including documents stolen from a number of individuals associated with the Clinton Campaign...The GRU released through dcleaks.com thousands of documents, including personal identifying and financial information, internal correspondence related to the Clinton Campaign and prior political jobs, and fundraising files and information. (p. 41)

GRU officers operated a Facebook Page under the DCLeaks moniker, which they primarily used to promote releases of materials.¹⁷⁹ The Facebook Page was administered through a small number of preexisting GRU-controlled Facebook accounts. GRU officers also used the DCLeaks Facebook account, the Twitter account @dcleaks_, and the email account dcleaksproject@gmail.com to communicate privately with reporters and other US persons. (p. 42)

Mueller Report footnote number 142 names Facebook Account 100008825623541, Alice Donovan,¹⁸⁰ as a persona involved in the operation.

Given the attribution links between Fancy Bear, DCLeaks, and several sports organization hacks, we are grouping our analysis of the Facebook-provided folders bearing names identical to APT

28-attributed operations into this subsection of the white paper, to provide temporal context for how they fit together.

Facebook's data set included folders for four separate Page accounts named after the hacking group:

- Account 579723595544849, simply called Fancy Bears
- Account 163747254078011, named Fancy Bears' Hack Team
- Account 285627401836235, also named Fancy Bears' Hack Team but contained no content
- Account 117210077618144, also named Fancy Bears' Hack Team but contained no content

It also contained data from two Pages from operations named for the document dumps:

- Account 793058100795341, called DCLeaks, a 2016 email hack-and-leak operation that targeted prominent political figures, including NATO Supreme Commander Philip Breedlove, former Secretary of State Colin Powell, Sen. John McCain, Sen. Lindsey Graham, Democratic Party lawmakers, Hillary Clinton's presidential campaign, and investor and philanthropist George Soros.¹⁸¹ The actors behind DCLeaks originally claimed to be "American hacktivists who respect and appreciate freedom of speech, human rights and government of the people."¹⁸²
- Account 150186875444079, Page name Foul Play, another 2016 hack-and-leak operation that targeted sports-related regulatory agencies, including the World Anti-Doping Association (WADA) and the International Association of Athletics Federations (IAAF).

There were 80 posts in total, spread across the three operations.

Page Name	# of Posts and Shares	Date of First Post or Share	Date of last Post or Share	Average # of Likes	Average # of All Reactions	Average # of Shares	Average # of Comments	Total Engagement
Fancy Bears	56	2016-09-12	2017-08-25	47.9	56.2	15.4	13.2	7,427
DCleaks	22	2016-06-08	2016-09-30	9.6	12.7	12.6	3.0	834
Foul Play	2	2016-10-21	2016-10-21	0	0	0	0	0

Table 6. Summary statistics for the hack-and-leak operations.

DCLeaks

The first posts in the Facebook data set for this group of APT 28-related activity appeared on the DCLeaks Page on June 8, 2016, when it announced the existence of dcleaks.com with four posts touting the hacks of Cdr. Breedlove and George Soros's emails. On June 14, 2016, it posted again, announcing the leak of documents from Hillary Clinton's presidential campaign. In a series of posts on July 11, it amplified press coverage from The Intercept, RT, and Veterans Today about a facet of the Breedlove emails in which his writing is framed as provoking President Obama into escalating conflict with Russia; a link to a CNN video appears as well, in which Breedlove defends

himself. A month later, the Page began to focus on George Soros's "plans to counter Russian policy," and to "capitalize on police killing to push their agenda of federalized US police." The DCLeaks operation and Page activity continued sporadically until September 30, 2016, primarily teasing findings related to Clinton campaign email releases.

The screenshot shows a Facebook post with the following details:

Image

From: Phil Breedlove <bvanaf16@gmail.com>
Sent time: 03/15/2015 01:20:40 AM
To: Harlan Ullman <harlankullman@gmail.com>
Subject: Re: idea

Great Minds think alike.... ok I'm taking literal license as it regards me.... but we are headed this way.... end of March we roll out a paper... then we start to roll out some things "we are already doing...."

I'm going to look for some time this week we can sit and chat.

On Mar 10, 2015, at 1:57 PM, Harlan Ullman <harlankullman@gmail.com> wrote:

Phil--as you know, I think NATO needs a stronger declaratory policy vis a vis Russia not so much to threaten but rather to explain what NATO is prepared to do. For example, the return of a heavy BCT to Europe seems to me to be something that needs to be given more attention and not page 20 in Defense news.

Below is my column this week on Hybrid War. The idea is for you and ACT to use hybrid war as the basis for a quick turn around effort on guidelines for countering a hypothetical hybrid attack put out by the two strategic commanders and possibly the subject of a SacEur war-game/seminar or ACT seminar.

Linked Media File: linked_media/photos_2058298363.png

Id: 2058298363

Title: Check the following link (<http://dcleaks.com/index.php/conversation-of-p-breedlove-with-harlan-ullman/>) which contains private correspondence between the Supreme Allied Commander Europe of NATO Allied Command Operations Philip Breedlove and Harlan Ullman, Senior Adviser at the Atlantic Council and the author of numerous policy books. For example P. Breedlove and H. Ullman talk about the leading role of the United States in hybrid war and tightening policy vis-a-vis Russia "not so much to threaten but rather to explain what NATO is prepared to do".

Uploaded: 2016-06-08 13:48:34 UTC

Figure 46. Material from the DCLeaks Facebook page.

Facebook engagement on DCLeaks' Page was minimal—834 engagements across all 22 posts over the four-month period. The Page owners did not run ads or appear to promote it in any way. Many of the documents were subsequently released via WikiLeaks—per the Mueller Report, the GRU reached out to WikiLeaks on June 14, 2016 to help coordinate the release of information related to Hillary Clinton's campaign; the Facebook Page did not link to WikiLeaks but the Twitter account retweeted WikiLeaks regularly. Twitter, a traditional amplification channel for disinformation campaigns, identified two sets of Russia-attributed accounts, both of which show attempts to spread DCLeaks content. Several of the IRA-attributed Twitter accounts, which were operational at the same time as the GRU operation, began to amplify #DCLeaks during the September Hillary Clinton campaign email leak period, primarily with retweets.¹⁸³ Three other accounts in the Twitter data set attributed to Russia, but seen as distinct from the IRA, reference DCLeaks: @CovfefeNation, @CathyTo47590555, and a hashed username account; these also primarily served as amplifiers by retweeting @wikileaks and @DCleaks_. The content also appeared on Reddit.¹⁸⁴ It was additionally covered by RT and state media.

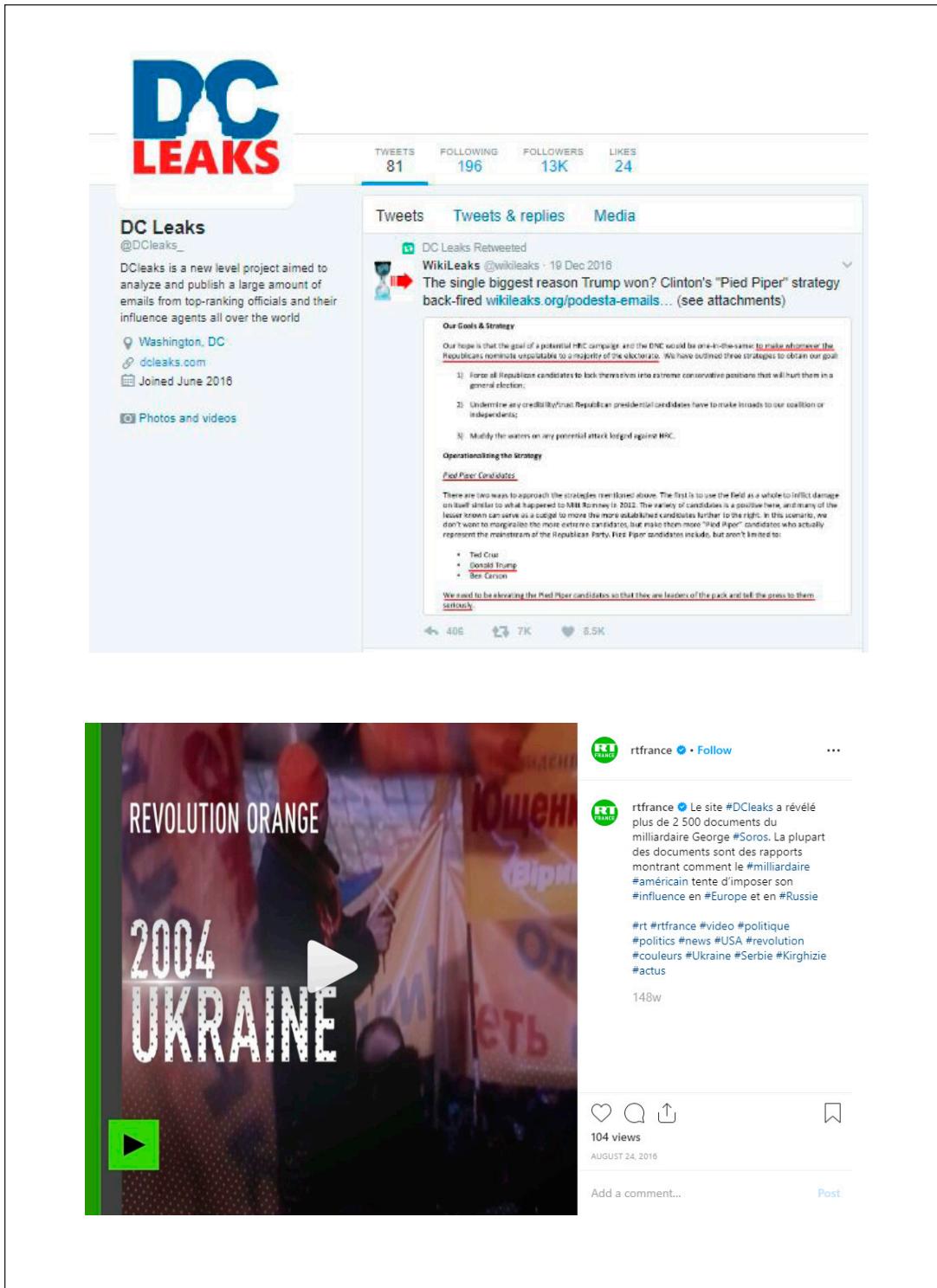


Figure 47. An archived screenshot of @DCLeaks_, and The RT France Instagram feed referencing DCLeaks and the hacked George Soros documents.

Although the GRU involvement in the hack-and-leak operation has been extensively covered, this additional glimpse into the distribution of the material strongly suggests that the GRU was ill-equipped to handle the distribution of the content on social media itself. While it did post via its own accounts, it appears to have achieved most of its traction through the dissemination via WikiLeaks, deliberate links sent to journalists via direct messages, and, subsequently, mainstream media coverage and the IRA influence operation's added lift in sharing the content.

Fancy Bears

Fancy Bears account -849, which began to post on September 12, 2016, contained status updates that linked to the website fancybear.net. This account was used to leak documents related to the GRU hacks of several sports-related entities. It used the hashtags #OpOlympics, #WADA, and #FancyBears, in addition to hashtags of the names of athletes included in the World Anti-Doping Association (WADA) leak. The affiliated website has since been seized by the United States Federal Bureau of Investigation. Note that the image to the left on the group's site is a bear wearing a Guy Fawkes mask; several GRU and IRA campaigns co-opted Anonymous iconography in misattribution efforts as they attempted to conceal their identities.¹⁸⁵

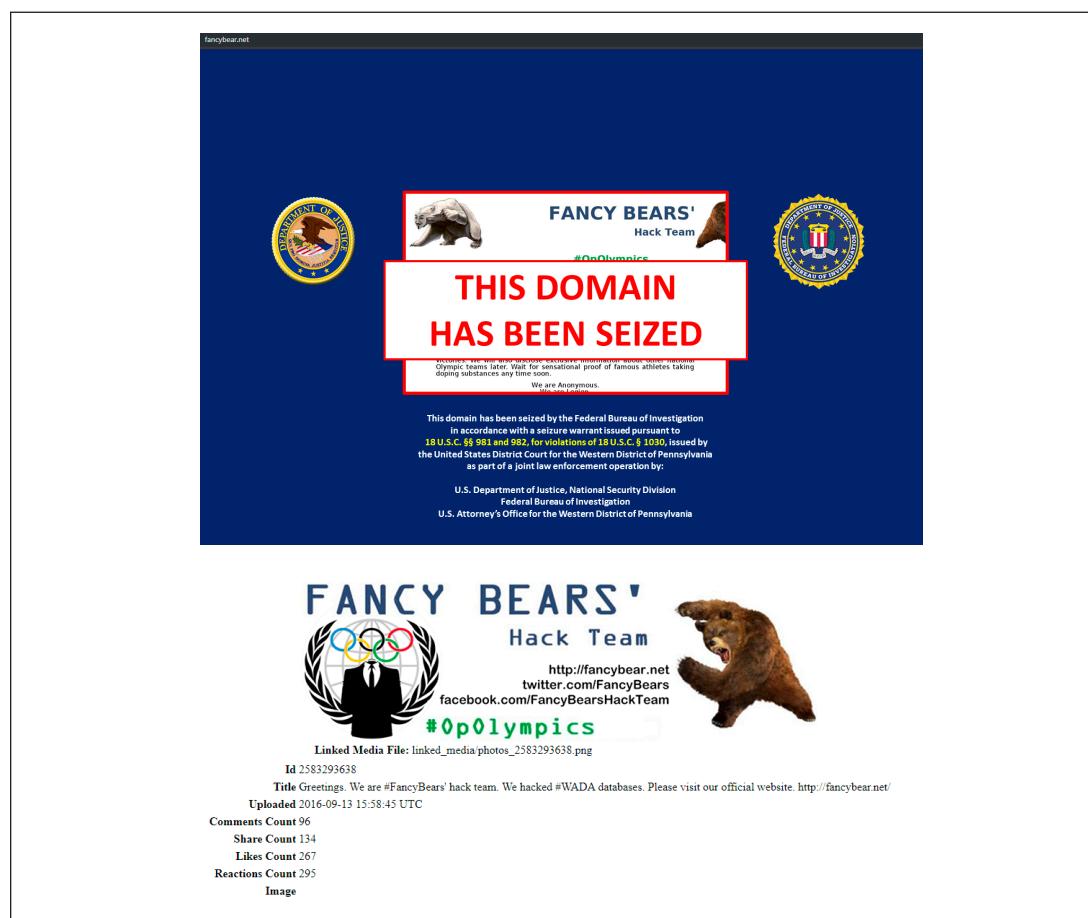


Figure 48. Screenshots of the Fancy Bears' Hack Team website, now seized by the FBI, and a post using the #OpOlympics hashtag.

This account's Fancy Bears' Page was active from September 12 to October 3, 2016, producing 42 posts and 5862 engagements. A majority were images of leaked health records from the WADA hack;¹⁸⁶ WADA stated in their incident report that not all data accurately reflected their database data, suggesting that perhaps the hackers altered or edited some of the data prior to dumping it.¹⁸⁷ It appears that WADA was selected as a target in retaliation for a report written in July 2016 advocating a ban on Russian athletes from the Olympic games due to a widespread doping-detection evasion scandal.¹⁸⁸

The Russian Embassy, UK Twitter account commented on the hack as news of it was unfolding.

The screenshot shows three tweets from the official Twitter account of the Russian Embassy in the United Kingdom (@RussianEmbassy). The first tweet, dated Sep 15, 2016, criticizes WADA for hacking and leaking doping files. The second tweet, also on Sep 15, 2016, uses a magnifying glass graphic to highlight 'Hypocrisy' in WADA's moral standards. The third tweet, dated Sep 14, 2016, compares WADA to Google, suggesting they are both involved in covering up doping.

Russian Embassy, UK @RussianEmbassy · Sep 15, 2016
1/1 @wada_ama hacking: there should be nothing private about doping files of participants of Olympics, which are a very public affair

Russian Embassy, UK @RussianEmbassy · Sep 15, 2016
Leaks: 25 athletes used doping with @WADA_ama knowledge & cover-up. Only 1 Russian, but 5 Brits, 10 Americans.

Russian Embassy, UK @RussianEmbassy · Sep 14, 2016
Released @WADA_ama files show US athletes' use of banned substances was tolerated and covered up. Quod licet Jovi...?

Figure 49. The Russian Embassy, UK tweet on the WADA hack.

The second account with content and the Page name Fancy Bears' Hack Team went live on October 4, 2016, one day after the first Page was active. Perhaps it changed names or administrators; perhaps one Page was shut down and the other spun up—the data provided does not explain the significance of the account numbers and does not include follower count information. The new Page began with another introductory post:

#OpOlympicGames

About us Greetings citizens of the world. Allow us to introduce ourselves... We are Fancy Bears' international hack team. We stand for fair play and clean sport. We announce the start of #OpOlympics. We are going to tell you how Olympic medals are won. We hacked World Anti-Doping Agency databases and we were shocked with what we saw. We will start with the US team which has disgraced its name by tainted victories. We will also disclose exclusive information about other national Olympic teams later. Wait for sensational proof of famous athletes taking doping substances any time soon. We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us. Anonymous – #OpOlympics <http://fancybear.net/>

This second Page posted 14 times through August 22, 2017, and generated 877 engagements.

There was also related Twitter activity: The hacking group displayed the Twitter handle @ FancyBears prominently on their site, strongly suggesting it is affiliated with this operation. The Twitter account is now suspended, though the tweets do not appear to have been released in any Twitter archive (unless it was hacked). The Internet Archive Wayback Machine for the Twitter account, in the last archive from September 2017, shows it used icons identical to those in the Facebook data set, that it joined in September 2016, and that it had 10,500 followers.¹⁸⁹ The Twitter account played a game called #DopingCartoon in its hashtags, encouraging users to create athlete memes about therapeutic use exemptions (TUEs).

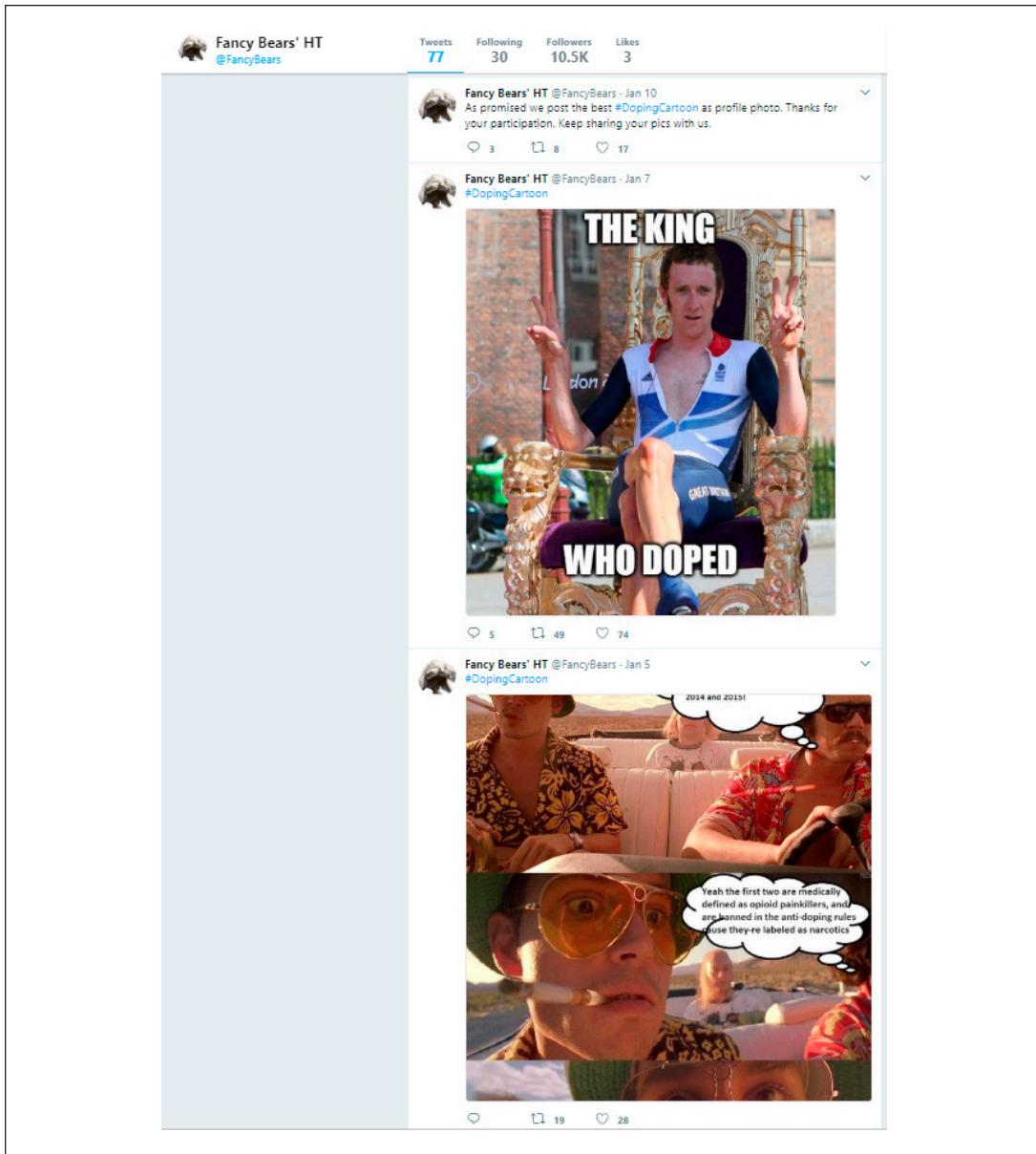


Figure 50. Tweets from @FancyBears.

Western media covered the Fancy Bears document dumps and the responses from the agencies extensively; the prevalent narrative from Western media was that what had been leaked did not expose secret violations but rather the acceptable use of TUEs by prominent athletes. Russian state-sponsored media covered the document dumps as well, creating a far different narrative. RT wrote about Fancy Bear activities on numerous occasions (including on an ongoing basis throughout 2018),¹⁹⁰ as did Sputnik; aligned media properties such as Mint Press News republished Sputnik's content.¹⁹¹ Both overt state-sponsored propaganda sites claimed that the leaks revealed Western hypocrisy about doping; they downplayed and disparaged the idea of Russian state involvement in the hack.

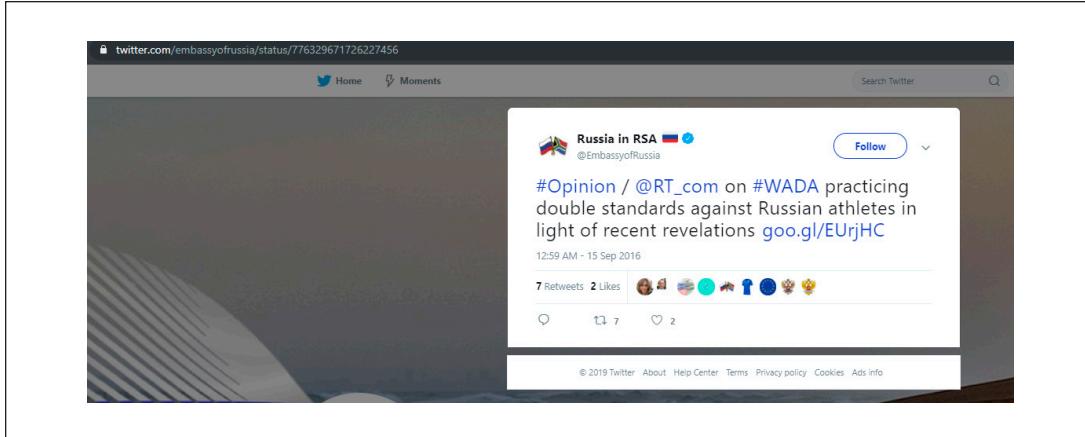


Figure 51. A tweet from the Embassy of Russia in South Africa.

As other disinformation researchers have noted, state media properties and IRA Twitter accounts (e.g., @nataturn¹⁹²) noted the WADA hacks, amplifying them to journalists to solicit further coverage. The Digital Forensic Research Laboratory's investigation into the WADA narrative also uncovered a Medium post about the issue written by prominent IRA troll Jenna Abrams.¹⁹³

Fancy Bear had more social engagement than DCLeaks, but again, its primary influence was through pickup by Russian state-sponsored media and Western media attention.

Doping vs Money, Who Wins?

C. REEDIE

WADA is such an independent agency, a great selfless organization living only on donations. Right? Oh, no, you can't be that naïve.

WADA is among those corrupted bastards, such as Clinton Foundation. WADA's head Craig Reedie always claims always complains about absence of donations and gets donations whenever he needs them.

Just recently a group of anonymous hackers hacked the WADA database and it turned out that there is more than one questionable case of rules violation.

Figure 52. Jenna Abrams' Medium post about the WADA hacks.

Foul Play

The final folder involved in this cluster of Fancy Bear hack-and-leak operations is Foul Play, which appears to have served as a site for editorializing the content in the sports hacks. The Facebook Page was a mere fragment; the folder contained no content other than two images (likely the banner and profile pictures, both uploaded on October 21, 2016).

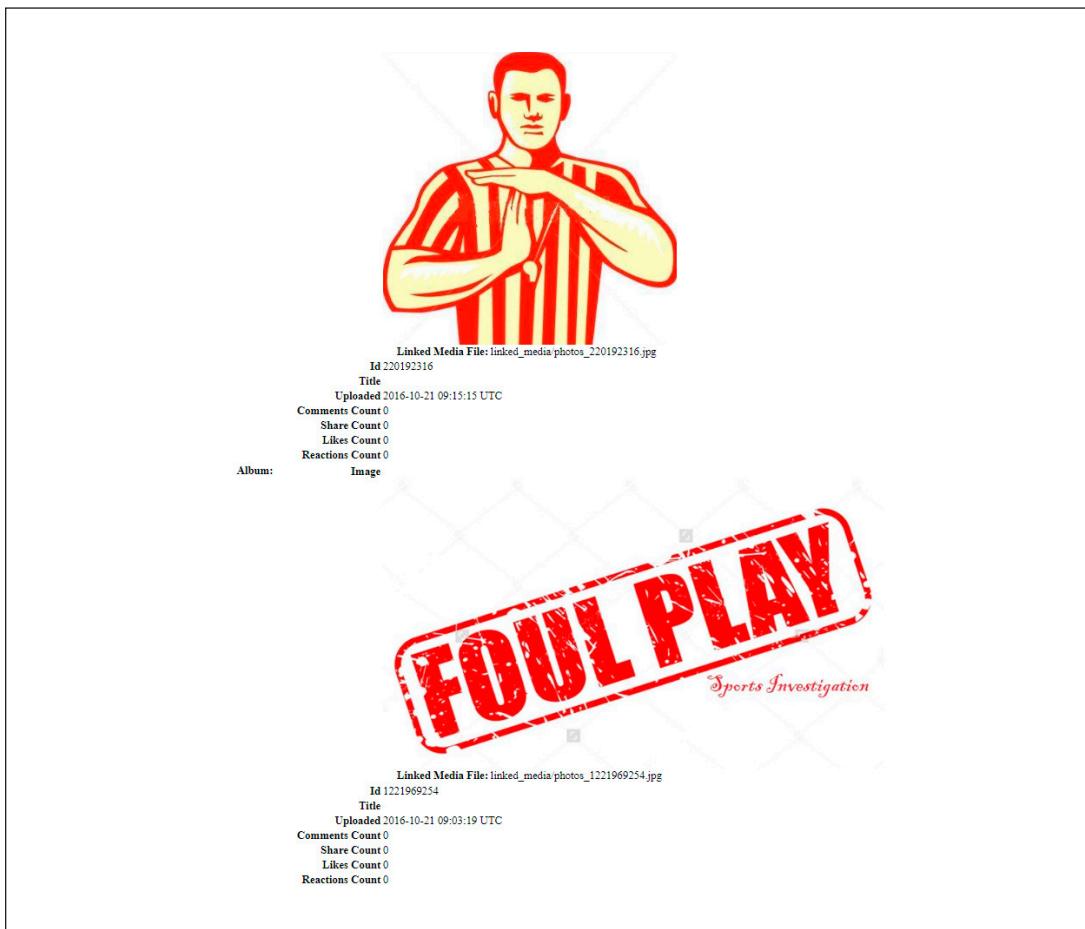


Figure 53. The banner and profile images associated with the Foul Play Page, identical to content that appeared on the still-live WordPress site.

However, the images and Page name match an external website with the same name begun in November 2016 that remains up. The About Page reads:

We represent a group of independent sports journalists who pay attention to the serious problems in today's sport. Unfortunately, nowadays sport has turned into a political tool. Cases of corruption and numerous scandals around different sports organizations and sports officials shouldn't be left unnoticed. Our goal is to unveil the lies. We stand for clean sport and for its noble role to unite people from all over the world.

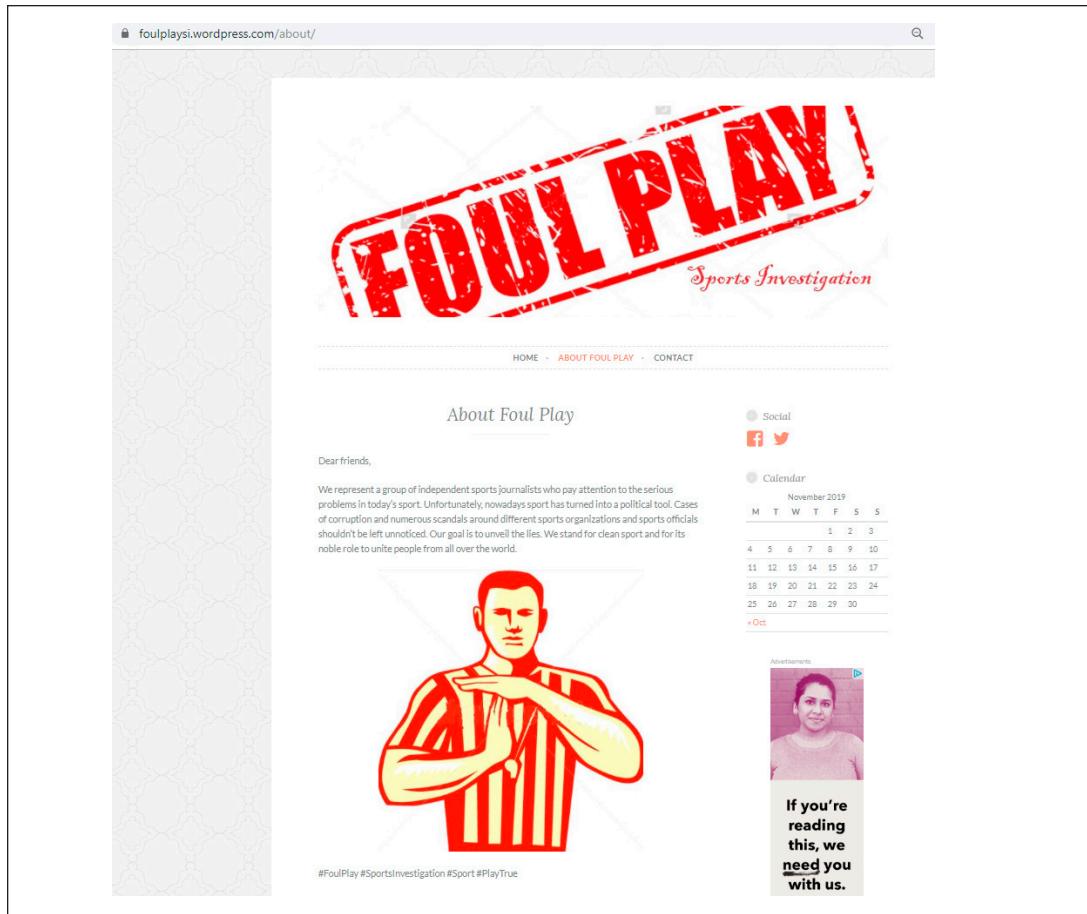


Figure 54. The About page of the Foul Play website.

The website links to Twitter account @FoulPlaySI,¹⁹⁴ created in Nov 2016, which is still live but dormant and has 143 followers. The website also links to a Facebook page, now removed, that was likely the Foul Play Page in this data set folder.¹⁹⁵

The website has an email address, foulplaysi@yahoo.com, which is also attached to a Medium account¹⁹⁶ that appears to repost content from the website. For example, the Medium account's Featured post echoes the About Page copy, adding four hashtags: #FoulPlay, #SportsInvestigation, #Sport, and #PlayTrue. Some of the Medium content appears to have been plagiarized from the BBC and other news sites. However, these posts are mixed in with original content that references Fancy Bear on two occasions: in a post from July 6, 2017,¹⁹⁷ and another on July 11, 2018¹⁹⁸ that defends Russia's hosting of the World Cup. That post was republished verbatim¹⁹⁹ on July 13, 2018, on wideshot.co.uk, under the byline of "Andy Holmes,"²⁰⁰ who also has a stub Medium profile reminiscent of other personas.

The Facebook image uploads for Foul Play have no engagement, and CrowdTangle notes sparse engagement (and a mere three Shares) on the WordPress and Medium content. It appears that the account owner created at least one message board account to share the content, but that too does not seem to have generated much engagement.²⁰¹

Stolen Football Holiday

July 11, 2018 · FoulPlay



Currently, 12 Russian cities host one of the main sport events of the quadrennial – the World Cup. A holiday, the national teams are being prepared for several years. In turn, the host country (or countries) strives to host this event at the highest level, prepares infrastructure, builds stadiums and provides security. This is all for the only one purpose – to allow millions of football fans to enjoy the unforgettable atmosphere of the championship, the spirit of competition and the unity of nations.

Russia has done everything possible and even a little more to put all this into practice. Thousands of fans arrived in this country, even in spite of the fact that the governments of a certain number of countries had called for a boycott of this event several months before the championship. Amid growing tension between Moscow and the European Union, British journalists and politicians tried to intimidate European citizens, sharing fake information about the inhumanity of Russian people, about poverty, about inability of this country to hold events of such level. No British official has visited a single match. So much the worse for them. Already now, at the semi-finals stage, the World Cup 2018 broke several sports records, gave us a series of very tough matches (not considering the match between teams France and Denmark, of course), shocked by Germany's inability to pass the group stage, and also allowed to see the real emotions of Panama national team's fans, who scored a historic goal against England.

Figure 55. A Foul Play Medium post defending Russia's hosting of the World Cup.

Throughout the GRU hack-and-leak operations, we observe activity from myriad actors with affiliations with Russia, in both the influence and cyber intrusion realms: hack-and-leak activity, including online entity creation to drop the leaked material, by the GRU; narrative framing and coverage, with disciplined messaging, by Russian state media; and promotion of the contents via IRA-attributed social media accounts—which also then participated, on all major social platforms, in pushing the narrative that the GRU hack was really a leak by murdered DNC staffer Seth Rich.

This same multi-entity activity appears in another hack-and-leak operation that we observe in the Facebook data set, involving an actor many suspect is attributable to the GRU: CyberBerkut.

Southern Front | Южный Фронт and Cyber Berkut

The Southern Front GRU-attributed Page claimed to represent CyberBerkut, a Russia-aligned hacker group with strident anti-Kyiv and anti-EU views that came into existence in the wake of Euromaidan. In the following section we review the activity of Southern Front and consider the evidence for and against linking it (and hence the GRU) with CyberBerkut. It is ultimately unclear whether or not this connection is genuine or an elaborate simulation.

First, it is important to note that, although CyberBerkut purports to be a Ukrainian entity—their shield features Ukrainian colors, and they take their name from the Ukrainian riot police who clashed with protesters during Euromaidan—they pursue a distinctly pro-Russian agenda. In tone and ideology they resemble a hacker-collective version of Antimaidan (see appendix). This has led many to assume that they are supported by or tied to Russian security agencies. The cybersecurity firms ThreatConnect and CrowdStrike have expressed confidence that CyberBerkut is connected to Russian intelligence, and in 2018 the UK National Cyber Security Centre asserted that CyberBerkut is “almost certainly” working within the GRU.²⁰² Other cybersecurity analysts argue that it is not necessary for CyberBerkut to be directly tied to the GRU to be useful to it.²⁰³ In any case, CyberBerkut has at every step aligned its actions with other Russian active measures in Ukraine.

These actions have included “distributed denial of service” (DDoS) attacks against Ukrainian and NATO computer systems,²⁰⁴ “tainted leaks” of fabricated documents intended to humiliate or undermine critics of the Russian government,²⁰⁵ and a multipronged hacking operation into Ukraine’s election systems prior to the 2014 presidential election.²⁰⁶ In addition, CyberBerkut has used its social media channels to spread disinformation and publish the results of its activities. At one time, the group was active on Facebook, Twitter, and the Russian social networks Vkontakte and Odnoklassniki. Of these pages, only those on Twitter and Vkontakte are still accessible (though dormant). CyberBerkut has also maintained its own website,²⁰⁷ where it posts “leaked” documents and diatribes against the US, NATO, and the EU. The group has not made any public announcements or published any materials since October 2018.

The Southern Front Facebook Page was active from April 13 until August 17, 2018. The name Southern Front, which is not found on other CyberBerkut pages, is likely a reference to the Soviet Union’s Southern Front in the Second World War, which encompassed Southern and Eastern Ukraine—the region CyberBerkut claims to be defending from Western interference.²⁰⁸ Over this period, Southern Front published approximately 20 discrete posts. Three of these posts were related to significant operations that CyberBerkut, via its primary website, claimed to have conducted:

- A “leak” of documents accompanying allegations that the US was working with the Ukrainian army to conduct a false flag operation in the Donbass using radioactive waste (August 15, 2018).
- A “leak” of documents and recordings purportedly showing that the Ukrainian government was gathering “Kompromat” on the Orthodox church (June 25, 2018).
- A long post intended to refute an investigation by the Bellingcat team related to the MH17 Malaysia Airlines disaster.

Інформаційно-довідковий матеріал про кількість іноземних інструкторів з підготовки о/с ЗС України							
	ШІМБ:	125 військово-тренувальний центр м.Бердичів	Навчальний центр ССнО м.Хмельницький:	УТрим.:	194 військовий центр с. Старичі	Центр розмінування (м. Кам'янка-Подільський):	
США	307	(39 – ІМТГ-У (California National Guard, US EUROCOM – Національна гвардія штату Каліфорнія (40), багатоділовими США в Європі); 195 – 3/15 IN Bde (механізовані бригади – Форт Стоарт, штат 42 – GLS (Global Linguistic Solution – фірма переважною – Головний офіс в Косово, філії Бонд Спш (Бондспіл)); 1 – 66 MI Bde/CI (Бригада інженерної розвідки – м. Вісбаден, федерація земель Гессен, Німеччина); – 80 CA (центр з логістики штабською адміністрацією та підтримки – м. Трайбенберг, федерація земель Баден-Вюртемберг, Німеччина); 3 – 18 ABN Corp (політично-дипломатичний корпус – Форт Брезз, штат Пенсільв'яна, США); – CALM (центр узасобів збройного бойового десанту – Форт Полк, штат Джорджія, США); 0 – AWG (група єдиних десантів збройної елізи – Форт Г.Макдугал, штат Меріленд, США). 22 – Visitors США)	44 (інформація щодо належності до підрозділу має граф обмеження доступу)		11 (Army Security Assistance Training Management Organization – Організація підготовки з програмами з підготовки в галузі безпековій допомоги ЗС США)	376	
Канада	185	(3 Army Bde – механізовані бригади СВ Канади, м. Вінніпег, провінція Кебек, Канада)		4	20 оперативний центр (Метріз), м.Лінчінз, Страффордшир) 4 військово-спеціальні у стану перед 21.05.16.	209	
Велика Британія	1	(РІНQ – Постійний об єдиний штаб)				1	
Литва	3	(механізовані бригади "Західний віск" – с. Рукла, Йонавський район, Литва)	16 (інформація щодо належності має граф обмеження доступу)			19	
Естонія			9 (інформація щодо належності має граф обмеження доступу)			9	
Латвія			6 (інформація щодо належності має граф обмеження доступу)			6	
Загалом	496		75	11	20	606	
ЗСУ	0		68 - кваліфікаційний курс спеціальних операторів (23.11 – серединя травня 2016, 29 курсантів – збірна група ССнО); - курси підготовки місіонерів (01.03-серединя травня 2016, 39 курс., роз. роз. 8 п СнП).	24 Курс "Застосуванням сили" (18-29.04.16). 29 курсантів – збірна група ССнО;	76 Курс підготовки санінструкторів (21.04-05.05.2016). До підготовки започатковано представництва різних частин ВСП ЗСУ.	0 Курс зі збору зеканів та Курс засвоєнням СВП (11.04-02.06.2016). До підготовки започатковано особовий склад Центру.	118
Загалом	496		14	143	28	738	

Figure 56. A leaked document on Southern Front purporting to give the identities and locations of groups of US military instructors in Ukraine. Circled in red is information related to the allocation of instructors; CyberBerkut claimed that this was evidence of an impending chemical attack.

The posts on the Southern Front Page related to these three operations were abbreviated versions of those appearing on CyberBerkut's website; the Southern Front posts did not include all of the items offered as "evidence" on the website and used entirely different text. Likewise, the Twitter account linked to CyberBerkut posted three times over this period about the same three operations. We do not further analyze these operations in this report because they are publicly available and the additional Facebook material does not constitute any new evidence of CyberBerkut's methods.²⁰⁹

АКТ ПРИЙОМУ-ПЕРЕДАЧІ МАТЕРІАЛІВ

Державна інспекція ядерного регулювання України, в особі Плачкова Григорія Івановича, Голови Державної інспекції ядерного регулювання України, та генерал-лейтенанта Збройних Сил України Луньова Ігоря Васильовича, Командира військової частини А0987, склали цей Акт від «02» квітня 2018 року про передачу Командуванню Сил спеціальних операцій Збройних Сил України 1 (одного) контейнера з обробленими радіоактивними відходами з ліквідованого сховища «Вакуленчук».

Здав
Голова Державної інспекції
ядерного регулювання України
Плачков Г.І.

«2» квітня 2018 р.

Прийняв
Командир військової частини А0987
Луньов І.В.

«2» квітня 2018 р.

Figure 57. A leaked document on Southern Front purporting to show the transfer of “radioactive waste” to be used in a chemical attack in the Donbass. CyberBerkut/Southern Front alleged that the Ukrainian military was working with US military instructors to create a “provocation” by dumping this radioactive waste in the Seversky Donets-Donbass Canal, which supplies the Donbass region with water. This “leak” came during a period in which Ukraine and Russia both accused the other of plotting chemical attacks in the region.

The rest of the posts on Southern Front appear to be unique to this Facebook Page. This content can be divided into several categories:

- CyberBerkut iconography
- A post related to the Skripal Incident
- Posts related to Telegram and Cloudflare’s DNS service
- A repost of a Fancy Bear leak
- 9/11 conspiracy videos
- A leaked conversation between a far-right Ukrainian figure and a policeman
- A post mocking Ukrainian President Petro Poroshenko

While it is difficult to discern the motivation behind several of these posts, such as those related to DNS and 9/11 conspiracies, others provide a link to GRU-attributed materials elsewhere on the

internet. On April 27, 2018, Southern Front posted about Fancy Bear's release of leaked emails related to problems encountered by the Swiss company Berlinger with their BEREK-KIT Geneva, a drug-testing kit used by WADA.²¹⁰ This post included two images—a stock image often used in articles about Fancy Bear and a screenshot of an email sent between officials at the Swedish Sports Federation—as well as a Status Update: “#FancyBear’ Berlinger & Co. AG Hastily Tried to Conceal the Problem with BEREK-kit Geneva.”²¹¹ If Southern Front does in fact represent CyberBerkut, this post appears to be the only time content was cross-posted between the groups, despite the fact that, as ThreatConnect points out, they often target the same entities.²¹²

From Jan Engström (RF) <Jan.Engstrom@rf.se>☆
Subject VB: Important notice: Correct closing of BEREK-KIT Geneva anti-doping sample bottles
To Jenny Schultze (RF) <Jenny.Schulze@rf.se>☆, Peter Ström (RF) <Peter.Strom@rf.se>☆
2018-01-28 오전 1:02

Utgårt att ni fägt detta, men utfall int.....

Jan Engström
RIKSIDROTTSFÖRBUNDET
Antidopingavdelningen
+46 70 671 68 53 (mobile)
jan.engstrom@rf.se
www.rf.se
Besöksadress
Skansbronsgatan 7, 118 60 Stockholm
Postadress
Box 11016, 100 61 Stockholm
Sverige

folj oss på
Facebook

Från: Info Special [mailto:info.special@berlinger.com]
Skickat: den 26 januari 2018 17:53
Till: Info Special <info.special@berlinger.com>
Ämne: Important notice: Correct closing of BEREK-KIT Geneva anti-doping sample bottles

Dear Sir, Dear Madam

The BEREK-KIT Geneva, a product for use in anti-doping tests that has been developed and is manufactured by Berlinger Special AG of Switzerland, was launched in a new and further refined version in Autumn 2017. Some 60 000 kits of these security bottles have already been delivered, and are in use all over the world. A small number of reports have been received in the last few weeks – particularly from doping sample testing laboratories – of BEREK-KIT Geneva bottles containing doping samples that are still open or are not fully closed. Berlinger Special AG has responded to these reports immediately, and has also been able to examine some of these bottles at the laboratories involved. These investigations have revealed that, the bottles concerned were not correctly closed after the sample had been provided.

In view of this, we would like to emphasize once again, with this communication and the video link it includes, that the security bottles in the BEREK-KIT Geneva must always be closed in full accordance with the handling instructions, which are included in every kit in printed document form. By ensuring that these bottles are closed correctly after the sample has been provided, you will ensure that the sample concerned will be valid, and that it can be either securely stored or safely transported to wherever it needs to go.

To offer you further assistance in handling the BEREK-KIT Geneva (or in providing your doping control officers and athletes with the instructions for doing so), we have produced a brief instructional video that details the correct bottle closing procedure. Please show this video to all your doping control officers and – if possible – to all the athletes who are required to provide an anti-doping sample before such samples are obtained.

You will find the video here: <https://www.berlinger.com/Index.php?id=376>

This video has also been supplied (in ten different language versions) to the Local Organization Committee of the 2018 Olympic Winter Games in PyeongChang, South Korea, to the International Olympic Committee in Lausanne, Switzerland and to the World Anti-Doping Agency in Montreal, Canada. All these organizations fully support our initiative to ensure the correct closure of the BEREK-KIT Geneva anti-doping security bottles of Berlinger Special AG.

If you have any questions or remarks on the video, or on the handling of our BEREK-KITS, please do not hesitate to contact us at info.special@berlinger.com.

Sincerely,
Andrea Berlinger

Figure 58. An email from an official at the Swedish Sports Confederation that was leaked by Fancy Bear and reposted on Southern Front.

The GRU has also been implicated in attempts to compromise the Spiez Laboratory, the Swiss lab charged with testing the nerve agent used to poison Sergei and Yulia Skripal in March, 2018.²¹³ The Spiez Laboratory was at the center of a significant disinformation push by the Russian Ministry of Foreign Affairs, which sought to reframe the Laboratory's findings in a way that exonerated Russia.²¹⁴ These claims were rejected by the Lab,²¹⁵ but this did not prevent the claims from spreading on RT and other pro-Russian outlets.²¹⁶ Southern Front joined the fray as well, posting a picture of the BZ molecule and a screenshot of an exchange on Twitter in which Spiez Laboratory, claiming that it could not comment on its investigation, appeared reluctant to reveal its findings.

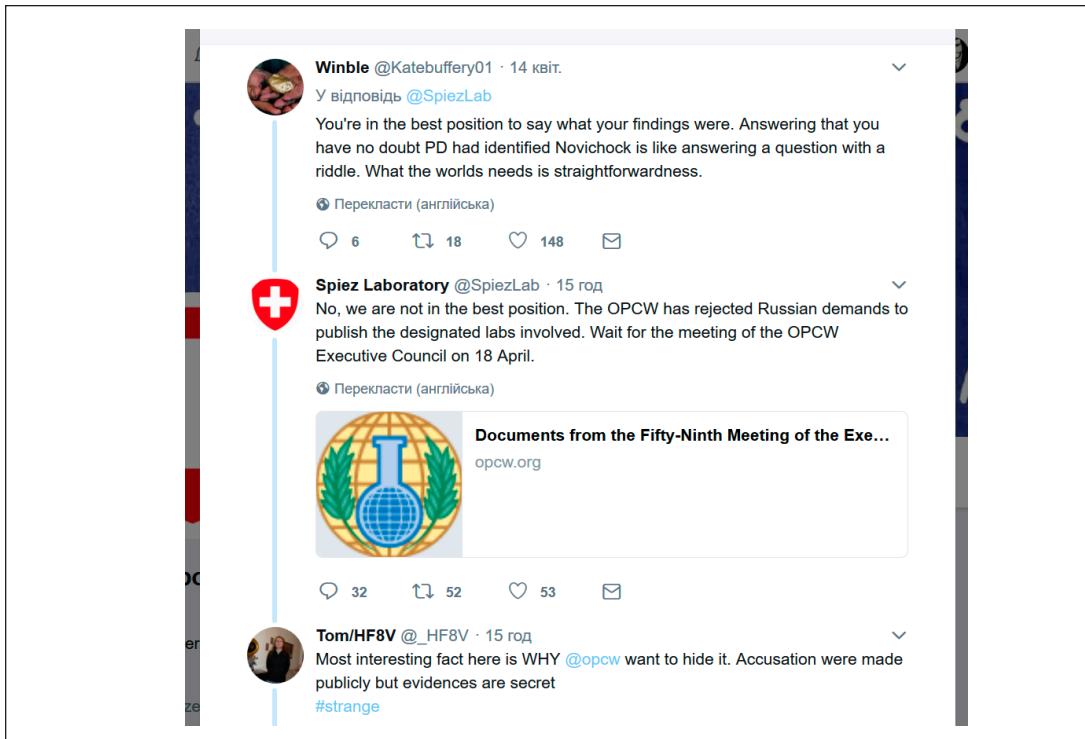


Figure 59. A screenshot of an exchange on Twitter that appeared on Southern Front. The account language for the logged-in user is Ukrainian.

As before, this content is unique in CyberBerkut social media activity, and if Southern Front is connected to it, this would be another instance of CyberBerkut publishing on matters related to other GRU operations—in this case not a hack-and-leak operation but the attempt to compromise the Spiez Laboratory.



Figure 60. An image posted by Southern Front borrowing the aesthetics of the hacktivist group Anonymous. This image appeared alongside CyberBerkut's reply to Bellingcat's investigation into Oleg Ivannikov.²¹⁷

These items stand out because CyberBerkut's website and other social media pages post content almost exclusively about Ukrainian themes. There is no mention of the other issues that dominated Russian influence operations happening concurrently: the war in Syria, the Skripal affair, US election interference, WADA and doping scandals, etc. It is important to remember that CyberBerkut purports to be Ukrainian, so that focus makes sense. CyberBerkut also hews closely to a "house style." This style is, to be sure, stridently anti-Western but typically does not deviate from CyberBerkut's core aesthetic, which does not include posting Anonymous-inspired images and 9/11 conspiracy videos. The posts that are unique to the Southern Front Page arguably "break character" by commenting on issues that have little to do with Ukraine. This argues in favor of a weak connection between Southern Front and CyberBerkut itself, despite their ideological alignment.

Thus, based on Facebook's attribution of the Southern Front Page to the GRU, we assess that there are two likely scenarios:

1. A weak connection between Southern Front and CyberBerkut: in this scenario, the GRU set up a Page purporting to represent CyberBerkut on Facebook in order to spread the results of its operations, which were undoubtedly useful to the Russian government, to a wider public in English and Russian. Although the goals and interests of the two are aligned, they did not work together on Southern Front.
2. A strong connection: this scenario provides more evidence that CyberBerkut is supported by, or part of, the GRU, something ThreatConnect has posited.²¹⁸ In this scenario, Southern Front might have been the CyberBerkut Facebook Page, since taken down, that they refer to in their header:



Figure 61. The header from CyberBerkut's Twitter profile; note the link to a Facebook Page.

It is clear that CyberBerkut has had trouble staying up on Facebook. Southern Front might have been merely its most recent effort to establish a presence on the social network, since it is unlikely that it did not have a Page for the first four years of its existence. Evidence that this Page, which is present in CyberBerkut's iconography and their official website, was in fact Southern Front would support the strong connection scenario.

Engagement across “Southern Front” was minimal; most of its Posts received no engagement at all. The highest number of interactions any Southern Front post received was four—the number of reactions received by the Anonymous image shown above. This is in distinct contrast to CyberBerkut’s VK and Twitter pages, on which posts routinely attracted hundreds of Likes and dozens of retweets, respectively.

What was the aim of creating Southern Front as a Facebook Page? The GRU’s continual hack-and-leak operations are well known; what it needs is a way to get the material from these leaks—and the broader narrative they support—into the media ecosystem. After the seizure of fancybear.net by the FBI in early 2018, the GRU might have been looking for another way to publish compromising material and inject it into an organic community that would propagate it more widely. The community that had sprung up around CyberBerkut might have seemed like a good solution to this problem. Whether the Page’s failure to get engagement was a result of disinterest or incompetence, this approach seems likely to be attempted again.



6 CLOSING NOTES AND FUTURE THREATS

When we assess the data set holistically, we observe a series of tactics repetitively deployed—to varying degrees of success—with the intent to influence narratives of strategic interest to the Russian state. Throughout the data set, for a range of countries and across a range of issues, we observe the development of media, civil society, and pseudo-academic fronts; the leveraging of purportedly independent media that acts, at best, as an uncritical recipient of contributed pieces; and the construction of fake authors and fake grassroots amplifiers to execute both the creation and amplification of the state’s point of view.

6.1 Assessments Related to Prior Data Sets

The existence of this data set invites certain comparisons to another Facebook-attributed data set: that of the Internet Research Agency. While research into the degree of coordination and content overlap is ongoing, we offer the following initial impressions.

First, the similarities: the GRU and IRA were operational at the same time. They shared some common topical areas of activity, most notably Syria, Ukraine, and race relations in the United States. They shared some similar operational approaches related to the creation of fake media entities, fake personas, and fake amplification patterns.

There are also several significant divergences in their approach. In the GRU data set, we observe that Pages were created and run within a distinctly short timeframe, often with frenetic posting patterns. They were spun up in response to a geopolitical event or provocation—including to serve as a public drop for hacked materials. The effort expended on attracting audiences, even via obvious strategies like running ads, was conspicuously minimal; the marked lack of engagement is indeed somewhat perplexing. There are a few possible explanations for this: the first is that social influence was not the focus nor the goal of GRU activity, which was primarily concerned with media hacking; this would suggest that the social pages were the backstop to the journalistic narrative operations rather than the other way around. A second explanation is that they didn’t fully understand the dynamics of social platforms. A third is that they were simply ineffectual or incompetent in their execution.

The IRA, by contrast, developed sustained audience relationships over a period of years, building their audiences methodically with a collection of strategies, including ads. They inflected their content with precision, using audience segmentation techniques regularly deployed by social media agencies. Although they created their own fake media properties, they also widely leveraged authentic domestic aligned media. They used a more modern form of memetic propaganda—concise messaging, visuals with high virality potential, and provocative, edgy humor—rather than the narrative propaganda (long-form persuasive essays and geopolitical analysis) that is most prevalent in the GRU material. Perhaps most importantly, the IRA infiltrated communities and masqueraded as members of the groups they were targeting—traditionally an activity far more reminiscent of an intelligence agency than a marketing entity. There is evidence that the GRU attempted this as well, with Baltimore is Everywhere, but it does not seem to have integrated its personas deeply into the social circles to which they purportedly belonged.

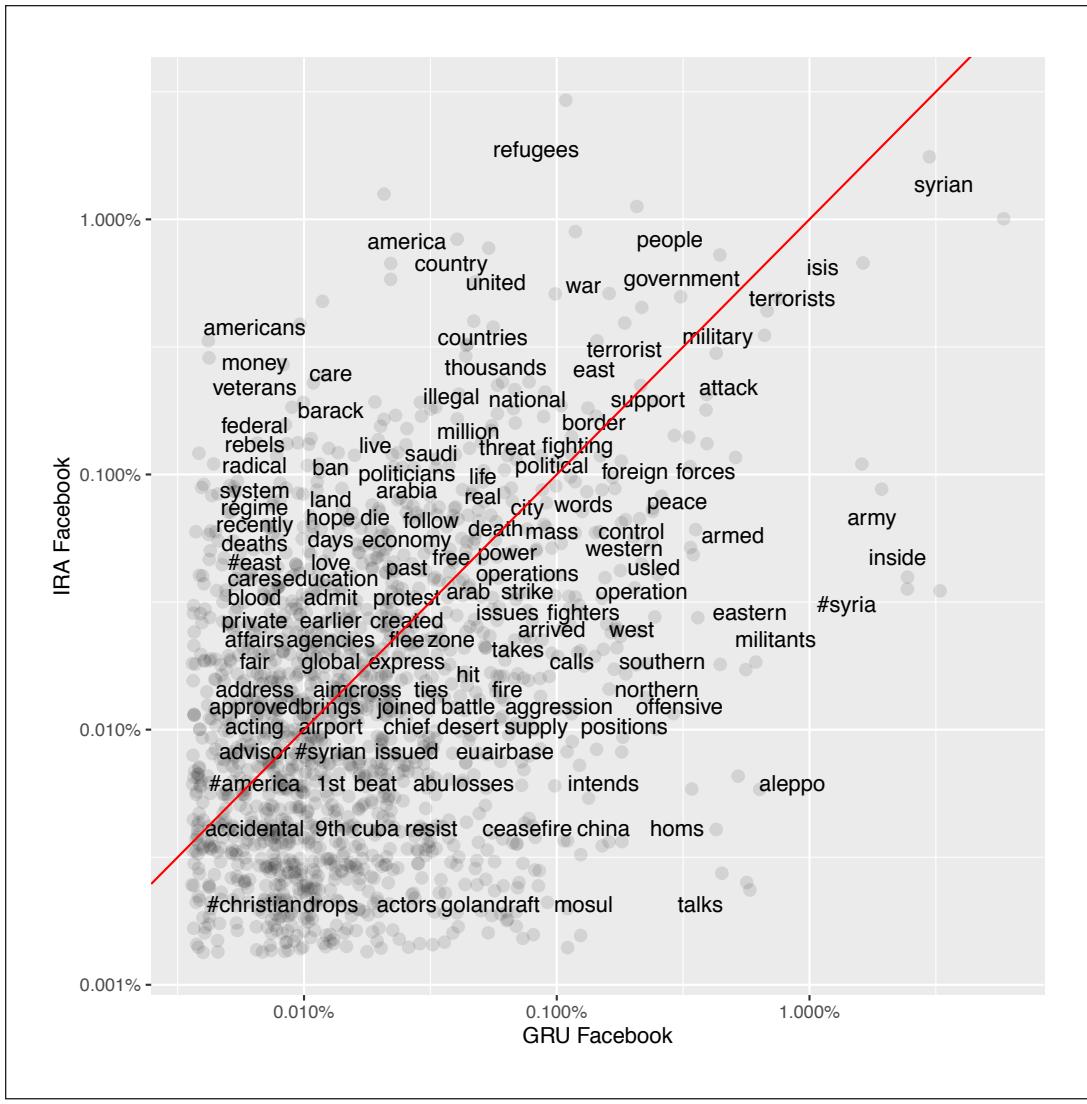


Figure 62. A comparison of word frequency across IRA and GRU Facebook posts about Syria. Words farther from the red line are more unique to the IRA or the GRU. The GRU Facebook posts about Syria ($n=2,013$) started in November 2015 and ended in August 2018. They are primarily—though not exclusively—from Inside Syria Media Center. The IRA Facebook posts about Syria ($n=931$) began in June 2015 and ended in August 2017. GRU posts typically describe battles or events in the Syrian conflict. IRA posts are more sensationalist, discussing the implications of Syria's war for the US and Europe.

It is in assessing the reach and impact of narratives that we observe that these two entities combined offer Russia a powerful information operations capability and present an ongoing future threat. The IRA's modern tactics and millennial employees place it on the cutting edge of socially disseminated propaganda and influence: a number of its accounts had over 100,000 followers, its content was shared by reputable high-profile American influencers and media properties on numerous occasions, and it successfully incited in-the-streets protests. Its independent ownership offers it continued plausible deniability against accusations of state involvement that the GRU does not possess. However, particularly in the case of the US, the GRU hacking team successfully extricated the material from the Democratic National Committee

and Hillary Clinton campaign. That content, disseminated via WikiLeaks and then dissected and speculated upon by every major newspaper and television station in America, arguably had more of an impact on the US election than any social influence operation. While it remains unclear whether the IRA knew of the GRU dumps in advance, they did create and repurpose accounts to participate in the dissemination and narrative-shaping close to the time of their release. While we hesitate to make an assessment on deliberate coordination, we note two points: (1) there was not substantial overlap across the GRU and IRA activities in terms of unique hashtags nor driving users to the same websites, but (2) there appears to be tactical, topical, and temporal overlap between GRU and IRA activities, across multiple platforms, that warrant further research. Looking forward, if appropriately coordinated, the combined capability potential between the GRU (hacking; narrative laundering) and the IRA (subversive social influence; memetic propaganda) could result in significantly impactful information operations.

6.2 Research Limitations

This report and analysis is presented with the caveat that we are reliant on the attribution assessments of the social platforms, in this case Facebook. However, a number of their attribution assessments have been echoed in the Special Counsel's Report and in a series of indictments, suggesting that the attributions underlying this report have a high degree of accuracy.

Our assessments of other platforms are based on independent investigative processes followed by subsequent corroboration with their threat assessment teams wherever possible. Some had discovered fragments of the activity years back when it happened, and removed it. One challenge in the investigation process is that removed content is rarely archived or released publicly, and as such is not able to be fully incorporated into future research. Once these entities are removed, links that connect activities to other prior—or ongoing—operations are lost forever. Having a partial picture of an influence operation hinders researchers' ability to develop a complete understanding of malign activities. We therefore wish to reiterate that information sharing and collaborative research are necessary both to detect and to fully understand the scope of influence operations, and that we hope to see the appropriate frameworks for multi-stakeholder work continue to progress.



7 APPENDIX

7.1 Minor Operation: Antimaidan ukraine [sic]

The GRU-attributed Facebook data included a Page titled Antimaidan ukraine, although there was no content associated with this Page. While the data provided by Facebook does not allow us to draw any conclusions about the GRU's methods in this case, we can look to other pages and sites associated with Antimaidan to try to discern its motivation in creating the Page.

Some background on Antimaidan and related groups and Pages may be helpful. "Antimaidan" is an epithet adopted by a number of protest groups and initiatives united around a core set of ideas: rejection of the Euromaidan movement, the current Ukrainian government, and what is perceived as "Western" influence in Russia and Ukraine. The first protests to identify themselves as Antimaidan occurred in Eastern Ukraine in late 2013 and intensified after the flight of Yanukovych, before the full-scale rebellion that broke out in the Donbass in April 2014.²¹⁹ Around that time the first Russian organizations calling themselves Antimaidan began forming, including, most notably, a group led by Kremlin allies Dmitry Sablin, Alexander Zaldostanov, and Yulia Berezhkova.²²⁰ This group applied the concept to domestic matters, using the pretext of thwarting a potential Maidan-like movement in Russia in order to attack critics of Putin and independent political forces in Russia.²²¹ Thus, "Antimaidan" could be taken, depending on whom you asked, to mean a return to the pre-Euromaidan Yanukovych government, or the incorporation of Eastern Ukraine into Russia, or opposition to liberalization in Russia. Because it is used by groups of such diverse origin, holding such diverse views, Antimaidan is perhaps better understood as a concept than as a protest movement—but there is a degree of ideological unity binding the various groups.

What we can observe from other authentic Antimaidan accounts on Facebook and Twitter is that there is a core group of websites, revolving around the website [antimaidan.ru](#) and a VKontakte (VK) Antimaidan profile, that generate content and images for the others, including those writing for non-Russian audiences.²²² The extent of this network awaits investigation, but it is clear that, while the contours of the narrative shift with each account and target audience, there are explicit connections leading back to this core.

It is possible that the Antimaidan ukraine Page that Facebook attributed to the GRU was created with the intention of adding another node to this network. The name "Antimaidan ukraine," for instance, would put it in the company of a handful of other social network profiles with this name: the words "Antimaidan ukraine" do not appear together very frequently in English, perhaps because the first assumes the second. The English- and German-language Antimaidan profiles mentioned above link to a dormant YouTube channel called "Antimaidan Ukraine," which was active from 2014 to 2015 and appears to have been set up to support these accounts.²²³ This channel predominantly posted translations of videos—some of them amateur, some from Russian state media—into other European languages, and from here they were shared on Twitter and Facebook. There are also profiles identified by "antimaidan ukraine" and "antimaidan_ukraine" on Facebook, VK, and Odnoklassniki—although these profiles use this phrase in their handles only and are not titled "Antimaidan Ukraine."²²⁴

All of these pages are in Russian, and all of them advance versions of the Antimaidan narrative described above. It is possible that the Antimaidan ukraine Page was created for the same purpose. If so, the GRU's goal may have been simply to inject their own content into a large, and, in many cases, seemingly organic network of pro-Russian and anti-Western accounts already spreading content in various languages in order to delegitimize the government in Kyiv.

7.2 Residual Pages

A number of the Pages in the Facebook data set contained minimal activity, and research revealed no attributable presence on the broader web. We mention these Pages here.

- A Page named **Anal**, for reasons unknown, which contains one post with a URL pointing to <http://mirkavkazu.ru/>. The post was created June 18, 2015, and had no engagement. The title of the single Share on the Page curiously does not appear to be linked to the article that appears below it. The title reads, “Баку откроется филиал Первого Московского государственного медицинского университета имени И.М.Сеченова,” which translates into “Baku branch of the First Moscow State Medical University named after I. M. Sechenov”—an event that appears to have happened in September 2015 based on press coverage that remains online.

The summary of the post, however, is a headline in Russian: “Россия и Армения планируют создать совместный спасательный центр гуманитарного реагирования”; translated, it reads, “Russia and Armenia plan to create a joint rescue center for humanitarian response.” This text is the precise headline of a May 18, 2015 post on a site with the same domain as the URL, which goes into specifics around the rescue center’s location.²²⁵

The Mirkavkazu website itself appears to have largely stagnated after 2015, with no new posts. It is currently down, but visible in the Internet Archive Wayback Machine. There is what appears to be a Facebook Page²²⁶ (Конкурс молодых журналистов, “Young Journalists Contest”), related to the domain, that is still live but dormant, with 75 Likes. It focuses on a young journalists’ competition that the center appeared to regularly run. Curiously, and similarly to activity throughout the GRU-attributed data set, most of the posts appear to be from two date clusters, on October 8 and October 12, 2015. There is a VK club focused on the same competition.²²⁷ There is also a still-live but dormant Facebook Group dedicated to the Mirkavkazu center, featuring photos from what appears to be a reception for one year of the competition. The Group is Public, and posts as well as accounts participating can be observed.²²⁸

In 2017, after being dormant for over a year, the “Young Journalists Contest” Page had one post that contained no text, simply a link directing people to another Facebook Page, InfoRos.²²⁹ As discussed previously in this white paper, InfoRos has been associated with GRU Unit 54777.

- A Page by the name of **Babygone**, which may be a reference to a region in St. Petersburg, Russia. The Page had one post from June 17, 2015, which was an image of Monument Valley, Utah.
- A Page called **Conflict Zone**. This Page had one post from 2015, which referenced (in English) a story about a Russian pilot who was rescued after his plane was shot down near the Syria-Turkey border.²³⁰ The post linked to conflictzone.info, which is now down.²³¹ An article from conflictzone.info about Canada slowing down its intake of Syrian refugees was once shared by @balaban_off.²³² That user is the only follower of @politespb, the Twitter account that appears to be associated with another Page in the set, Polite People of the Capital of Culture; these may be two distributor accounts.
- A Page called **Mycompany**, containing one photo, uploaded in 2012, of search results for phone numbers in Megafon (a Russian telecommunications provider) in a browser window. There was a scandal in late 2011 in which Megafon users’ SMS messages could be read because of a leak, but there may be no connection.

- A Page called **Polite People of the Capital of Culture** that appears to be a promotional Page for a museum. There are images of a Saint Petersburg photo booth tourist attraction and a hashtag for visitors: #politespb. The museum appears to be the Military Historical Museum of Artillery, Engineers, and Signal, which is owned by the Ministry of Defence.²³³ There were a few social media accounts, including a Twitter handle @PoliteSPB.²³⁴ People who appear to be ordinary visitors did post selfies of themselves in the museum photo attraction to Instagram under the hashtag #politespb.
- A Page called **Sadam Alwahdi**. This Page had a small number of photos, including a slightly altered image featuring the logo of authentic online community The Anonymous Writer.²³⁵ The other image is a cropped photo of Budapest's Anonymous Statue. There was one post from March 14, 2017 (in Arabic) expressing consternation that Iran and Russia were not invited to participate in the global coalition against the Islamic state. We were not able to find a social media account for Sadam Alwahdi, or other variants of the name.
- An additional four pages contained no content and turned up no presence at all elsewhere online. These included **Fdfxc**, **FozNews'**, **Music and Company**, and **Sdf**. Sdf may have been a reference to the Syrian Defense Forces.



ENDNOTES

- 1 All URLs in this report have been archived either on archive.is or archive.org.
- 2 “What is the GRU?”, *The Economist*, September 11, 2018, <https://www.economist.com/the-economist-explains/2018/09/11/what-is-the-gru>.
- 3 Robert S. Mueller III, Report on the Investigation into Russian Interference in the 2016 Election, vol. 1, (Washington, D.C.: US Department of Justice, 2019), 14.
- 4 Adam B. Ellick and Adam Westbrook, “Operation Infektion: Russian Disinformation: From Cold War to Kanye,” November 12, 2018 in *The New York Times*, video, <https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html>.
- 5 J. Michael Waller, *Strategic Influence: Public Diplomacy, Counterpropaganda, and Political Warfare*, (Washington, D.C.: Institute of World Politics Press), 160.
- 6 Dilip Bobb, “Book on KGB Unveils Russian Agency’s Ops in India During Cold War, Political Storm Ensues,” *India Today*, October 3, 2005, <https://www.indiatoday.in/magazine/nation/story/20051003-mitrokhin-archive-kgb-operations-in-india-during-cold-war-786931-2005-10-03>.
- 7 Mueller, *Report On The Investigation*.
- 8 Mueller, *Report on the Investigation*, 42-43.
- 9 Dmitri Alperovitch, “Bears in the Midst: Intrusion into the Democratic National Committee,” *CrowdStrike*, June 15, 2016, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.
- 10 Renée DiResta et al., “The Tactics & Tropes of the Internet Research Agency,” (Austin, TX: New Knowledge, 2018), <https://digitalcommons.unl.edu/senatedocs/2/>.
- 11 Philip N. Howard et al., “The IRA, Social Media and Political Polarization in the United States, 2012-2018,” (Oxford: Oxford Internet Institute, 2018), <https://comprop.ox.ac.uk/research/ira-political-polarization/>.
- 12 “What Is the GRU? Who Gets Recruited to Be a Spy? Why Are They Exposed So Often?”, *Meduza*, November 6, 2018, <https://meduza.io/en/feature/2018/11/06/what-is-the-gru-who-gets-recruited-to-be-a-spy-why-are-they-exposed-so-often>.
- 13 Mark Galeotti, *Putin’s Hydra: Inside Russia’s Intelligence Agencies*, (London: European Council on Foreign Relations, 2016), https://www.ecfr.eu/publications/summary/putins_hydra_inside_russias_intelligence_services.
- 14 Mueller, *Report on the Investigation*, 14.
- 15 While the IRA did create seventeen known fake media domains—most notably blackmattersus.com—they did not emphasize bylined long-form content. Rather, the IRA’s preferred form of propaganda was a “digital native” internet-first memetic variety, designed to fit the preferred format of the social platforms upon which it was deployed.
- 16 Adam Entous, “The Rise and Fall of a Kremlin Troll,” *The New Yorker*, July 19, 2018, <https://www.newyorker.com/news/news-desk/the-rise-and-fall-of-a-kremlin-troll>.
- 17 Guy Faulconbridge et al., “West Accuses ‘Pariah State’ Russia of Global Hacking Campaign,” *Reuters*, October 4, 2018, <https://www.reuters.com/article/us-britain-russia-cyber-idUSKCN1ME1HE>.

18. Her Telegram account is <https://t.me/miralhijab>. Additionally, many of her articles in Arabic were reposted on sites like Iraq.dk. She appears to have had a WordPress blog as well, at <https://miralhijab.wordpress.com>, in which the author photo was a close-crop of a photo of film director Yamina Benguigui https://commons.wikimedia.org/wiki/File:Yamina_Benguigui.jpg.
19. <https://www.counterpunch.org/2018/01/05/ghosts-in-the-propaganda-machine/>.
20. <https://twitter.com/saidkhalaki>.
21. We elected not to link to this profile for privacy reasons.
22. <https://twitter.com/AJaunger>.
23. <https://www.counterpunch.org/2018/01/05/ghosts-in-the-propaganda-machine/>.
24. <https://twitter.com/SophiaMangal>. The Twitter photo appears to be a mirror image of a photo here: <https://www.remocontro.it/2018/11/13/ricordate-leroica-kobane-curda-turchia-alla-resa-dei-conti/>.
25. <https://medium.com/@sophiamangal>.
26. <https://www.quora.com/profile/Sophie-Mangal>. In one post she sought out a research collaborator, and at least one person, a World Bank Consultant, responded: <https://www.quora.com/What-is-the-text-of-Russian-draft-of-Syrian-constitution-completely>.
27. https://blog.twitter.com/en_us/topics/company/2019/further_research_information_operations.html.
28. <https://medium.com/@firassamuri>.
29. <https://money.cnn.com/2018/08/23/technology/facebook-twitter-syria-media-center/index.html>; <https://www.thedailybeast.com/alleged-russian-operatives-spreading-fake-news-sneak-back-onto-facebook>; Sam Thielman, “Kremlin Troll ‘Alice Donovan’ Reportedly Writing News As Recently As October,” *Talking Points Memo*, December 26, 2017, <https://talkingpointsmemo.com/muckraker/kremlin-troll-alice-donovan-was-criticizing-us-foreign-policy-in-october>; Donara Barojan, “Questionable Sources on Syria,” *DFRLab*, September 24, 2017, <https://medium.com/dfrlab/questionable-sources-on-syria-36fcabddc950>; Jeffrey St. Clair and Joshua Frank, “Ghosts in the Propaganda Machine,” *Counterpunch*, January 5, 2018, <https://www.counterpunch.org/2018/01/05/ghosts-in-the-propaganda-machine/>.
30. Note that there exists a real person named Jonivan Jones, who is a musician; this discussion does not refer to him.
31. <https://web.archive.org/web/20170311183454/http://theinformer.life/author/informer/>; <http://theinformer.life/author/jonivan-jones/>.
32. <https://medium.com/@jonivan999>.
33. We elected not to link to this profile for privacy reasons.
34. <https://medium.com/@crnagoranews/followers>.
35. <https://medium.com/@milkojeovic/unknown-hackers-attacked-several-montenegro-websites-ac7700660bcf>.
36. <https://www.globalresearch.ca/author/milko-pejovic>.
37. <http://www.forum-cg.ru/user?id=283370768685445>.

38. <https://muckrack.com/jelena-rakocevic/articles>.
39. Interestingly, several co-bylines in the Muck Rack profile appear to no longer be valid on the article sites as they currently appear.
40. <http://www.prnob.com/release/show/jelena-rakocevic-synaxis-of/44366>; <http://www.jetopisautomotive.com/mercedes/diplomatic.html>.
41. <https://muckrack.com/jelena-rakocevic/articles>.
42. <https://www.geopolitica.ru/en/person/adomas-abromaitis>; https://www.opednews.com/articles/Lithuania-s-new-chief-of-d-by-Adomas-Abromaitis-Military_Military-Madness_Military-Officers_Military-Spending--Foreign-190730-132.html; <https://www.eurasiareview.com/author/adomas-abromaitis/>; <https://europeansting.com/tag/adomas-abromaitis/>; <https://theduran.com/author/adomasabromaitis/>; <https://balticword.eu/iiiss-research-europe-cannot-defend-itself-without-u-s/>; <https://medium.com/intpolicydigest/trump-buys-lithuania-3b280b454938>; <https://katehon.com/person/adomas-abromaitis>.
43. <https://www.facebook.com/photo.php?fbid=116166895427719&set=a.116166922094383&type=3&theater>.
44. <https://adomasabromaitis.blogactiv.eu/author/adomas-abromaitis/>; <https://medium.com/@adomas333>. We had not reached out to Medium about this account prior to its 410 takedown.
45. <https://www.reddit.com/user/adomas333>; <https://www.pinterest.es/adomas333>.
46. <https://hotandspicyforums.com/memberlist.php?mode=viewprofile&u=312&sid=4dc08898f99e515f65aef08a194087b4>.
47. <https://www.counterpunch.org/2017/12/25/go-ask-alice-the-curious-case-of-alice-donovan-2/>; <https://www.counterpunch.org/2018/01/05/ghosts-in-the-propaganda-machine/>.
48. <https://theduran.com/duran-alice-donovan-tale-fbi/>.
49. <https://web.archive.org/web/20180722023604/https://en.insidesyriamc.com/>.
50. “Taking Down More Inauthentic Content,” Facebook, August 21, 2018, <https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/>.
51. We determined this by translating 10 randomly sampled Arabic headlines.
52. The primary site was https://web.archive.org/web/20171129200027/https://twitter.com/Inside_Syria, which is now down. <https://web.archive.org/web/20171129200027/https://insidesyriamcen.wordpress.com>, which appears to be a version of the site—though not all original articles appear in full on this site—is live. The last post on the wordpress version was on September 8, 2018.
53. <https://web.archive.org/web/20170610121543/https://en.insidesyriamc.com/about/>.
54. For more on internet discourse around the White Helmets, see <https://medium.com/@katestarbird/content-sharing-within-the-alternative-media-echo-system-the-case-of-the-white-helmets-f34434325e77>.
55. “Syria/Russia: School Attacks a Possible War Crime,” *Human Rights Watch*, November 6, 2016, <https://www.hrw.org/news/2016/11/06/syria/russia-school-attack-possible-war-crime>.
56. <https://off-guardian.org/2016/11/16/32360/>.
57. <https://insidesyriamcen.wordpress.com/tag/syrian-constitution/>.

- 58 https://web.archive.org/web/20171129200027/https://twitter.com/Inside_Syria.
- 59 St. Clair and Frank, “Ghosts in the Propaganda Machine.”
- 60 <https://web.archive.org/web/20180416051811/https://www.youtube.com/channel/UC2IyyQFqPQFCsn30n7DEleA>.
- 61 <https://t.me/insidesyriamc>.
- 62 This was the typical trajectory, but occasionally posts appeared elsewhere before appearing on ISMC. For example, one article appeared first on almasdarnews.com, and then the next day on ISMC, but with different headlines.
- 63 Original post: <http://en.insidesyriamc.com/2018/07/12/breaking-syrian-opposition-and-western-ngos-hire-actors-for-chemical-weapons-provocation/>. Full text here: <https://fromthetrenchesworldreport.com/syrian-opposition-and-western-ngos-hire-actors-for-chemical-weapons-provocation/229828>.
- 64 <http://iblagh.com/en/syrian-opposition-western-ngos-hire-actors-chemical-weapons-provocation/>.
- 65 <https://fromthetrenchesworldreport.com/syrian-opposition-and-western-ngos-hire-actors-for-chemical-weapons-provocation/229828>.
- 66 <https://fbreporter.org/2018/07/13/breaking-syrian-opposition-and-western-ngos-hire-actors-for-chemical-weapons-provocation/?fbclid=IwAR1tyY5fGnf8Oob9lp4i-AT7UFIhr0YEsbwZbT5aSA6eu2ajVdwOzBMAdyA>.
- 67 <https://www.21cir.com/2018/07/breaking-syrian-opposition-and-western-ngos-hire-actors-for-chemical-weapons-provocation/>.
- 68 <https://beastwatchnews.com/breaking-syrian-opposition-and-western-ngos-hire-actors-for-chemical-weapons-provocation>.
- 69 <https://kousdas.wordpress.com/2018/07/13/breaking-syrian-opposition-and-western-ngos-hire-actors-for-chemical-weapons-provocation/>.
- 70 <https://www.ghanagrio.com/news/478095-breaking-syrian-opposition-and-western-ngos-hire-actors-for-chemical-weapons-provocation.html>.
- 71 <https://southafricatoday.net/world-news/middle-east/breaking-syrian-opposition-and-western-ngos-hire-actors-for-chemical-weapons-provocation/>.
- 72 <https://quemadoinstitute.org/syria/>.
- 73 <https://www.globalresearch.ca/chemical-attack-in-idlib-duplication-of-scenario-in-eastern-ghouta/5584281>.
- 74 <https://www.facebook.com/pakistanidefence/posts/10154799372522663>.
- 75 Thielman, “Kremlin Troll ‘Alice Donovan.’”
- 76 Donie O’Sullivan, “Facebook Removes Syrian War Page It Believes Is Linked to Russian Intel, Twitter Keeps It Online,” CNN, August 23, 2018, <https://money.cnn.com/2018/08/23/technology/facebook-twitter-syria-media-center/index.html>.
- 77 e.g. <https://www.prnewswire.com/news/inside-syria-media-center>.
- 78 <http://archive.is/u9M8S>.

- 79 Example content: “The US presidential election this November will tell whether a majority of the US population is irredeemably stupid. If voters elect Hillary, we will know that Americans are stupid beyond redemption...”
- 80 <http://archive.is/u9M8S>.
- 81 Ben Farmer, “Russia Plotted to Overthrow Montenegro’s Government by Assassinating Prime Minister Milo Djukanovich Last Year, According to Senior Whitehall Sources,” *The Telegraph*, February 19, 2017, <https://www.telegraph.co.uk/news/2017/02/18/russias-deadly-plot-overthrow-montenegros-government-assassinating/>.
- 82 In 2016 the Page linked to all three of these domains, but in 2017 it linked only to cgna.me. The only one of these domains where archived content is accessible is cgna.me.
- 83 Twitter user @MilkoPejovic, a likely persona discussed in Section 5.1, shared this email address as well: <https://twitter.com/milkopejovic/status/787590042978058240>. The user’s associated Facebook Page is down: <https://www.facebook.com/milkopejoviccc/posts/402491153436407>. On Twitter, he frequently linked to CGNA content: <https://twitter.com/MilkoPejovic/status/806448402363977729>. Pejovic began tweeting in September 2015, and in November 2015 he began sharing CGNA content frequently. This suggests the CGNA Facebook Page appeared at least a year after CGNA website started.
- 84 <https://www.facebook.com/Infobalkani/>. The website associated with this Facebook Page is infobalkani.wordpress.com. The administrators for this Facebook Page are located in Bulgaria (4), Russia (1), and the US (1). Created in 2012, the Page is currently live but has had no posts since February 2017. The last two posts were about Russia—one about Gazprom, the other suggesting that the Syria crisis could be resolved if the US lifted sanctions against Russia. The Infobalkani Facebook Page has over 80,000 Likes and followers.
- 85 <https://medium.com/@crnagoranews>.
- 86 <https://twitter.com/Goran25082>; <https://twitter.com/89Lmao/>; <https://twitter.com/milkopejovic>; <https://twitter.com/2286485Milica>.
- 87 <https://www.facebook.com/profile.php?id=100011599029729>; <https://www.facebook.com/milkopejoviccc/posts/399241067094749>.
- 88 <http://www.forum-cg.ru/user?id=283370768685445>.
- 89 <https://twitter.com/MilkoPejovic/status/712212195371827201>; https://twitter.com/lekovic_mont/status/715166537322201088.
- 90 <https://www.facebook.com/portalcrnagora/posts/483595041838395>.
- 91 Guy Delauney, “Montenegro and Nato: Foes to Friends?” *BBC News*, February 15, 2016, <https://www.bbc.com/news/world-europe-35563081>.
- 92 <https://www.stalkerzone.org/montenegrin-elections-alternative-djukanovics-prospectless-policy/>.
- 93 <https://web.archive.org/web/20161007041822/http://votemontenegro.eu/auth>.
- 94 <https://www.facebook.com/votemontenegro>.
- 95 <https://www.facebook.com/Infobalkani/posts/636467736491426>.
- 96 <https://stanjestvari.com/2016/10/10/crna-gora-news-agency-kako-ukrasti-milione/>.

- 97 <http://bgr.news-front.info/2016/10/16/evrokomisiyata-preduprezhdava-za-veroyatno-falshifitsirane-na-izborite-v-cherna-gora/>; <https://eadaily.com/ru/news/2016/10/15/evrokomissiya-opasaetsya-falsifikacii-parlamentskikh-vyborov-v-chernogorii>. While domain registration information is hidden for eadaily.com, the seemingly identical eurasiadaily.net was registered in Russia.
- 98 See for example <https://stanjestvari.com/2016/10/10/crna-gora-news-agency-kako-ukrasti-milione/>, <http://www.koren.rs/kako-u-crnoj-gori-ukrasti-milione-i-ostati-na-vlasti/>, and <http://www.politicalforum.com/index.php?threads/%22prva-banka%22-family-business-at-the-expense-of-state-and-people-or-how-the-dps-campa.478728/>.
- 99 Evgenii Reigand, “TASS predupredil o fal’sifikatsiiakh na vyborakh v Chernogorii, ssylaias’ na feikovoe agentstvo,” *The Insider*, October 17, 2016, <https://theins.ru/news/33382>; Julia Petrovskaja, “Crna Gora i globalni interesи ruske propagande,” *Radio Slobodna Evropa*, October 20, 2016, <https://www.slobodnaevropa.org/a/crna-gora-rusija-interesi/28063793.html>.
- 100 <https://forum.cdm.me/showthread.php?180294-Izbori-2016/page176>.
- 101 https://wikivisually.com/wiki/User:JamesBWatson/PROD_log.
- 102 Full Hong Kong article: https://web.archive.org/web/20191103231341/http://nbenegroup.com/analytics_en/article/hong-kong-autonomy-of-china-or-not.
- 103 There is also an old version of the site that they link to on the current site: http://old.nbenegroup.com/index_en.html.
- 104 https://web.archive.org/save/http://nbenegroup.com/analytics_en/article/phenomenon-of-russia-within-united-states-of-america.
- 105 <https://www.liveleak.com/c/NBeneGroup>.
- 106 <https://www.instagram.com/nbenegroup/>.
- 107 <http://diyarmirza.ir/1393/07/%DA%86%D9%87%D8%B1%D9%87-%D9%88%D8%A7%D9%82%D8%B9%DB%8C-%D8%A7%D8%A8%D9%88%D8%A8%D9%A9%D8%B1-%D8%A7%D9%84%D8%A8%D8%BA%D8%AF%D8%A7%D8%A-F%D8%8C%D8%B9%DA%A9%D8%B3/>.
- 108 <https://www.reddit.com/domain/nbenegroup.com/>.
- 109 https://www.reddit.com/r/politics/comments/5avbah/the_usa_antimissile_defense_system_provokes_the/.
- 110 <http://www.debatepolicy.com/showthread.php?66665-The-new-Treaty-or-electoral-policy-of-Washington>.
- 111 <https://www.debate.org/forums/politics/topic/4336782/1>. The profile picture he uses appears on several sites warning people about dating.
- 112 <https://twitter.com/search?q=nbenegroup.com&src=typd>.
- 113 <https://twitter.com/Andrew324r>.
- 114 Justin A. Evison, “Migs and Monks in Crimea: Russia Flexes Cultural and Military Muscles Revealing Dire Need for a Stronger International Norm of *Uti Possidetis*,” *Military Law Review* 220, (Summer, 2014): 103-4, https://www.loc.gov/rr/frd/Military_Law/Military_Law_Review/pdf-files/220-summer-2014.pdf.
- 115 Many of these plagiarized articles were attributed to John Daniels and Jonivan Jones. <https://web.archive.org/web/20170311183454/http://theinformer.life/author/informer/>.

- 116 <http://theinformer.life/us-military-bio-labs-ukraine-production-bio-weapons-disease-causing-agents/>. These allegations would surface again in 2018 on the Southern Front Page, described below.
- 117 <https://www.globalresearch.ca/us-military-bio-labs-in-ukraine-production-of-bio-weapons-and-disease-causing-agents/5605307>.
- 118 <http://theinformer.life/european-prudence-lessen-u-s-russia-nuclear-tension/>.
- 119 <http://theinformer.life/washington-threatens-global-security-violating-inf-treaty/>.
- 120 <http://theinformer.life/white-helmets-prepare-provocation-syrian-idlib/>.
- 121 <https://ekurd.net/white-helmets-provocation-syrian-2018-08-26>.
- 122 <https://www.change.org/p/help-us-save-our-future-children-of-syrian-people-need-you-join-our-movement-in-support-of-peace>. The email associated with the petition is aalrashed-al-Sumari@mail.com. The Twitter handle associated with that user is @ savesyriafuture, which joined in March 2017 but has only one follower.
- 123 <https://www.reddit.com/user/Hathapsonel70/comments/>.
- 124 <https://www.facebook.com/groups/UnitedResistance/>, <https://www.facebook.com/groups/1213941462028181/permalink/1537900879632236>.
- 125 <https://www.facebook.com/utlaw/posts/101565555621279515>.
- 126 http://theinformer.life/apples-deal-for-shazam-delayed-in-europe-over-data-concerns/?platform=hootsuite&fbclid=IwAR2O_iXcLt8LcVbvka84RTr_jl0L_H6IXwm1lwdfW8-6Bu_P3X2RIUxPu8A. See Adam Satariano, “Apple’s Deal for Shazam is Delayed in Europe over Data Concerns,” *New York Times*, April 23, 2018, <https://www.nytimes.com/2018/04/23/business/apple-shazam-eu-data.html>.
- 127 We chose not to share the name of the individual for privacy reasons.
- 128 <https://worldnewsobserve.wordpress.com/2016/10/28/montenegrinische-behorden-decken-den-echten-organisator-des-umsturzes/>.
- 129 <https://worldnewsobserve.wordpress.com/2016/09/22/die-ostliche-gefahr-fur-europa-ist-ein-produkt-der-us-propaganda/>.
- 130 <https://worldnewsobserve.wordpress.com/2016/08/26/erdogan-deutschlands-partner-und-pate-des-terrors/>.
- 131 <https://twitter.com/Stefstrom>. A user with the same profile photo “liked” one of the site’s posts: <https://worldnewsobserve.wordpress.com/2016/09/22/die-ostliche-gefahr-fur-europa-ist-ein-produkt-der-us-propaganda/>. <https://en.gravatar.com/ottolarenz>.
- 132 victoryforpeace.ru.
- 133 Lev Gudkov, “The Fetters of Victory: How the War Provides Russia with Its Identity,” *Eurozine*, May 3, 2005, trans. Mischa Gabowitsch, <https://www.eurozine.com/the-fetters-of-victory/>.
- 134 The Russian Ministry of Foreign Affairs gave us another example of this quite recently, when its Embassy in South Africa asserted that the USSR did not invade Poland in September, 1939 but merely “entered” it: <https://russianembassyza.mid.ru/-/80-years-since-the-start-of-world-war-ii-a-russian-perspective-based-on-facts>.

- 135 John Biersack and Shannon O'Lear, "The Geopolitics of Russia's Annexation of Crimea: Narratives, Identity, Silences, and Energy, *Eurasian Geography and Economics* 55, no. 3, (2014): 247-269, DOI: 10.1080/15387216.2014.985241.
- 136 <https://www.kommersant.ru/doc/2688755>. An English translation of this speech and others was the last item to appear on "Victory for Peace."
- 137 http://victoryforpeace.ru/?lng=en&module=publications&action=list&id=5&id_pub=53.
- 138 The data provided by Facebook only included figures, not a currency designation. We have assumed that the figures given for ad spends represent Russian roubles. The amounts spent correspond roughly to the average cost of Facebook ads generating the given number of impressions.
- 139 <https://www.facebook.com/pg/Infores.en/about/>. 10,500 people currently Like the Page, which was created on March 1, 2012. Its tagline is "The World Through The Eyes of Russia," and the Page is still actively updated with what appears to be primarily a news feed. Currently there are posts about MH17, Ukraine, and Syria, slanted to the Russian government's point of view, including MH17-related denials that any Russian army missile system had ever crossed the Ukrainian border.
- 140 A recent article on Ukrainian President Volodymyr Zelensky, for example, was taken from TASS; the main Antimaidan VK page also reposted the article.
- 141 Anton Troianovski and Ellen Nakashima, "How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels with the West," *Washington Post*, December 28, 2018, https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html.
- 142 Andrei Soldatov and Irinia Borogan, "Russia's Approach to Cyber: The Best Defence Is a Good Offense," in *Hacks, Leaks, and Disruptions: Russian Cyber Strategy*, Chaillot Paper 148, ed. Nicu Popescu and Stanislav Secrieru, (Paris: European Union Institute for Security Studies, 2018), 18, https://www.iss.europa.eu/sites/default/files/EUSSIFiles/CP_148.pdf.
- 143 Nadia Diuk, "EUROMAIDAN: Ukraine's Self-Organizing Revolution," *World Affairs* 176, no. 6 (2014): 10-11.
- 144 See Adrian Karatnycky, "Ukraine's Orange Revolution," *Foreign Affairs* 84, no. 2, (March, 2005): 35-52, <https://www.foreignaffairs.com/articles/russia-fsu/2005-03-01/ukraines-orange-revolution>, and Anders Aslund and Michael McFaul, eds., *Revolution in Orange: The Origins of Ukraine's Democratic Breakthrough*, (Washington, D.C.: Carnegie Endowment for International Peace, 2013).
- 145 "A Tale of Two Countries," *The Economist*, February 24, 2014, <https://www.economist.com/eastern-approaches/2014/02/24/a-tale-of-two-countries>.
- 146 Oleksandr Bohomolov and Oleksandr Lytvynenko, *A Ghost in the Mirror: Russian Soft Power in Ukraine*, (London: Chatham House, 2012), 3-4, https://www.chathamhouse.org/sites/default/files/public/Research/Russia%20and%20Eurasia/0112bp_bogomolov_lytvynenko.pdf.
- 147 Kathryn Stoner, "Putin's Search for Greatness: Will Ukraine Bring Russia the Superpower Status It Seeks?" *Foreign Affairs*, March 2, 2014, <https://www.foreignaffairs.com/articles/russia-fsu/2014-03-02/putins-search-greatness>.
- 148 David R. Marples, "Russia's perceptions of Ukraine: Euromaidan and historical conflicts," *European Politics and Society*, 17, no. 4 (March 2016), 425-427, <https://doi.org/10.1080/23745118.2016.1154129>.

- 149 These measures are key parts of the Russian government's larger cyber strategy. See Soldatov and Borogan, "Russia's Approach to Cyber," 15-23.
- 150 Anna Colin Lebedev, "From a Mother's Worry to Soldiers' Mothers' Action: Building Collective Action on Personal Concerns," in *Understanding Russianness*, ed. Risto Alapuro et al., (Abingdon, United Kingdom: Routledge, 2011), 98-112. The CSM has publicized Russian casualties in Eastern Ukraine, and was slapped with the label "Foreign Agent" as a result. See Reid Standish, "Is Vladimir Putin Covering Up the Deaths of Russian Soldiers in Ukraine?" *Foreign Policy*, September 1, 2014, <https://foreignpolicy.com/2014/09/01/is-vladimir-putin-covering-up-the-deaths-of-russian-soldiers-in-ukraine/>.
- 151 Indeed, the CSMU does publish content that is problematic for the Ukrainian government. A Facebook Page associated with the group goes even further, calling for an end to a "senseless" war: "The Committee of Soldiers' Mothers of Ukraine is a society of women speaking out against the murder of their sons, husbands, and fathers, who are being sent to a senseless, bloody war."
- 152 <http://materi-ua.com/>.
- 153 https://vk.com/materi_ykraunu; <https://www.facebook.com/groups/materi.ykraunu/>.
- 154 <https://www.facebook.com/profile.php?id=100004308134206>.
- 155 "Socio-Political Expectations: April, 2014," *Rating Group Ukraine*, April 7, 2014, http://ratinggroup.ua/en/research/ukraine/obschestvenno-politicheskie_ozhidaniya_grazhdan_aprel_2014.html.
- 156 Tarik Cyril Amar, *The Paradox of Ukrainian Lviv: A Borderland City between Stalinists, Nazis, and Nationalists*, (Ithaca, NY: Cornell University Press, 2015), 1-21.
- 157 It is not clear why this Status Update was written in English, since the Page's audience could be assumed to be speakers of Ukrainian, Polish, and Russian. Indeed, all of the other posts that appeared on the Page were in these three languages. One possibility is that this English-language post was an attempt to reach readers in other parts of Europe. In any case, it did not attract any engagement.
- 158 Jason Parham, "Targeting Black Americans, Russia's IRA Exploited Racial Wounds," *Wired*, December 17, 2018, <https://www.wired.com/story/russia-ira-target-black-americans/>.
- 159 <https://www.facebook.com/pages/Justice-For-Jerame-Reid/410967189058821>.
- 160 Andrea B. Scott, "Police Kill Nearly 25 Dogs Each Day," *The Nation*, July 5, 2016, <https://www.thenation.com/article/police-kill-nearly-25-dogs-each-day/>.
- 161 <http://blacklivesmatter.media/post/6177094/antoine-fuqua-to-develop-film-based-on-black-panther-murdered-by>.
- 162 P. R. Lockhart, "The Largest Black Lives Matter Page on Facebook Was a Scam," *Vox Media*, April 11, 2018, <https://www.vox.com/identities/2018/4/10/17219676/facebook-black-lives-matter-page-fake>.
- 163 <https://medium.com/dfrlab/trolltracker-russias-other-troll-team-4efd2f73f9b5>.
- 164 "State Dept Sideshow: Jen Psaki's Most Embarrassing Fails, Most Entertaining Grillings," *RT*, June 1, 2014, <https://www.rt.com/usa/162608-jen-psaki-fails-grilling/>.
- 165 Nick Gass, "The Russian Media's Obsession with Jen Psaki," *Politico*, February 19, 2015, <https://www.politico.com/story/2015/02/jen-psaki-russian-media-obsession-115318>.

- 166 Robert Mackey, “Russian State Media Focuses Attacks on Kerry’s Spokeswoman,” *New York Times*, June 6, 2014, <https://www.nytimes.com/2014/06/07/world/europe/russian-news-media-amplifies-attacks-on-kerrys-spokeswoman.html>.
- 167 Felicia Schwartz, “Jen Psaki’s Boot Kicks up Russian State Media Attention,” *The Wall Street Journal*, August 1, 2014, <https://blogs.wsj.com/washwire/2014/08/01/jen-psakis-boot-kicks-up-russian-state-media-attention/>.
- 168 Alister Doyle, “Russia Warns of More Visits to Disputed Islands,” Reuters, November 2, 2010, <https://www.reuters.com/article/us-japan-islands/russia-warns-of-more-visits-to-disputed-islands-idUSTRE6A13NI20101102>.
- 169 <https://www.facebook.com/people/Andrew-Kolkovich/100010148792094>. Archived version: <http://archive.is/zuMrc>
- 170 <https://twitter.com/andrew324r>.
- 171 <http://newsland.com/user/4297768747>; <http://maxpark.com/user/4295213781>.
- 172 <http://newsland.com/user/4297768747/content/ssha-politika-indeiskikh-rezervatsii/4404755>.
- 173 A stub Page with only an uploaded photo as its content, called Mycompany, made a post in 2012.
- 174 https://web.archive.org/web/20151212054900/https://www.livleak.com/c/Andrew_Kolkovich.
- 175 <https://www.quora.com/profile/Andrew-Kolkovich>.
- 176 Entous, “Rise and Fall.”
- 177 Cybersecurity firms Crowdstrike, SecureWorks, ThreatConnect, and Fireeye’s Mandiant had all written about APT 28’s likely association with the Russian government prior to the Special Counsel’s attribution.
- 178 Mueller, *Report on the Investigation*.
- 179 Also noted in the Netyksho indictment, p. 38, <https://www.justice.gov/file/1080281/download>.
- 180 Entous, “Rise and Fall.”
- 181 Josh Meyer, “Experts: Same Russians Hacked Olympic Whistleblower, Democrats,” *NBC News*, August 27, 2016, <https://www.nbcnews.com/storyline/2016-rio-summer-olympics/experts-same-russians-hacked-olympic-whistleblower-democrats-n637871>.
- 182 <https://web.archive.org/web/20190824234352/https://dileaks.com/index.php/about/>.
- 183 These include @wadeharriot, @rh0lbr00k, @patriotblake, @melanymelanin, @j0hnlarson, @finley1589, @donnabrivera, @cynthiamhunter, @emileewaren, @chadsloyer, @ameliebaldwin, and @alecmooooody.
- 184 <https://www.reddit.com/domain/dileaks.com/>.
- 185 “Russian Cyber Operations on Steroids,” *ThreatConnect*, August 19, 2016, <https://threatconnect.com/blog/fancy-bear-anti-doping-agency-phishing>.

- 186 “Cyber Hack Update: Data Leak Concerning 41 Athletes from 13 Countries and 17 Sports,” *World Anti-Doping Agency*, September 23, 2016, <https://www.wada-ama.org/en/media/news/2016-09/cyber-hack-update-data-leak-concerning-41-athletes-from-13-countries-and-17>.
- 187 “Cyber Security Update: WADA’s Response,” *World Anti-Doping Agency*, October 5, 2016, <https://www.wada-ama.org/en/media/news/2016-10/cyber-security-update-wadas-incident-response>.
- 188 Richard H. McLaren, *McLaren Independent Investigation Report*, (Montreal: World Anti-Doping Agency, 2016), <https://www.wada-ama.org/en/resources/doping-control-process/mclaren-independent-investigations-report-into-sochi-allegations>; “WADA Statement: Independent Investigation Confirms Russian State Manipulation of the Doping Control Process,” *World Anti-Doping Agency*, July 18, 2016, <https://www.wada-ama.org/en/media/news/2016-07/wada-statement-independent-investigation-confirms-russian-state-manipulation-of>.
- 189 <https://web.archive.org/web/20170916004246/twitter.com/FancyBears>.
- 190 “‘Asthma + TUE = Olympic Medals’: Fancy Bears Reveals Formula of Western Athletes’ Success,” *RT*, January 24, 2018, <https://www.rt.com/sport/416866-fancy-bears-tue-doping/>.
- 191 <https://www.mintpressnews.com/hacktivists-reveal-many-us-olympians-allowed-taking-banned-substances/220449/>.
- 192 https://russiatweets.com/tweet-search?terms=wada&language=English®ion=&start_date=&end_date=&orderby=&author=naturn.
- 193 Ben Nimmo, “#PutinAtWar: WADA Hack Shows Kremlin Full-Spectrum Approach,” *DFRLab*, October 14, 2018, <https://medium.com/dfrlab/putinatwar-wada-hack-shows-kremlin-full-spectrum-approach-21dd495f2e91>.
- 194 <https://twitter.com/FoulPlaySI>.
- 195 <https://www.facebook.com/FoulplaySportsInvestigation/>.
- 196 <https://medium.com/@FoulPlay/about-foulplay-4b4e4f26b8ee>.
- 197 <https://foulplaysi.wordpress.com/2017/07/06/backstage-secrets-of-the-alex-schwazer-case-investigation/#more-784>.
- 198 <https://foulplaysi.wordpress.com/2018/07/11/stolen-football-holiday/>.
- 199 <https://wideshot.co.uk/stolen-football-holiday/>.
- 200 Andy Holmes also posted about Fancy Bears’ WADA leaks on Medium; see note 201.
- 201 <https://www.covers.com/forum/Profile/834577/FoulPlaySI>.
- 202 “Belling the Bear,” *ThreatConnect*, September 28, 2016, <https://threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/>; *2015 Global Threat Report*, CrowdStrike, February, 2016, <https://go.crowdstrike.com/rs/281-OBO-266/images/15GlobalThreatReport.pdf>; “Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed,” *National Cyber Security Centre*, October 3, 2018, <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed>.
- 203 Jeff Stone, “Meet CyberBerkut, the Pro-Russian Hackers Waging Anonymous-Style Cyberwarfare Against Ukraine,” *International Business Times*, December 17, 2015, <https://www.ibtimes.com/meet-cyberberkut-pro-russian-hackers-waging-anonymous-style-cyberwarfare-against-2228902>.

- 204 Adrian Croft and Peter Apps, “NATO Websites Hit in Cyber Attack Linked to Crimea Tension,” *Reuters*, March 15, 2014, <https://www.reuters.com/article/us-ukraine-nato/nato-websites-hit-in-cyber-attack-linked-to-crimea-tension-idUSBREA2E0T320140316>.
- 205 Adam Hulcoop et al., “Tainted Leaks: Disinformation and Phishing with a Russian Nexus,” *Citizen Lab*, May 25, 2017, <https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/>.
- 206 Mark Clayton, “Ukraine Election Narrowly Avoided ‘Wanton Destruction’ from Hackers,” *The Christian Science Monitor*, June 17, 2014, <https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers>.
- 207 <https://cyber-berkut.org/en/>.
- 208 CyberBerkut, similarly to the Antimaidan ukraine page discussed in the appendix, refers frequently to the Second World War in its content, often asserting that the government in Kyiv is in thrall to far-right followers of Bandera, the Ukrainian nationalist who collaborated with the Nazis.
- 209 For more information on CyberBerkut’s operations, see Hulcoop, “Tainted Leaks” and Vitaly Shevchenko, “Ukraine conflict: Hackers take sides in virtual war,” *BBC News*, December 20, 2014, <https://www.bbc.com/news/world-europe-30453069>.
- 210 For context, in January, 2018, it was revealed that the BEREG-KIT Geneva bottles could be opened manually without evidence of tampering. This led many in the Russian media, including RT, to cast doubt on the evidence WADA had brought forward between 2015 and 2017 leading to the IOC’s decision to ban a number of Russian athletes from the 2016 Summer Olympics in Rio de Janeiro and to ban the Russian Olympic Team from the 2018 Winter Olympics in Pyeongchang altogether. Fancy Bear conducted several hack-and-leak operations in support of this campaign, one of which was reposted on Southern Front.
- 211 This leak appears not to have been picked up by the press, so it appears in few places. However, there is evidence that fake accounts attempted to spread the story. One apparent persona, Andy Holmes, posted about it on Medium: <https://medium.com/@gentleandrew01/fancy-bears-strike-at-berlinger-and-swedish-anti-doping-agency-b7af09213829>. This persona also posted content on Twitter questioning the fairness of the IOC’s banning of the Russian team.
- 212 “Belling the Bear,” *ThreatConnect*. Since much of Fancy Bear’s work has been taken down, including its website, it is difficult to confirm whether or not Fancy Bear shared CyberBerkut material.
- 213 Daniel Boffey and Patrick Wintour, “Dutch Expelled Russians Over Alleged Novichok Lab Hacking Plot,” *The Guardian*, September 14, 2018, <https://www.theguardian.com/uk-news/2018/sep/14/dutch-expelled-russians-over-alleged-novichok-laboratory-hacking-plot>; United States of America v. Moronets, <https://assets.documentcloud.org/documents/4954141/Indictment-7-GRU-Officers-Oct2018.pdf>.
- 214 https://twitter.com/mfa_russia/status/985189624720093186.
- 215 “Opening Statement by the Director-General to the Executive Council at its Fifty-Ninth Meeting,” *Organization for the Prohibition of Chemical Weapons*, April, 2018, https://www.opcw.org/sites/default/files/documents/EC/M-59/en/ecm59dg01_e_.pdf.
- 216 <https://www.rt.com/news/424149-skripal-poisoning-bz-lavrov/>.
- 217 <https://www.bellingcat.com/news/uk-and-europe/2018/05/25/mh17-russian-gru-commander-orion-identified-oleg-ivannikov/>
- 218 See note 189.

- 219 Serhy Yekelchyk, *The Conflict in Ukraine*, (Oxford: Oxford University Press, 2015), 141-142.
- 220 “Ukraine Crisis: Moscow Rally Against ‘Coup’ One Year On,” *BBC News*, February 21, 2015, <https://www.bbc.com/news/world-europe-31561769>.
- 221 “Russia’s Levada Centre Polling Group Named Foreign Agent,” *BBC News*, September 5, 2016, <https://www.bbc.com/news/world-europe-37278649>.
- 222 Antimaidan.ru and the Antimaidan VK page are still up as of November, 2019: <https://vk.com/antimaydan>.
- 223 <https://www.youtube.com/c/AntimaidanUkraine>.
- 224 <https://www.facebook.com/antimaidanukraine>; <https://vk.com/antimaidanukraine>; https://vk.com/antimaidan_ukraine; <https://ok.ru/antimaidanukraine>.
- 225 <http://www.mirkavkazu.ru/2015/?lng=ru&module=news&action=view&id=507>.
- 226 <https://www.facebook.com/mirkavkazu.ru/>.
- 227 <https://vk.com/club44721636>.
- 228 https://www.facebook.com/groups/mirkavkazu/?ref=pages_groups_card&source_id=357757690983115.
- 229 <https://www.facebook.com/lnforos.ru>.
- 230 Description of event: https://en.wikipedia.org/wiki/2015_Russian_Sukhoi_Su-24_shootdown.
- 231 <http://conflictzone.info/top-news/14-missing-russian-jet-pilot-alive-and-well-in-syria.html>.
- 232 https://twitter.com/balaban_off/status/669536378804375553.
- 233 https://en.wikipedia.org/wiki/Military_Historical_Museum_of_Artillery,_Engineers_and_Signal_Corps.
- 234 <https://twitter.com/politespb>, <https://www.facebook.com/politespb2015/>.
- 235 <https://www.facebook.com/TheAnonymousWriter>. Note that this Page appears to be authentic; it has existed since 2012.

The **Stanford Internet Observatory** is a cross-disciplinary program of research, teaching and policy engagement for the study of abuse in current information technologies, with a focus on social media. Under the program direction of computer security expert **Alex Stamos**, the Observatory was created to learn about the abuse of the internet in real time, to develop a novel curriculum on trust and safety that is a first in computer science, and to translate our research discoveries into training and policy innovations for the public good.

By providing researchers across Stanford with cutting edge data analytics and machine learning resources we will unlock completely unforeseen fields of research. We envision a world where researchers do not limit themselves to the data that is easy to access, but instead dive into the toughest and most important questions by leveraging the capabilities of the Stanford Internet Observatory.

Stanford | Internet Observatory
Cyber Policy Center

Encina Hall
616 Jane Stanford Way C100
Stanford University
Stanford, CA 94305-6055
650.723.4581