Covid-19 Disinformation and social media manipulation

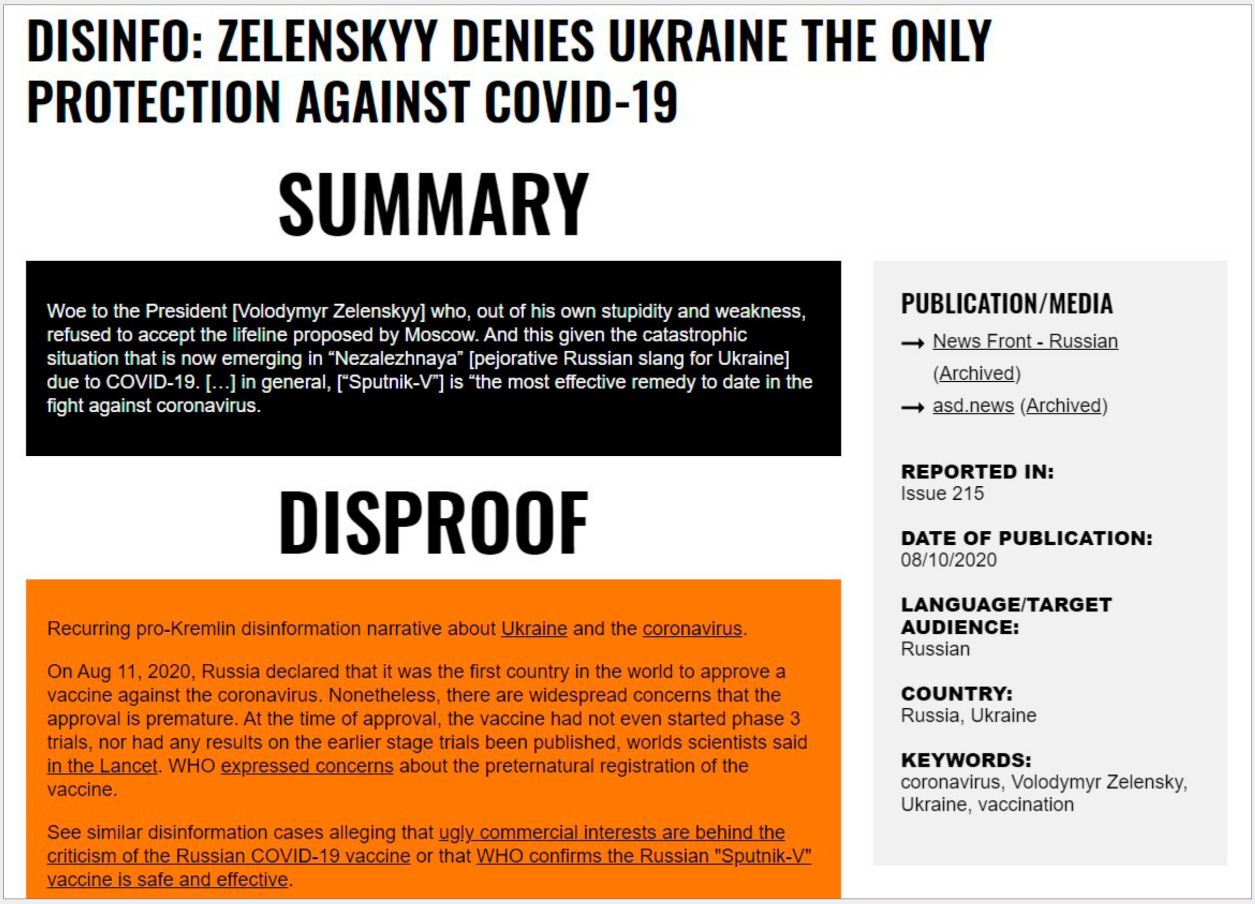
Ray Serrato and Dr Jake Wallis

Covid-19 and the reach of pro-Kremlin messaging

Introduction

This research investigation examines Russia's efforts to manipulate the information environment during the coronavirus crisis. It leverages data from the European External Action Service's East StratCom Task Force, which, through its EUvsDisinfo project, tracks pro-Kremlin messages spreading in the EU and Eastern Partnership countries. The taskforce monitors media in those countries to identify and expose Russian disinformation, maintaining a regularly updated database of samples (Figure 1). Using this open-source repository of pro-Kremlin disinformation in combination with OSINT investigative techniques that track links between online entities, we analyse the narratives being seeded about coronavirus and map the social media accounts spreading those messages.

Figure 1: Example entry in the EUvsDisinfo database



DISINFO: ZELENSKYY DENIES UKRAINE THE ONLY PROTECTION AGAINST COVID-19

SUMMARY

Woe to the President [Volodymyr Zelenskyy] who, out of his own stupidity and weakness, refused to accept the lifeline proposed by Moscow. And this given the catastrophic situation that is now emerging in "Nezalezhnaya" [pejorative Russian slang for Ukraine] due to COVID-19. [...] in general, ["Sputnik-V"] is "the most effective remedy to date in the fight against coronavirus.

DISPROOF

Recurring pro-Kremlin disinformation narrative about Ukraine and the coronavirus.

On Aug 11, 2020, Russia declared that it was the first country in the world to approve a vaccine against the coronavirus. Nonetheless, there are widespread concerns that the approval is premature. At the time of approval, the vaccine had not even started phase 3 trials, nor had any results on the earlier stage trials been published, worlds scientists said in the Lancet. WHO expressed concerns about the preternatural registration of the vaccine.

See similar disinformation cases alleging that ugly commercial interests are behind the criticism of the Russian COVID-19 vaccine or that WHO confirms the Russian "Sputnik-V" vaccine is safe and effective.

PUBLICATION/MEDIA

→ News Front - Russian (Archived)

→ asd.news (Archived)

REPORTED IN:
Issue 215

DATE OF PUBLICATION:
08/10/2020

LANGUAGE/TARGET AUDIENCE:
Russian

COUNTRY:
Russia, Ukraine

KEYWORDS:
coronavirus, Volodymyr Zelensky, Ukraine, vaccination

October 2020

We found that the key subjects of the Kremlin's messaging focused on the EU, NATO, Bill Gates, George Soros, the World Health Organization (WHO), the US and Ukraine. The narratives in the messages included well-trodden conspiracies about the source of the coronavirus, the development and testing of a potential vaccine, the impact on the EU's institutions, the EU's slow response to the virus and Ukraine's new president. We also found that Facebook groups are a powerful hub for the spread of some of those messages.

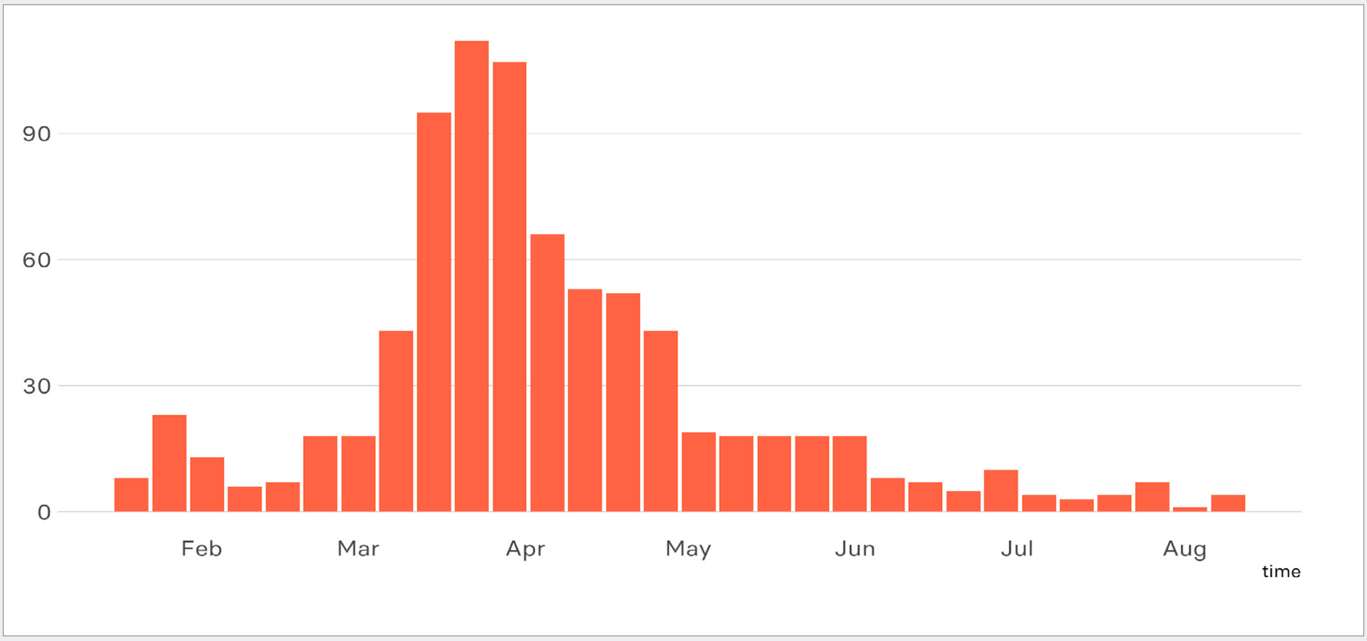
In the course of this investigation, we discovered numerous sites and associated social media accounts apparently targeting Iraqi and Arab audiences. The sites exclusively distribute articles with no by-lines, and all of the content we reviewed was plagiarised from other media sites. Our analysis of the sites demonstrates their connections by identifying shared metadata, tracking tags, IP addresses, and temporal signatures that suggest coordination between social media accounts. We have been unable to attribute this activity to a specific owner or media outlet.

Tracking the spread of Kremlin Covid-19 messages

We used the EUvsDisinfo database to retrieve 808 pieces of multilingual, multimedia content (media articles, images and videos) that contained the index keywords 'Covid-19' or 'coronavirus' and had been assessed by the EU East StratCom Task Force as messages that provided a 'partial, distorted, or false depiction of reality and spread key pro-Kremlin messages'.[1]

The content we scraped was published between January and August 2020, with a peak in publishing between March and April, shortly after the WHO announced the global pandemic (Figure 2).

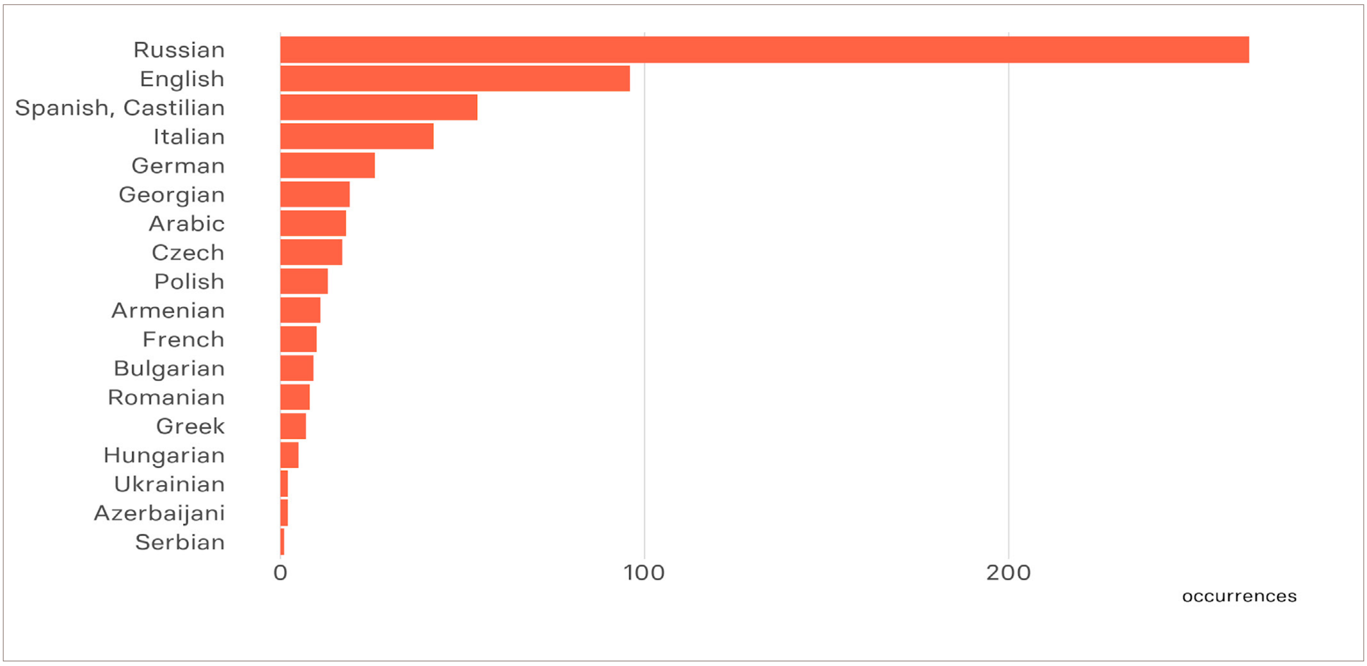
Figure 2: Weekly number of Covid-19 articles containing pro-Kremlin messaging, February to August 2020



Source: Data taken from the EUvsDisinfo Database.

Additionally, Covid-19 content containing pro-Kremlin messaging was published in 19 different languages (Figure 3), illustrating the diversity of targets. However, Russian-language content far outnumbered other languages, followed by English, Spanish (or Castilian), Italian and German.

Figure 3: Target languages for pro-Kremlin messaging on Covid-19



Source: Data taken from the EUvsDisinfo Database.

This content was published across 760 different media sites, and the vast majority was hosted on sites of varying credibility. Although content from YouTube was the most frequently cited material, only 3% of all content came from social media platforms (Facebook, YouTube or Instagram).

Table 1: Top 20 publishers

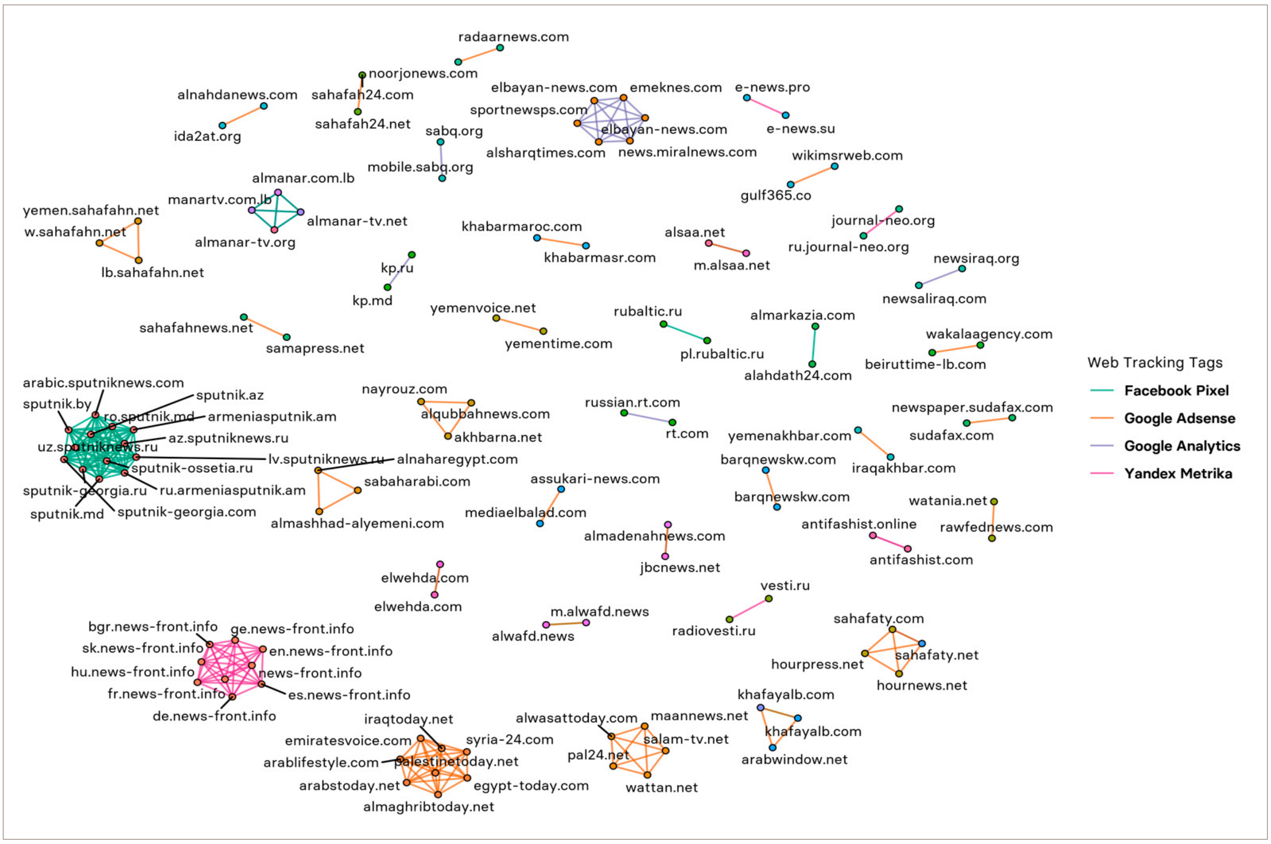
Domain	Count
youtube.com	84
www.albidda.net	77
www.saadaonline.net	55
ar.rt.com	50
www.geopolitica.ru	49
southfront.org	42
es.news-front.info	36
sportnewsps.com	30
nabd.com	29
ru.armeniasputnik.am	27
www.bbcnews1.com	26
mundo.sputniknews.com	24
www.rt.com	23
www.facebook.com	22
katehon.com	21
news.dmcnews.org	21
kol-masr.com	18
www.akhbarlibya.net	18
cz.sputniknews.com	17
lomazoma.com	17

Unsurprisingly, Russian state-controlled media were among the most frequent publishers of Covid-19 disinformation (Table 1), as well as other propaganda outlets such as *News Front* (which was also a dissemination node in our previous analysis of pro-Russian vaccine disinformation[2]) and *South Front*—both media organisations implicated earlier this year in a network of inauthentic activity on Facebook and Instagram.[3] The most frequently used domain suffix (the last part of a domain name), or 'top level domain', was Russia (.ru), followed by Armenia (.am), Palestine (.ps) and Syria (.sy).

We also scraped HTML code from the home pages of all 760 sites publishing pro-Kremlin messaging on Covid-19. Using that data, we extracted web tracking tags to identify sites that shared identical tags, which would suggest a principal owner. Tracking tags are pieces of code that website owners can embed within their sites to capture analytics about how users interact with the site. The tags help site owners to gather data about users who visit their sites—data such as audience size, demographics, page views, conversions from Facebook ads and more. As an example, a Google Analytics tag contains a unique eight-digit identification number (appearing as *UA-XXXXXXXX*) that's linked to a Google Analytics account and can be used on multiple sites operated by the same owner; many other tracking tags work in much the same way.

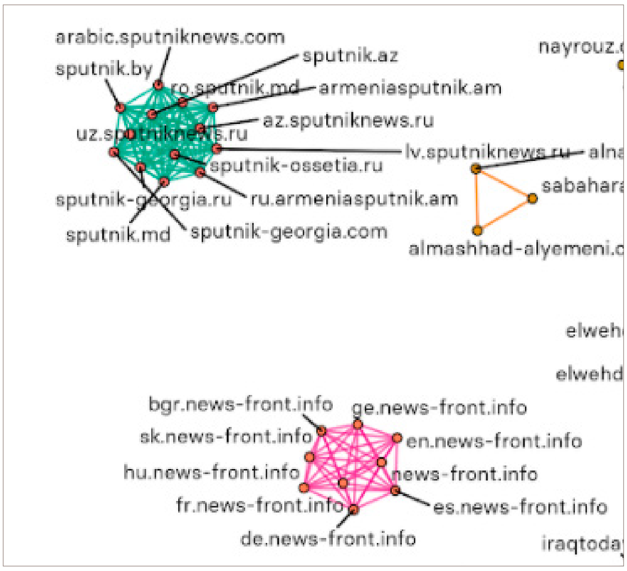
In the network graph (Figure 4), we've visualised all sites that are connected via shared tracking tags: sites are represented as nodes (coloured by community), and tracking tag links (coloured by a specific tag) are represented as connections between nodes. This analysis shows clusters of sites linked and probably owned by the same entity, even where that relationship might not be readily apparent.

Figure 4: Visualisation of sites connected by shared tracking tags



The largest clusters of sites (Figure 5) consist of *Sputnik* and *News Front* assets connected via Facebook pixel and Yandex Metrika tags. *Sputnik* is a Russian state-owned news agency that produces pro-Kremlin content in multiple languages. *News Front* presents itself as independent media and publishes in multiple languages, yet is based in eastern Ukraine, is editorially pro-Kremlin and is linked to pro-Russian separatists. *News Front* has had multiple accounts removed from Facebook for coordinated inauthentic behaviour on behalf of a foreign entity and is suspended from Twitter and YouTube for breaches of their terms of service. According to *Die Zeit*, a former *News Front* employee has alleged that the agency receives funding from Russia's security apparatus.

Figure 5: Close up of clusters of *Sputnik* and *News Front* sites linked by tracking tags



The focus of pro-Kremlin messaging

The most frequently mentioned entities in the Kremlin messaging were the EU (mentioned 96 times) and NATO (mentioned 36 times); together, the EU and NATO were mentioned in nearly 25% of all cases we reviewed. Other targets in Kremlin messaging included Bill Gates, George Soros, the WHO, the US and Ukraine.

Narratives in the messages included well-worn conspiracy theories about the source of the coronavirus ('The main source of the coronavirus was an American laboratory in Armenia'), the development and testing of a potential vaccine ('NATO soldiers have already been vaccinated against Covid-19'), the impact of the pandemic on the EU's institutions ('The Covid-19 outbreak means the end of Europe; Russia and China will rise'), the EU's slow response to the virus ('EU has been unable to support its most affected members'), and Ukraine's new president ('Zelensky introduces tax on war and coronavirus in Ukraine'). Table 2contains a random sample of case titles on each of those specific topics.

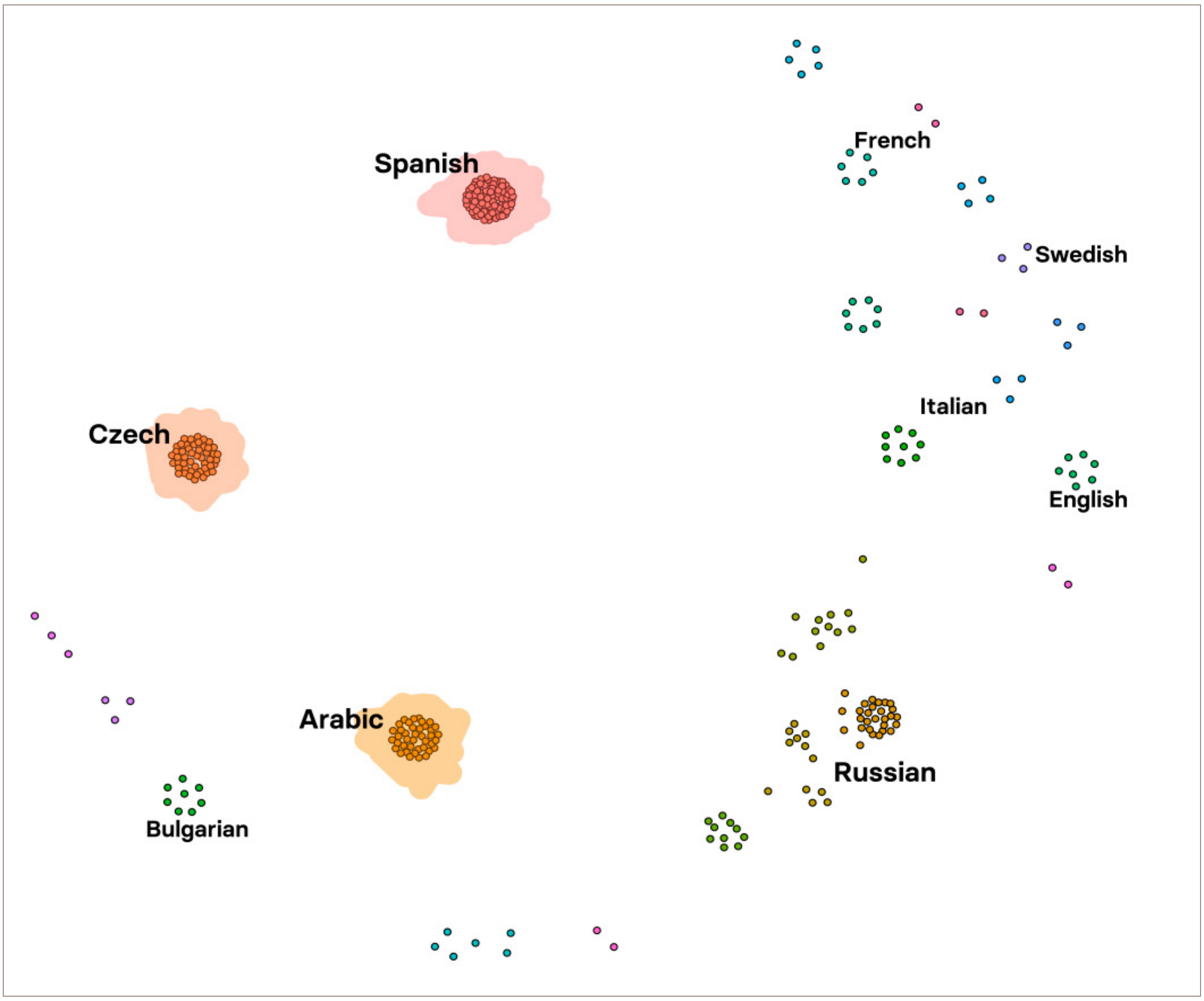
Table 2: Sample of content containing disinformation, by topic

Topic	Title
Bill Gates	Bill Gates is working on depopulation policies and plans for dictatorial control of world politics
Bill Gates	Bill Gates warns of an ineffective coronavirus vaccine
Bill Gates	Covid-19 vaccines are a big pharma fraud led by Bill Gates
China	Moldova is helped only by China and Russia in the fight with COVID-19
China	China's political system prevails over the European Union in the fight against coronavirus
China	Coronavirus is psychological warfare against enemies like China and Iran
EU	The coronavirus puts EU's existence into question
EU	As a result of the coronavirus pandemic the end of the EU is approaching
EU	Illegal EU sanctions hinder Syria's ability to fight COVID19
NATO	NATO countries have been increasing the defense spending and now they don't have lung ventilators
NATO	Coronavirus may be the latest step in NATO's containment strategy against China
NATO	The coronavirus destroyed the myth of the NATO's super army, NATO is fleeing Europe
Ukraine	In Ukraine, doctors quit en masse because of Ukrainian soldiers with COVID-19
Ukraine	A pensioner died in Ukraine after being fined for violating quarantine
Ukraine	There is no one to fight the coronavirus in Ukraine, the epidemiological system is destroyed
US	Czechia is US's puppet, removal of Konev's monument was sanctioned by Washington
US	Coronavirus an Anglo-Saxon biological warning: originates in US labs; targets opponents of the US
US	The coronavirus infection on a US aircraft carrier jeopardises the invasion of Venezuela

Network structure

We also analysed the network groupings of public Facebook pages and groups that had a tendency to share similar links to Kremlin-aligned messaging on Covid-19. Figure 6 shows the network between 366 Facebook pages and groups (as nodes) that shared any of this content.

Figure 6: Network clusters of Facebook pages and groups based on language



The network shows distinct regional and linguistic communities: Czech, Spanish, Arabic, Italian, Russian, Polish, French, Swedish, English and other language groups and pages. The largest groups are highlighted; the Spanish cluster is characterised mainly by cross-posters in groups and centres on a *Sputnik Mundo* story alleging that the WHO and Microsoft would sabotage a newly announced Russian vaccine. Similarly, the Czech cluster centres on a *Sputnik* article in Czech that covers Russia's announcement of a new drug to treat the effects of Covid-19. The Arabic cluster, meanwhile, is a link to an *RT Arabic* language video titled 'Russia repelled a stronger epidemic than Corona …'

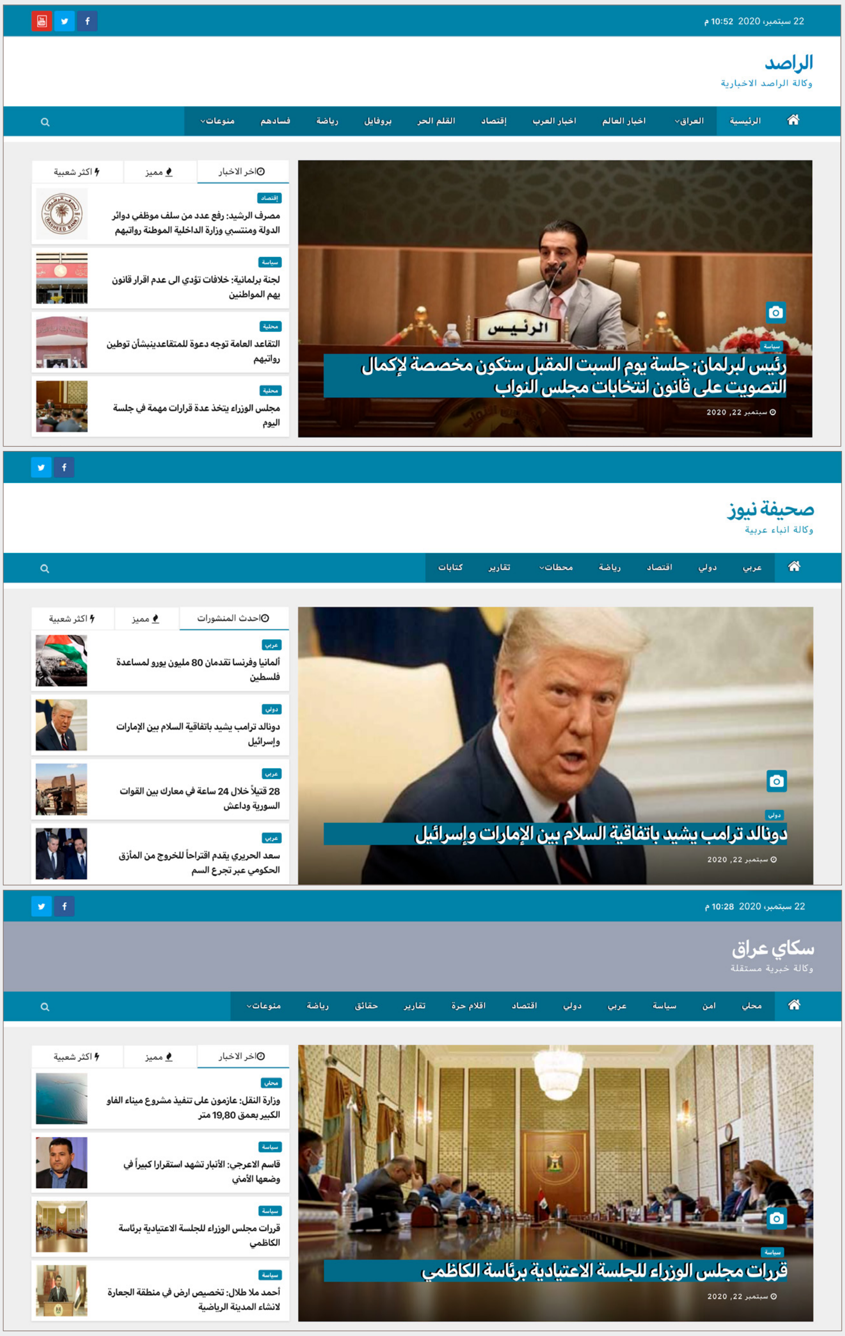
The graph also shows that Facebook groups are a powerful hub for the spread of Kremlin narratives about Covid-19, making up 83% of the sharers on Facebook. Our analysis of the accounts suggests spaces dedicated to various, but adjacent, beliefs: the *Australian Climate Sceptics Group*, *Man Made Global Warming is a HOAX*, *Anti Soros*, *QAnon Latin America*, *QAnon Colombia* and others.

Suspicious Iraqi-focused sites

During this research, we uncovered eight suspicious sites and associated social media accounts aimed at the Iraqi population. Several of the sites use the same WordPress templates (Figure 7) and purport to be ‘independent news’ agencies, but contain no information about their ownership, staff or editors. Our review of them shows that they exclusively publish content that’s copied wholesale from other regional and international news sites.

The screenshots in Figure 7 show the home pages of three of these sites: sahefa.news, alrassid.org and skyiraq.news.

Figure 7: Home pages of sahefa.news, alrassid.org, and skyiraq.news



اقتصاد
مصرف الرشيد: رفع عدد من سلف موظفي دوائر الدولة ومنتسبي وزارة الداخلية الموطنة رواتبهم

سياسة
لجنة برلمانية: خلافات تؤدي الى عدم اقرار قانون يهم المواطنين

محلية
التقاعد العامة توجه دعوة للمتقاعدينبشأن توطين رواتبهم

محلية
مجلس الوزراء يتخذ عدة قرارات مهمة في جلسة اليوم

سياسة
رئيس لبرلمان: جلسة يوم السبت المقبل ستكون مخصصة لإكمال التصويت على قانون انتخابات مجلس النواب

سبتمبر 22, 2020

عربي
ألمانيا وفرنسا تقدمان 80 مليون يورو لمساعدة فلسطين

دولي
دونالد ترامب يشيد باتفاقية السلام بين الإمارات وإسرائيل

عربي
28 قتيلاً خلال 24 ساعة في معارك بين القوات السورية وداعش

عربي
سعد الحريري يقدم اقتراحاً للخروج من المأزق الحكومي عبر تجرع السم

دولي
دونالد ترامب يشيد باتفاقية السلام بين الإمارات وإسرائيل

سبتمبر 22, 2020

محلي
وزارة النقل: عازمون على تنفيذ مشروع ميناء الفاو الكبير بعمق 19,80 متر

سياسة
قاسم الاعرجي: الأنبار تشهد استقرارا كبيراً في وضعها الأمني

سياسة
قررات مجلس الوزراء للجلسة الاعتيادية برئاسة الكاظمي

سياسة
أحمد ملا طلال: تخصيص ارض في منطقة الجعارة لانشاء المدينة الرياضية

سياسة
قررات مجلس الوزراء للجلسة الاعتيادية برئاسة الكاظمي

سبتمبر 22, 2020

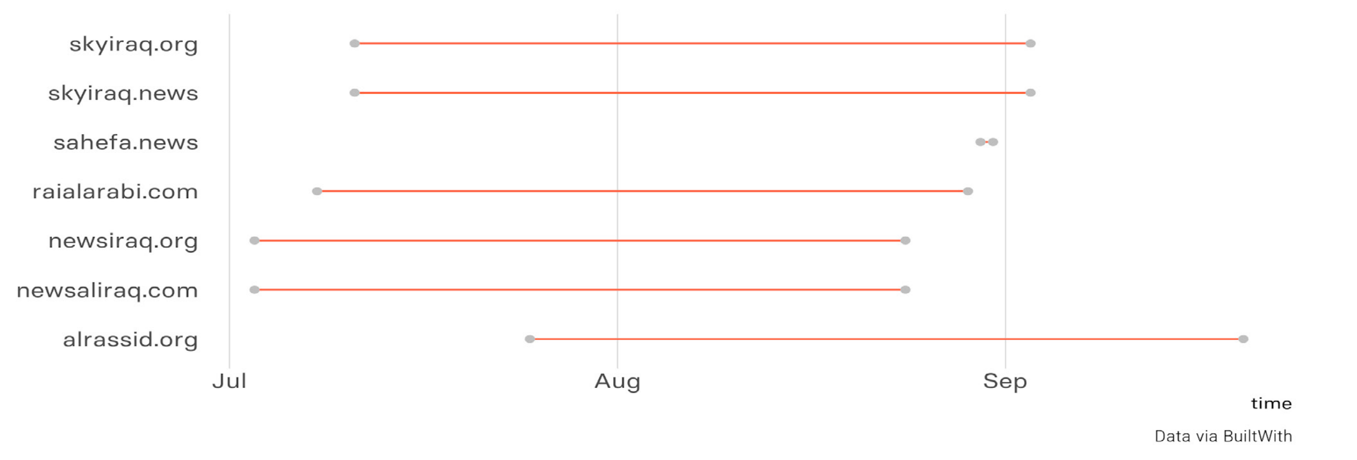
How are the sites connected?

We found several signs suggesting that the sites and their associated social media accounts are connected and coordinated, despite no obvious link between them.

Shared analytics tags

First, we found that seven sites were at one point linked by a Google Adsense code, and two sites were linked by a Google Analytics tag. All seven sites shared a Google Adsense code between July and September 2019 (Figure 8), whereas two sites (skyiraq.news and skyiraq.org) shared a Google Analytics tag between February 2018 and April 2020.

Figure 8: Shared Google Adsense timeline for domains, July to September 2019



Data via BuiltWith

Shared IP infrastructure and metadata

Notably, all but one of the sites are hosted on a server with the IP address 78.128.6.24 (located in Bulgaria). We used a passive DNS tool, *Risk IQ*, to look at the historical links between those sites' domains and IP addresses.

We found that two of the earliest sites were registered between 2013 and 2014, and three other sites were registered between 2015 and 2016. The first two sites (samabaghdad.org and newsaliraq.com) were registered by the same organisation, 'News AlIraq', whereas the three other sites (alrassid.org, sahefa.news and skyiraq.news) were registered by a shared e-mail address. However, all six of the sites share other data, including the same street and state locations. All sites except for one (samabaghdad.org) were updated to the Bulgarian IP in 2019.

Shared metadata for social media accounts

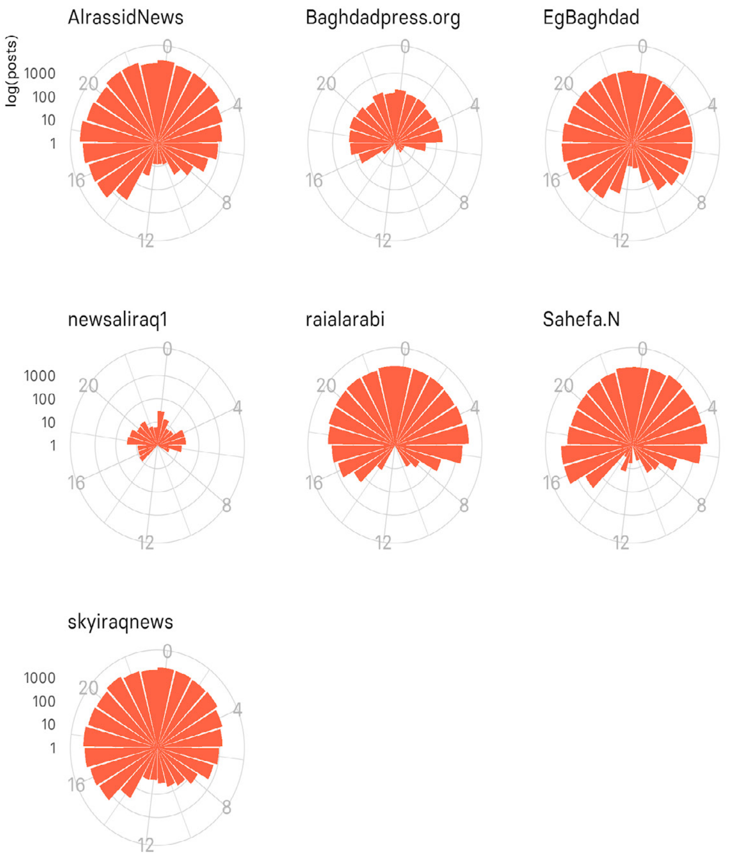
The social media accounts affiliated with these sites also appear to share similar metadata. Four Facebook pages have page administrators located in Turkey, and two pages have administrators located in Austria. All pages have administrators with hidden locations, and one page has an administrator located in Germany. Notably, no page administrators are listed with locations in Iraq (Table 3).

Table 3: Metadata associated with Facebook pages

Page URL	Page created	Page administrator locations
https://www.facebook.com/EgBaghdad/	28 January 2015	Turkey (2), Hidden (7)
https://www.facebook.com/newsaliraq1/	4 February 2015	Hidden (4)
https://www.facebook.com/AlrassidNews	7 January 2016	Turkey (2), Hidden (6)
https://www.facebook.com/skyiraqnews/	1 April 2016	Hidden (4)
https://www.facebook.com/Sahefa.N/	8 October 2016	Austria (2), Turkey (1), Hidden (2)
https://www.facebook.com/raialarabi	28 December 2016	Germany (1), Hidden (5)
https://www.facebook.com/Baghdadpress.org/	11 October 2018	Austria (1), Hidden (1)
https://www.facebook.com/alqishlahNews	28 February 2020	Turkey (2), Hidden (1)

An analysis of posting timestamps by the pages also suggests that they hold closely to the same hourly pattern, posting generally between 16:00 and 08:00, Baghdad time (Figure 9).

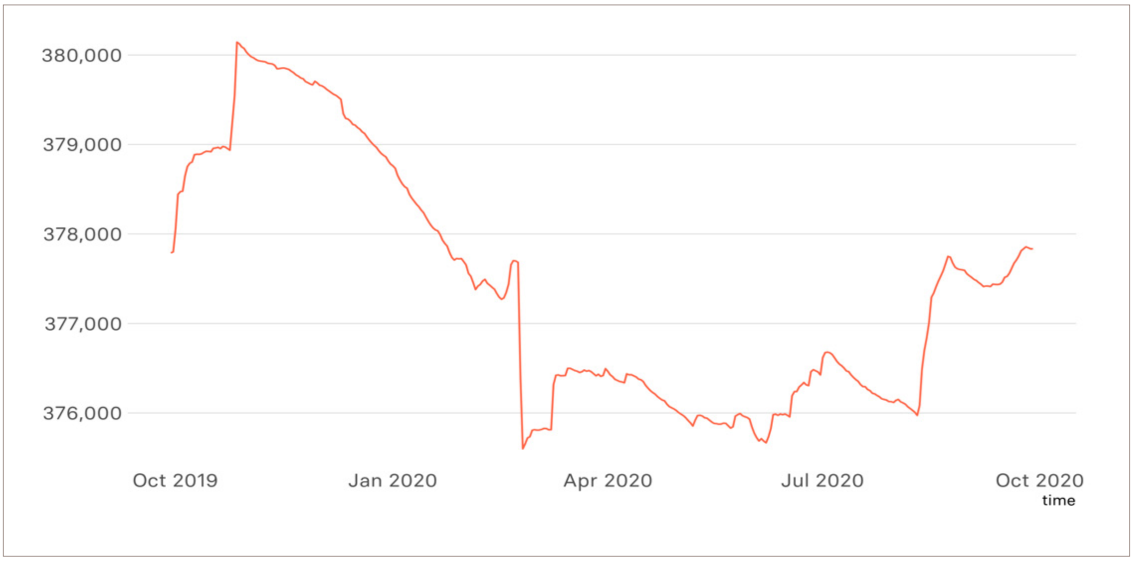
Figure 9: Hourly posting-frequency of Iraqi-focused Facebook pages, between 1 January 2016 and 17 September 2020



Data via CrowdTangle

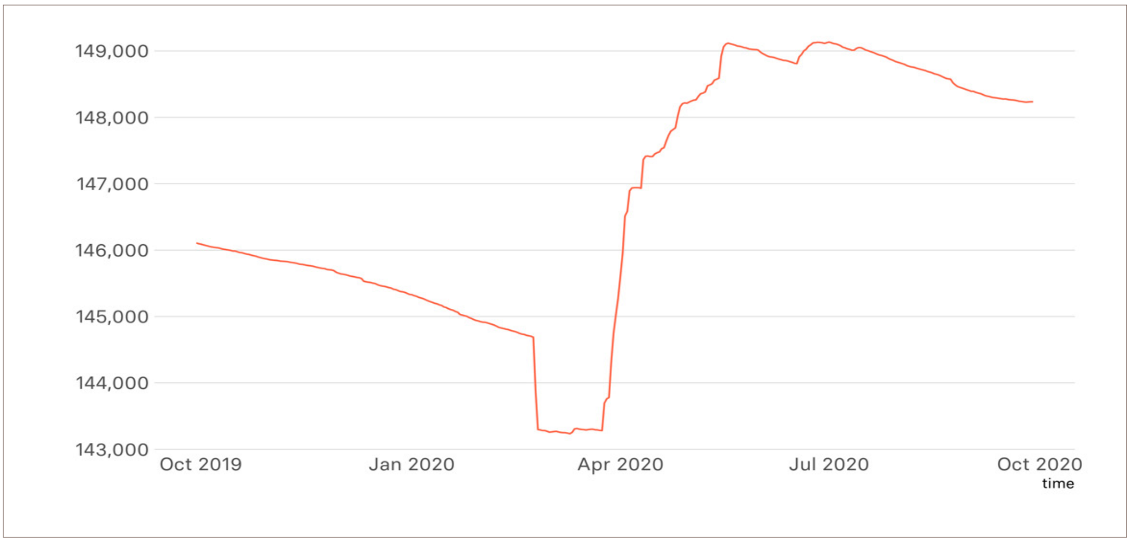
Almost all pages have shown decreases in page likes, and at least two of the pages have shown stark plummets and increases in the number of 'page likes' over time (Figures 10 and 11). When a user likes a page, they effectively agree to see posts from the page in their feeds. The dramatic drops and increases in page likes could be due to the removal of inauthentic accounts liking the pages or artificially boosting them.

Figure 10: Daily page likes for *Bagdad News Agency*



Source: Data via CrowdTangle.

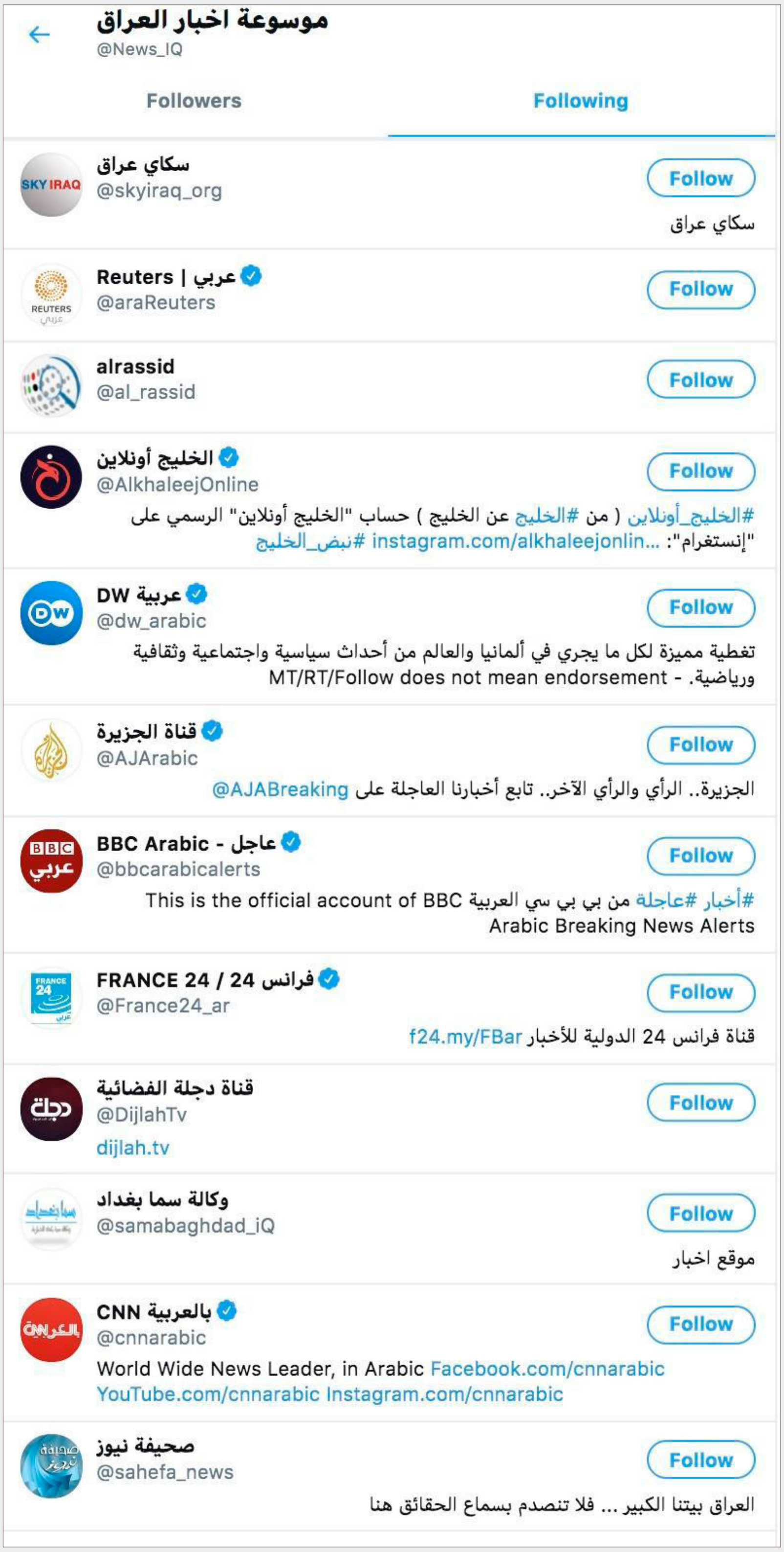
Figure 11: Daily page likes for *Alrassid News*



Source: Data via CrowdTangle.

For almost every site, we also found associated Twitter accounts that showed some association. The Twitter account of *News AlIraq* (@News_IQ) first followed the Twitter accounts of *Sahefa News* (@sahefa_news), SamaBaghdad (@samabaghdad_IQ), and later, Al Rassid (@al_rassid) and Sky Iraq (@skyiraq_org) (Figure 12). Similarly, the *Sahefa News* account would later follow the @News_IQ account, one of few among its friends. Notably, the @samabaghdad_IQ account is inactive, and its most recent retweets were links from the @al_rassid account.

Figure 12: Followers of the @News_IQ Twitter account



موسوعة اخبار العراق
@News_IQ

سكاي عراق
@skyiraq_org
Follow
سكاي عراق

Reuters | عربي
@araReuters
Follow

alrassid
@al_rassid
Follow

الخليج أونلاين
@AlkhaleejOnline
Follow
#الخليج_أونلاين (من #الخليج عن الخليج) حساب "الخليج أونلاين" الرسمي على
"إنستغرام": ...instagram.com/alkhaleejonlin #نبض_الخليج

DW عربية
@dw_arabic
Follow
تغطية مميزة لكل ما يجري في ألمانيا والعالم من أحداث سياسية واجتماعية وثقافية
ورياضية. - MT/RT/Follow does not mean endorsement

قناة الجزيرة
@AJArabic
Follow
الجزيرة.. الرأي والرأي الآخر. تابع أخبارنا العاجلة على @AJABreaking

BBC Arabic - عاجل
@bbcarabicalerts
Follow
#أخبار #عاجلة من بي بي سي العربية This is the official account of BBC
Arabic Breaking News Alerts

FRANCE 24 / 24 فرانس
@France24_ar
Follow
قناة فرانس 24 الدولية للأخبار f24.my/FBar

قناة دجلة الفضائية
@DijlahTv
Follow
dijlah.tv

وكالة سما بغداد
@samabaghdad_iQ
Follow
موقع اخبار

CNN بالعربية
@cnnarabic
Follow
World Wide News Leader, in Arabic Facebook.com/cnnarabic
YouTube.com/cnnarabic Instagram.com/cnnarabic

صحيفة نيوز
@sahefa_news
Follow
العراق بيتنا الكبير ... فلا تنصدم بسماع الحقائق هنا

Summary

In this report, we've leveraged data collected by the EU's East StratCom Task Force to show the targets of pro-Kremlin messaging on Covid-19 and the sites publishing that content, as well as its reach on social media and the primary vectors of that spread. We haven't attempted to investigate every publisher of pro-Kremlin disinformation or analyse any links they may have to other known propaganda outlets. Instead, we've shown how open-source investigators can begin with a set of known sites and use them to advance an investigation using Passive DNS, WHOIS data, web tracking tags and social media data to uncover additional information and links.

Our findings include an analysis of 'media' sites aimed at Iraqi- and Arabic-speaking audiences, connected by a common hosting provider; web tracking tags; and associated social media accounts that share similar metadata and temporal patterns. Nowhere is it apparent that these sites would be otherwise linked. Our goal has been to show the iterative process of an investigation, different analytical methods (text, temporal and network analysis), and the corroborative evidence required to make claims about links between multiple domains. This report should serve as a resource for researchers interested in using open-source databases for future investigations.

Notes

[1] Inclusion in the EUvsDisinfo database doesn't mean that a specific outlet was or is linked to the Kremlin or editorially pro-Kremlin, or that it has intentionally sought to disinform.

[2] Elise Thomas, Albert Zhang, Emilia Currey, *Pro-Russian vaccine politics drives new disinformation narratives*, ASPI, Canberra, 24 August 2020, online.

[3] Facebook, *April 2020 coordinated inauthentic behavior report*, 5 May 2020, online.

Acronyms and abbreviations

EU	European Union
NATO	North Atlantic Treaty Organization
WHO	World Health Organization

About the authors

Ray Serrato is an independent open source investigator and social media analyst researching online disinformation, election integrity and human rights

Dr Jake Wallis is a senior analyst working with the International Cyber Policy Centre.

Acknowledgements

ASPI's International Cyber Policy Centre receives funding from a variety of sources including sponsorship, research and project support from across governments, industry and civil society. ASPI is grateful to the US State Department for providing funding for this research project.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements.

ASPI International Cyber Policy Centre

ASPI's International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber, emerging and critical technologies, issues related to information and foreign interference and focuses on the impact these issues have on broader strategic policy. The centre has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building, satellite analysis, surveillance and China-related issues.

The ICPC informs public debate in the Indo-Pacific region and supports public policy development by producing original, empirical, data-driven research. The ICPC enriches regional debates by collaborating with research institutes from around the world and by bringing leading global experts to Australia, including through fellowships. To develop capability in Australia and across the Indo-Pacific region, the ICPC has a capacity building team that conducts workshops, training programs and large-scale exercises for the public and private sectors.

We would like to thank all of those who support and contribute to the ICPC with their time, intellect and passion for the topics we work on. If you would like to support the work of the centre please contact: icpc@aspi.org.au

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional.

ASPI

Tel +61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC

First published October 2020.

ISSN 2209-9689 (online), ISSN 2209-9670 (print)

A S P I
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

INTERNATIONAL
CYBER POLICY
CENTRE

Funding for this report was provided by the US State Department

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

INTERNATIONAL
CYBER POLICY
CENTRE