Research Article

Mona Elswah*, Mahsa Alimardani

Propaganda Chimera: Unpacking the Iranian Perception Information Operations in the Arab World

<https://doi.org/10.1515/opis-2020-0122>

received February 3, 2021; accepted August 11, 2021.

Abstract: In the past four years, Iranian Information Operations (IOs) have received a lot of scrutiny by social media companies and policymakers. From 2018 to 2021, several accounts on Twitter, Facebook, and Instagram were taken down by tech companies for engaging in coordinated inauthentic behaviour. Despite the heated relationship between Iran and many Arab countries, the Iranian IOs in the Arabic online sphere have received less academic attention over the years. This study fills this gap by being one of the few studies to investigate the Iranian IOs in the Arab world. We analyse more than 9.3 million tweets posted from 2008 to 2020 using the hashed datasets shared by Twitter’s Election Integrity Hub. We found that Iran’s IOs have made the Arab world its primary target—despite the attention the US claims to receive from them. However, these IOs demonstrate very little engagement and reach amongst Arab users, limiting the possibilities of Iran infiltrating the online Arabic sphere, and fostering weak yet unruly Arab counterpublics. This study argues that Iran’s IOs garner their power from being perceived as efficient and dangerous operations that could pollute the public sphere of overseas nations, rather than through actual infiltration through engagement. We understand Iran’s efforts to be preoccupied with old propaganda efforts, through their investment in websites and imitation of news organisations. However, their efforts prove that Iran adopted the tactics of “new propaganda” that depend on creating a perceived atmosphere of distrust and chaos. We contribute to the discussion on information operations by proposing the term “perception IOs”, referring to IOs by governments that aspire to be perceived as effective meddling countries in foreign politics.

Keywords: Information Operations; Iran; the Arab World; Twitter; Perception IOs; and propaganda.

1 Introduction

In the past four years, Iranian Information Operations (IOs) have brought attention to themselves. This includes news about their role in hijacking the US elections, targeting foreign audiences, and polluting the online public sphere with attempts at fostering unruly counterpublics. Researchers and policymakers have heavily emphasized Iran’s role as a significant factor behind foreign influence campaigns. These concerns have led social media platforms to take countermeasures against Iranian foreign content by labelling Iranian English-language state-media outlets and taking down more accounts involved in IOs. Besides, governments have also enforced additional measures to limit Iranian online interference. For example, the US government has seized more than one hundred Internet domains in 2020 associated with Iranian IOs (Warminsky, 2020).

Iran has always aspired to maintain a strong presence in the Arab world to defy its regional rivals, using a variety of soft and sharp power tools. In addition, Iran has supported several TV stations to achieve its soft power ambitions in the Arab world. Iran currently supports several Arabic-speaking TV channels like *Al-Alam* TV and *Al-Manar*¹ in addition to many other outlets (Friedman, 2012). Since the 2011 Arab Spring, Iran’s involvement in the region has become more

*Corresponding author: Mona Elswah, University of Oxford, Oxford, Oxfordshire, United Kingdom, E-mail: mona.elswah@oii.ox.ac.uk
Mahsa Alimardani, University of Oxford, Oxford, Oxfordshire, United Kingdom,

prominent in Bahrain, Syria, and Yemen (Elswah, Howard, and Narayanan, 2019). Benefiting from the affordances of social media platforms, Iran sponsored campaigns that target Internet users all over the world. However, the Iranian IOs attempting to manipulate the Arabic online sphere have largely gone understudied in academia.

In this study, we analyse six hashed datasets of tweets identified by Twitter as Iranian IOs from 2008 to 2020, measuring their tactics, targets, and engagement. Despite the media focus Iranian meddling has received as a threat to the US (Timberg and Romm, 2019; Barnes and Sanger, 2020), we found that Iranian IOs focus more on the Arab world, primarily targeting countries like Lebanon, Egypt, Bahrain, Algeria, and Saudi Arabia—a list of countries with Iran's rivalries and proxies, unlike other countries in the region which are either not of strategic importance or are already firmly under their influence. In this study, we argue that although the Iranian IOs we examine aspired to pollute the Arabic online sphere, their attempts were failing to engage Arab users over the years. We name Iran's efforts as *perception information operations (IOs)*, meaning that the power of the Iranian IOs stems from being perceived as powerful and impactful meddler, creating a sense of incursion and influence in foreign politics. Perception IOs aim to give the mostly false sense of counterpublics and chaos in their targeted country. What these Iranian IOs do accomplish is to position Iran as a powerful country that could skew the public opinion of Arab audiences, sowing distrust instead of actually embedding the false narratives. We contribute to the information operations literature by arguing that researchers need to distinguish between the *perceived* and the *actual* threat while investigating online political meddling.

2 Public Sphere, Social Media, and Information Operations

The work of the German Philosopher Jürgen Habermas attempted to explain the role of the public sphere in forming a democracy. In Habermas's concept, the public sphere refers to the unrestricted social realm accessible to all citizens away from the state's intervention (Habermas, Lennox & Lennox, 1974; Lunt & Livingstone, 2013). While Habermas's conception of the public sphere is important to our understanding of the impact of IOs within Arab countries, it is important to understand the limits of what Habermas provides. Reconceiving the notion of the public sphere is important, especially in understanding the impact of IOs. Habermas's theory of the public sphere deals with an orderly deliberation within a backdrop of white, male, European bourgeois in the midst of peace and social order (Calhoun, 1992).

Understanding how foreign state information operations work within Middle Eastern authoritarian settings needs to start at the point of understanding that the lack of trust is a major impediment in democratic deliberation. Unlike traditional media, social media has enabled horizontal communication, unencumbered by previous authoritarian gatekeepers, that ensured equality and engagement of citizens and empowered various voices (Abdulla, 2014). Social media has created the “new public sphere” where people can interact and exchange ideas, especially in highly censored countries (Lynch, 2012). However, the horizontal flows of communication do not manifest within the frameworks of democratic deliberation Habermas envisioned. At its core Habermas's public sphere privileges rational deliberation through speech as the exclusive mode of communication in the public sphere. The recent online transformations, with the prevalence of IOs, are defining these dynamics and even mere existence of “rational deliberation” globally. In the western context, it means that the public sphere is “vulnerable to disinformation, propaganda, and just sheer bullshit” (Benkler, Farris, and Roberts, 2018).

Before we tackle the role of online propaganda, we should first examine the role of democracy within the online Arabic public sphere. Important contributions have been made in understanding the role of information and communication technologies (ICTs) in democracy building. Many studies from the early 2010s were caught up in a positivist approach for the role of ICTs. Iran's Green Movement and the 2011 Arab Spring protests had cemented the role of ICTs as a force for political change (Schiffrin, 2017). The discussion surrounding the role of the ICTs in contexts within the Middle East and North Africa (MENA) region was furthered by the work done in relation to the 2011 Arab Spring. This was in turn helping to hold MENA governments more accountable and nurturing the public sphere. However, at a similar moment, other researchers have given less credit to social media in mobilizing the 2011 protest events. Evgeny Morozov's *The Net Delusion* attempted to puncture the techno-utopian bubble, by arguing governments could similarly use ICTs for their own propaganda or to monitor their opposition (2011).

Indeed, governments attempted to control this new public sphere to impose their hegemony on the online spaces. Domestic and foreign information operations intended to hijack these new spaces, by either limiting access to them or manipulating their discussions. Scholars have raised concerns about the power of IOs in dominating the online sphere and skewing public opinion (Narayanan, Howard, Bence, Elswah, 2017; Bradshaw & Howard, 2019). With the rise of the IO field, spurred on by activities associated with Russia, studies have placed an undue focus on the breakdown of trust in Western institutions in what has been known as an “information disorder” (Wardle & Derakhshan, 2017).

However, one other theory that we are using to understand the effects of disinformation within the online public sphere is the one proposed by one of Habermas’s most notable critics, Nancy Fraser and her theory of *counterpublics*. Counterpublics refer to “the parallel discursive arenas where members of subordinated social groups invent and circulate counter discourses to formulate oppositional interpretations of their identities, interests and needs” (Fraser, 1990). Fraser saw their “function as bases and training grounds for agitational activities directed toward wider publics” (Fraser, 1990). Counterpublics have already been configured as important theoretical frameworks for dealing with “unruly publics” especially those waging online disinformation efforts (Bjola and Papadakis, 2020; Kaiser and Rauchfleisch, 2019). We explore the role of Iran as the “unruly actor” within the Arabic public sphere.

Much of the empirical work on IOs has been focused on foreign campaigns targeting the US or Europe with a few exceptions in the Arab region. However, the intent and effects of disinformation campaigns aimed at non-Western societies have had relatively little study in academia. While in democratic contexts, digital propaganda’s role in creating these counterpublics often translates into compromising the democratic process. In authoritarian contexts, digital propaganda is meant to question the control or legitimacy of the state. The nature of this new “information disorder” might be new and novel in democratic societies, meanwhile the strategies of information control have long been woven into the fabric of authoritarian governments (Maréchal, 2017; Alimardani and Milan, 2018).

The empirical work done in relation to IOs in the Arab world have been centred on Syria and the Qatar blockade. Studies have found that the Syrian White Helmets — a volunteer humanitarian and civil defence group in the rebel held areas in Syria — have been a target of cross-platform smear campaigns sponsored mainly by the Syrian regime and Russia (Starbird et al., 2017; Pacheco et al., 2020; Cosentino, 2020). Other studies have uncovered IO campaigns during the Qatar diplomatic crisis by the neighbouring Arab blockade countries (Jones, 2019; Alli, 2019). These campaigns used bots, fake news, and promoted anti-Qatar tweets (Jones, 2019). Despite the growing attention to the field of IO in the region, many operations remain understudied.

3 The Evolution of Iranian Information Operations

With the growing importance of digital technologies, Iran has worked to harness the power of social media. Domestic IO campaigns in Iran, particularly those focused on controlling the narrative of the COVID19 outbreak, were seen to manifest on popular platforms in Iran such as Telegram and Instagram (Alimardani and Elswah, 2020a; 2020b). Much media focus, state-led inquiries and alarm have been placed on Iran’s foreign targeted IO campaigns.

Despite the attention Russian operations achieved in 2016, Iranian IOs were only uncovered in August 2018 when Facebook removed 652 pages, groups, and accounts originating from Iran for engaging in “coordinated inauthentic behaviour” (Facebook News, 2018). Following that, Twitter announced the suspension of the first takedown of 770 accounts in the same month (Gadde and Roth, 2018). These accounts promoted pro-Iranian government messages and acted as amplifiers of news websites that promoted Iran’s political agendas (Elswah et al., 2019). An analysis of the English-language tweets promoted by the early Iranian operations has shown that they were intending to promote an anti-US sentiment among American users by impersonating news outlets and amplifying links to third-party websites tied to the IRIB (Blondet, 2018). Further analysis of Iran’s Arabic-language tweets has found similar evidence. Researchers found that Iranian IO accounts were using Modern Standard Arabic *Fusha* to engage Arab users (Elswah et al., 2019). These early campaigns demonstrated low engagement, distinguishing these efforts from the Russian IOs which usually received higher levels (Elswah et al., 2019; Howard et al., 2018; Brooking & Kianpour, 2020).

From August 2018 to December 2020, six more information operations associated with Iran were detected on Twitter and six others on Facebook (Twitter Election Integrity Hub, 2021 & Facebook News, 2021). Following the killing of the Iranian commander Qasem Soleimani in January 2020, Iranian IOs escalated on Twitter, Instagram, and Facebook,

aiming to infiltrate American users (Guynn, 2020). Thus, social media platforms have taken down more accounts that originated in Iran suspected of being Iranian operations (Robinson & Sardarizadeh, 2020).

Closer to the 2020 US presidential election date, fears of Iranian interference pervaded briefings from the US government and media headlines. Iranian IOs during the US Presidential elections involved “perception hacks” (Barnes and Sanger, 2020; Gleicher, 2020). This operation was called a “perception hack” because of the limited sophistication of the campaign and its effectiveness relying not on the actual campaign but on the perceptions created through media and political hype. To run this operation, Iran used the US voter registration information, which is mostly available online, to threaten American voters to vote for Trump. Immediately this IO made headline news and elicited a response from the US Department of Justice. Iran evoked the *perception* of meddling in American democracy and undermining the overall trust in it (Barnes and Sanger, 2020), emulating the Russian model of “new propaganda”.

In its original conception, “old propaganda” efforts were created to manipulate target audiences towards a predetermined direction (Cull et al., 2003; Bjola and Papadakis, 2020). What has been deemed as the “new propaganda” that is defining sophisticated online influence operations is not to drive a specific agenda or view, but rather to generate a sense of scepticism in the public sphere. This “new propaganda” agenda has largely defined the influence operations led by Russia against Western democracies during the past decade (Mejias and Vokuev, 2017; Bjola and Papadakis, 2020). The Russian efforts have been seen as detrimental to the foundations of American or European democracies, as it has worked to destroy trust (Ramsay, 2019; Ramsay and Robertshaw, 2019).

This study, however, explores Iran’s strategy as it targets its regional Arab neighbours—typically non-democratic, or authoritarian states, in its effort to foster counterpublics. Here, we will explore whether there has been any growth from the initial understanding of Iran’s ineffective “old propaganda” model.

Trying to understand this understudied topic of how Iranian IOs target the Arab world we ask: to what extent Iranian IOs are present in the Arabic online sphere? What are the main tactics the IOs are using to manipulate Arab users on Twitter? And how are these IOs engaging with the users in the Arab world? This is one of the few studies that explores Iranian digital interference in the Arab world on a large scale.

4 Data and Analysis

To unpack the Iranian IOs in the Arab world, we analysed six Twitter datasets, released from October 2018 to October 2020 to understand Iran’s dominance in this online sphere using R script. Twitter’s Transparency Center provides this hashed data to academic researchers and policymakers. Due to the lack of access or releases from Facebook regarding similar accounts or campaigns, our focus is limited to operations on Twitter. Although Twitter is not the most popular platform in North African countries, it is among the most visited websites in Gulf countries, especially in Saudi Arabia (Statista, 2020). Twitter’s presence in the region for a number of years also means we can track the evolution of Iranian IOs overtime. We used the publicly available data on Twitter’s Election Integrity Hub—a platform Twitter launched to share hashed data of suspended accounts that were part of state-sponsored information operations. In the Iranian takedowns and according to Twitter, Iranian IOs have created accounts with a wider range of personas to artificially amplify the Iranian messages and narratives.

In these datasets, accounts with less than 5,000 followers were hashed and anonymized by Twitter to protect the accounts’ privacy and avoid any possible false positives. Twitter does not usually identify how the platform detected the IOs but they allow users to appeal if they were mistakenly included in any of the takedowns. In some cases, Twitter spotted these IOs in collaboration with cybersecurity firms and industry peers.

The datasets we examined in this study included profile information, Tweet texts, URLs shared, hashtags, and media (e.g., images and videos) from accounts that were suspended. Our study examined the most shared URLs, a majority of which belonged to expired or seized domains. We explored the content and themes of the seized or expired domains through the last available screen grab taken by the Internet Archive Wayback Machine (see Appendix, images 1-5).² To the date of writing this paper, Twitter has shared hashed six datasets of tweets related to Iran, comprising more than nine million tweets in about 65 different languages. In the coming sections, we divide our analysis into influence tactics, targets, and engagement levels.

4.1 Detecting Influence Tactics

To answer our first research question regarding the scale of the interference in the Arab world compared with other regions, we analysed the proportion of the Arabic tweets in the 9.3 million hashed tweet datasets. We found that Arabic was the most used language in the tweets that targeted various global audiences (see Figure 1). Out of the 9,317,279 tweets, there were more than two million tweets in Arabic, English was the second language, with just under two million tweets, and then followed by Persian, with nearly one and a half million tweets.

The Iranian IOs used four main tactics to influence Arab Twitter users. First, directing Arab users to third-party websites that are in line with Iran's foreign policy in the Arab world. About 30% ($n = 642,209$) of the Arabic tweets included URLs to third-party websites. More than 150,000 of these URLs were using link shorteners such as TinyURL and Goo.gl. After expanding these links, we found that all the URLs shared by Iranian accounts in the Arabic tweets directed to about 2,030 unique domains.

When we analysed the most shared websites (see table 1.1), we found that most of them were directed to expired, compromised, or seized domains. Aside from social media websites, most of the websites in table 1.1 were linked to Iran in previous work (Elsawah et al., 2019, Stubbs & Bing, 2018). The most frequently shared domain name was *nilenetonline*, which targeted Egyptian users to represent the Egyptian government as weak and inefficient. This website was shared by the IOs from 2012 until 2018 in the Arabic tweets in our data. Also, *Alwaienews* and *alarabiya24* were promoting an anti-Saudi sentiment, *countdown2040* wrote about Israel, and *al-hadath24* and *Jordan-times* focused on different countries in the Arab world. Previous studies of Iranian disinformation networks also indicated *countdown2040* to be a central reference for "Iranian trolls" when promoting disinformation, coming second only to Iran's English state-run media, PressTV (Al-Rawi, 2021).

The second tactic we observed was the imitation of website names. Similarly, this tactic was observed in previous Iranian domestic campaigns to discredit the BBC Persian and their staff. In 2013, a website emulating BBC Persian using the domain *persianbbc.ir* was discovered spreading smears (Dehghan, 2013). The most shared website in this dataset of the Arabic tweets we analysed was *nilenetonline*. This website imitated the name of the famous Egyptian TV channel Nile TV, which is run by Egypt's public broadcaster *Maspero*. Similarly, *al-hadath24* and *alarabiya24* imitate the Saudi *Al-Hadath* and *Al-Arabiya* channels. In addition, these Iranian IOs acquired different Top-Level Domains (TLDs) for the same domain names. We found in the dataset that the IOs shared URLs to the same domain names with different TLDs such as *nilenetonline.com*, *nilenetonline.net*, *nilenetonline.org*, *qudspal.com*³, *qudspal.net*, *qudspal.org*, *hourriya-tagheer.org*, *hourriya-tagheer.com*, *hourriya-tagheer.net*, *hourriya-tagheer.org*.

The third tactic we observed was creating a cross-platform disinformation campaign. Although the data we analysed was from Twitter, the top shared URLs aimed to direct Arab Twitter users to pages and accounts on Facebook and YouTube. When we expanded the shortened URLs, we found thousands of links that led to Instagram, Soundcloud, Change.org, Vimeo, WhatsApp groups, and Telegram channels. This shows that the Iranian IOs are well-established beyond Twitter in the Arabic online sphere.

Unlike previous analysis of the first takedown (Elsawah et al., 2019) that showed that Iranian IOs relied on impersonating regional news outlets on Twitter, we found in these datasets that this strategy was less salient. The majority of the top active accounts (table 1.2) impersonated Twitter users from Bahrain, Iran, Lebanon, and Saudi Arabia. Also, in an earlier analysis, researchers found that the Arabic used by Iranian IO accounts were only Modern Standard Arabic. When we analysed these larger datasets that comprised different IO operations, we found that Tweets were written in both the Modern Standard and Dialectical Arabic. The pivot towards more citizen voices, as opposed to "news" sources indicates a mishmash of strategies. By analysing these large datasets, we can say that there were varying efforts by the Iranian IOs, and that they often did not follow a standard strategy to skew public opinion. These chaotic tactics and strategies might indicate a decentralised system behind these operations, whereby various different institutions within the Iranian state are behind these operations. This gives merit to what has long been suspected about Iranian actors in the IO space. Iran does not have one specific institution responsible for online information operations. Elements within Iran's Ministry of Intelligence and Revolutionary Guards have been linked with online operations. Other evidence such as parliamentary budget reports have indicated the Supreme Leader controlled Islamic Development organisation is likely behind online disinformation campaigns (Alimardani, 2021; IRNA, 2021), alongside government contractors such as the Masaf Institute and its founder Aliakbar Raefipour (Abuzar and Grossman, 2020).

Top five languages in Iranian IOs on Twitter **Figure 1:** Distribution of languages in the tweets in the Iranian IOs.

Source: Authors' analysis of the IO data available on Twitter Election Integrity Hub

Table 1.1: Top ten domains promoted by the Arabic Tweets.

Domain	~No. of times shared	Description	Domain Status
nilenetonline.com	92, 440	News website with interest in Egyptian affairs	Seized by the US Justice Department
youtube.com	35, 647	Social Media Platform	Active
twitter.com	35, 609	Social Media Platform	Active
facebook.com	31, 367	Social Media Platform	Active
countdown2040.com	26, 587	Blog with an anti-Israel sentiment	Expired
al-hadath24.com	25, 050	News website that focused on different countries in the Arab world	Expired
hourriya-tagheer.org	19, 089	News website with a focus on Saudi Arabia	Active
jordan-times.com	14, 956	News website that focused on different countries in the Arab world	Expired
alarabiya24.com	14, 613	News website that imitated the Saudi-funded Al Arabiya channel	Expired
alwaienews.net	14, 289	News website that focused on Saudi Arabia	Expired

Source: Authors' analysis of the IO data available on Twitter Election Integrity Hub.

Table 1.2: Top Ten Active Accounts in the Arabic dataset.

Screen Name	Profile Description	No. of Tweets	Reported Geolocation
siddiq_31	Justice For Everyone. No for sectarianism. People are two types: either a brother in faith or your counterpart in humanity (RT ≠ endorsement)	186,249	Bahrain
Maleka___M	I am the time of victories. I have fists for knowledge. I am for knowledge (RT ≠ endorsement)	157,261	NA
LailaMII	NA	156,756	Southern Lebanon
djXIHhnPuf6vbf2FLM-kUrX476KZeby4B2Ei-a99E+Xs=	O Allah, bless Muhammad and his family and hasten their relief	138,985	Islamic Republic of Iran
NileNetNews	Nile net news # news from # Egypt and the Maghreb. World news and news from # Mauritania, Libya, Tunisia and Algeria	131,50	Egypt
mohamadezdine	A writer from Lebanon? If Lebanon were not my homeland, I would have chosen Lebanon as my home	78,076	Lebanon, Beirut
Danielliban024	From Southern Lebanon. I vowed my blood for the sacrifice of the unjustly slaughtered people. I vowed my letters to Yemen, my prayer for the people of Bahrain, for Syria and Iraq, and all my love as long as I live in my tweets	68,142	In the heart of every honest free person
_jafar313	{And We wished to do a favour to those who were weak in the land, and to make them rulers and to make them the inheritors}	59,452	Nasiriyah
malak73366640	NA	58,072	NA
alsudanalyoum	A comprehensive Sudanese website ... local and international news - political, cultural and sports articles - opinion columns -features - reports	53,627	Saudi Arabia

Source: Authors' analysis of the IO's data available on Twitter Election Integrity Hub

Note: The accounts' descriptions were translated into English. One of these accounts was hashed by Twitter.

4.2 Targets of the Iranian IOs in the Arab World

The earliest Arabic tweet in this Iranian IO was written on the 20th of November in 2011 by an account that masqueraded as a Bahraini news outlet, supporting the Bahraini uprising. The last date of tweeting was on the 1st of July 2020 with an account geolocated to Kuwait, discussing the spread of the Covid19 virus in Kuwait among athletes.

This data of suspended IO accounts found the height of its tweet activity during the period from June 2017 till the end of 2018 (See Figure 2). A timeframe that matches the blockade or what was known as the “Qatar Diplomatic Crisis.” More than 30% of the Arabic tweets in this dataset were only written between June 2017 to December 2017.

To identify the targeted countries in the Arab world, we analyzed the top hashtags in the Arabic tweets. We found that the most popular hashtags were about Bahrain, Palestine, Rohingya Muslims, Saudi Arabia, and Algeria (See table 1.3). We also found that the majority of tweets were coming from accounts that claim to be located in Bahrain, Saudi Arabia, Iran, Lebanon, and Egypt. This shows that the Iranian IOs interest went beyond Saudi Arabia and included other countries in the region that are of interest to the Islamic Republic's foreign policy interests (Elsawah et al., 2019).

4.3 Engagement Garnered by IOs

The 2.1 million Arabic tweets were produced by only 2,723 accounts. Ten accounts have produced more than 50% of the Arabic tweets (see Table 1.1). These accounts have failed to produce high engagement rates over the years. When we

Figure 2: Frequency of Arabic Tweets by Iranian IOs by month.

Source: Authors' analysis of the IO data available on Twitter Election Integrity Hub

Table 1.3: Top Ten Frequent Hashtags use by IOs.

Hashtag	Translated hashtag	No. of tweets associated with the hashtag
Bahrain	Bahrain	21,377
البحرين	Bahrain	18,137
قروب_فلسطيني	Palestinian_Group	8,710
الصهيونية_تسقط	Zionism is down	4,689
بالمعادلة_الذهبية_انتصرنا	With the golden equation, we won	4,075
بني_جمرة4	Bani Jamra	3,975
الروهينغا_الابادة_الصامتة	Rohingya_silent_eradication	3,929
الحرب_الفاشله	Failed_war	3,572
السعودية	Saudi Arabia	3,323
الجزائر	Algeria	2,955

Source: Authors' analysis of the IO's data available on Twitter Election Integrity Hub

Note: Some of these hashtags were translated into English by the authors.

calculated the engagement points—retweets, likes, replies, and quote tweets—across our data, we found that the most engaging Arabic tweet received 2,272 engagement points. More than 86% of the Arabic tweets received zero engagement points ($n = 1,868,508$ tweets).

Also, the average engagement level was 1.7 points across all the Arabic tweets, showing that the Iranian IOs have not succeeded in reaching Arab users despite their high levels of tweeting (see Figure 3). What is notable in terms of engagement, however, was that despite the increase of tweets coming out during the time period of the Qatar Diplomatic Crisis, the levels of engagement with Iranian IO accounts remained at similar levels (see Figure 3). This likely indicates that regardless of the resource or effort, there seemed to be very little appetite for the content of the Iranian IOs.

Figure 3: Engagement with Arabic tweets in the Iranian IOs.

Source: Data collected from Twitter's Election Integrity Hub.

5 Discussion

Previous studies had indicated website-based IOs have been a favoured tactic by Iran (Elsawah et al., 2019; Lim et al., 2019). In this study, we indicated about 30% of the Arabic tweets heavily relied on this tactic. We also noticed that the most popular websites being shared within this dataset maintain uncanny resemblance in both name and branding to popular news outlets in the Arab world. This strategy has been a hallmark of Iranian disinformation efforts. Although it is hard to understand the impact of these websites on shaping public opinion, the evolution of the IO strategies away from the fake websites indicates a shift by this state. Researchers of IOs typically find it difficult to assess the precise impact of campaigns, given the limitations and data regarding viewership or reach of content beyond likes, quote tweets or retweets. When analysing engagement rates with the data Twitter has provided, we are not given a complete picture of the potential reach of the IOs amongst its targeted audience, which is a limitation of this study.

The better use of Arabic and local dialects that we found in the data demonstrates the varying tactics amongst these Iranian operations. This perhaps indicates that there are different institutions or actors within the Iranian state, with different language resources and skills responsible for these IOs. However, the generally low levels of engagement indicate very little viewership amongst Arab users. This could have had a different ability to infect the Arabic public sphere and foster effective counterpublics. Also, new datasets have revealed more sophisticated tactics amongst Iran's IOs, opposed to the website focused strategies.

This attention given to Iranian IOs is often at a level that mismatches the actual engagement of these operations. There have been a few studies prior to this that looked to empirically assess the methods and impact of Iranian IOs (Elsawah et al., 2019; Lim et al., 2019). Yet the number of non-empirical research studies commissioned from DC based think tanks and US media firms that concentrate on Iran is part of a wider issue. Narges Bajoghli defines it as the "predominant framework of US national security" that perpetuates at worst misinformation and at best a narrow view on a complex terrain" (2019). We argue, however, that these perspectives that dominate Western and Arab media and research discourses might give more weight to the power of Iranian IOs. While engagement of the Iranian IOs generally seem low, the sensationalism created around these operations lend themselves to the perception of the effective counterpublics.

Iranian IOs do not hide their traces properly. The accounts related to these operations were not hiding their political affiliations in many instances. Within Iran's original URL-based campaigns, accounts associated with the websites were easily identified to be tied to the Iranian state (Elsawah et al., 2019). This might indicate that the IO wanted to either get caught or that they were only targeting Iran-sympathetic Arabs. This uncertainty over how an account can be inauthentic

when its identity is transparent lends itself to the problems of lack of attribution disclosures by Twitter. This is perhaps the biggest limitation of this study -the lack of transparency in the methods of attribution. This leads us to question whether accounts might just authentically be ideologically aligned with Iran through personal connections rather than being inauthentic and part of a wider IO. These hesitations underline why it is of significant interest for researchers and policymakers for Twitter to document its attribution standards and methods. The documentation of evidence that associates these accounts to the Iranian government would help researchers understand the tactics performed by Iranian IOs. This would in turn help deflate the *perception* that this cultivation of Arabic online counterpublics poses a far greater threat than the actual efforts of their campaign.

6 Conclusion

As our study delved into the relationship between Iran, an influence operator, and its foreign target adversaries, we examined the Iranian IOs' extent, intent, and impact. Information operations increasingly have shaped themselves into a new form of new propaganda, whose flag bearer is Russia. In the context of this study, we frame these efforts as part of counterpublics within the Arabic public sphere. Counterpublics are about groups, or in this case state actors, seeking to use themes and topics to undermine or even block the functioning of the public sphere.

While much has been studied about the dangers posed to democracies and elections in Western contexts, very little has been done to understand what foreign IO campaigns in non-western settings. Iranian IOs against the Arab world have brought us to three conclusions. Firstly, the primary target of Iranian IOs was the Arab world through their emphasis on Arabic tweets in the datasets. Secondly, there is an old propaganda tactic that Iran has employed, known as imitation websites. Imitation websites have been a hallmark of many campaigns associated with Iran, including target audiences within Iran. Thirdly, the IOs adopted more tactics than what researchers analysed before. Fourthly, our concluding assessment of these new propaganda techniques is that the IOs do not necessarily require high engagement with users. Their presence is felt, and thus *perceived*, by taking advantage of the sensationalism associated with Iran as a bad actor. The IOs campaigns are defined by amplification— what we refer to as “perception IOs”. Here Iran has found utility in a chimaera of propaganda. They have harnessed the power of the perception of their meddling in the Arab world to create fear and distrust through their unruly counterpublics.

Notes

1. A channel supported by the Iranian backed Hezbollah party in Lebanon
2. <https://web.archive.org/>
3. A website that was seized by the US Justice Department in 2020 for its association with the Iranian IOs. It has been shared in the Arabic tweets more than 11, 684
4. A city in Bahrain.

References

- Abdulla, R. (2014). *Egypt's media in the midst of revolution*. Carnegie Endowment for International Peace. <https://carnegieendowment.org/2014/07/16/egypt-s-media-in-midst-of-revolution-pub-56164>
- Al-Rawi, A. (2021). How did Russian and Iranian trolls' disinformation toward Canadian issues diverge and converge? *Digital War*. <https://doi.org/10.1057/s42984-020-00029-4>
- Alli, A. (2019). *Khaleeji Weaponization of Twitter: Case of Gatari Blockade* [M.A., Hamad Bin Khalifa University (Qatar)]. <https://www.proquest.com/docview/2225348159/abstract/5753B8A2604F4A88PQ/1>
- Alimardani, M., & Elswah, M. (2020a). *Trust, Religion, and Politics: Coronavirus Misinformation in Iran* (SSRN Scholarly Paper ID 3634677). Social Science Research Network. <https://doi.org/10.2139/ssrn.3634677>
- Alimardani, M., & Elswah, M. (2020b). Online Temptations: COVID-19 and Religious Misinformation in the MENA Region. *Social Media + Society*, 6(3), 2056305120948251. <https://doi.org/10.1177/2056305120948251>

- Alimardani, M., & Milan, S. (2018). The Internet as a Global/Local Site of Contestation: The Case of Iran. In E. Peeren, R. Celikates, J. de Kloet, & T. Poell (Eds.), *Global Cultures of Contestation: Mobility, Sustainability, Aesthetics & Connectivity* (pp. 171–192). Springer International Publishing. https://doi.org/10.1007/978-3-319-63982-6_9
- Barnes, J. E., & Sanger, D. E. (2020, October 22). Iran and Russia Seek to Influence Election in Final Days, US Officials Warn. *The New York Times*. <https://www.nytimes.com/2020/10/21/us/politics/iran-russia-election-interference.html>
- Bajoghli, N. (2019). American Media on Iran: Hostage to a Worldview. *Anthropology Now*, 11(3), 31–38. <https://doi.org/10.1080/19428200.2019.1747886>
- Benkler, Y., R. Farris, and H. Roberts (2018) Network propaganda (Oxford: Oxford University Press, Oxford)
- Bjola, C., & Papadakis, K. (2020). Digital propaganda, counterpublics and the disruption of the public sphere: The Finnish approach to building digital resilience. *Cambridge Review of International Affairs*, 33(5), 638–666. <https://doi.org/10.1080/09557571.2019.1704221>
- Blondet, E. (2018). Facebook and Twitter Eye Iran in Latest Fake Account Crackdown. *Wired*. <https://www.wired.com/story/facebook-twitter-eye-iran-fake-account-crackdown/>
- Bradshaw, S., & Howard, P. N. (2019). *The Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation* (Working Paper 2019.3.). Oxford, UK. <https://comprop.oii.ox.ac.uk/research/posts/the-global-disinformation-order-2019-global-inventory-of-organised-social-media-manipulation/#continue>
- Brooking, E. T., & Kianpour, S. (2020). *Iranian Digital Influence Efforts: Guerrilla Broadcasting For The Twenty-First Century*. Atlantic Council.
- Calhoun, C. (1992). Habermas and the public sphere. Cambridge, MA: MIT Press.
- Cosentino, G. (2020). Post-truth Politics in Syria: ‘Rumor Bombs’ on the White Helmets. In G. Cosentino (Ed.), *Social Media and the Post-Truth World Order: The Global Dynamics of Disinformation* (pp. 87–111). Springer International Publishing. https://doi.org/10.1007/978-3-030-43005-4_4
- Cull, N. J., Culbert, D. H., & Welch, D. (2003). *Propaganda and Mass Persuasion: A Historical Encyclopedia, 1500 to the Present*. Santa Barbara, California: ABC-CLIO.
- Dehghan, S. K. (2013). Iran creates fake blogs in smear campaign against journalists in exile. *The Guardian*. <https://www.theguardian.com/world/2013/jan/24/iran-fake-blog-smear-campaign-journalist-bbc>
- Elsawah, M., Howard, P., & Narayanan, V. (2019). *Iranian Digital Interference in the Arab World*. Computational Propaganda Project. <https://comprop.oii.ox.ac.uk/research/posts/iranian-digital-interference-in-the-arab-world/>
- Facebook News. (2018, October 26). *Taking Down Coordinated Inauthentic Behavior from Iran*. <https://newsroom.fb.com/news/2018/10/coordinated-inauthentic-behavior-takedown/>
- Facebook News. (2021). *About Facebook*. <https://about.fb.com/news>
- Fraser, N. (1990). Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy. *Social Text*, (25/26), 56–80. doi:10.2307/466240
- Friedman, B. (2012). BATTLE FOR BAHRAIN: What One Uprising Meant for the Gulf States and Iran. *World Affairs*, 174(6), 74–84. <http://www.jstor.org/stable/23210463>
- Gadde, V., & Roth, Y. (2018). *Enabling further research of information operations on Twitter*. https://blog.twitter.com/en_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html
- Gleicher, N. (2020). Removing Coordinated Inauthentic Behavior. *About Facebook*. <https://about.fb.com/news/2020/10/removing-coordinated-inauthentic-behavior-mexico-iran-myanmar/>
- Gwynn, J. (2020). Facebook information warfare: Inside Iran’s shadowy operations to target you on social media. *USA TODAY*. Retrieved January 31, 2021, from <https://www.usatoday.com/story/tech/2020/01/10/iran-influence-operations-target-americans-after-soleimani-killing/4422491002/>
- Habermas, J. (1989). *The structural transformation of the public sphere: an inquiry into a category of bourgeois society*. Cambridge, MA: MIT Press.
- Habermas, J., Lennox, S., & Lennox, F. (1974). The public sphere: An encyclopaedia article (1964). *New German Critique*, (3), 49. doi:10.2307/487737
- Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J., & François, C. (2018). *The IRA, Social Media and Political Polarization in the United States, 2012–2018*.
- Jones, M. O. (2019). Propaganda, Fake News, and Fake Trends: The Weaponization of Twitter Bots in the Gulf Crisis. *International Journal of Communication*, 13(0), 27.
- Kaiser, J. & Rauchfleisch, A. (2019) Integrating Concepts of Counterpublics into Generalised Public Sphere Frameworks: Contemporary Transformations in Radical Forms. *Javnost - The Public*. DOI: 10.1080/13183222.2018.1558676
- Lunt, P., & Livingstone, S. (2013). Media studies’ fascination with the concept of the public sphere: critical reflections and emerging debates. *Media, Culture & Society*, 35(1), 87–96. doi:10.1177/0163443712464562
- Lynch, M. (2012). Political Science and the New Arab Public Sphere. *Foreign Policy*. <https://foreignpolicy.com/2012/06/12/political-science-and-the-new-arab-public-sphere/>
- Maréchal, N. (2017). Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. *Media and Communication*, 5(1), 29–41. <https://doi.org/10.17645/mac.v5i1.808>
- Morozov, E. (2011). *The net delusion: The dark side of internet freedom* (1st ed.). NY, NY: Public Affairs.

- Narayanan, V., Howard, P. N., Kollanyi, B., & Elswah, M. (2017). *Russian Involvement and Junk News during Brexit* (Data Memo 2017.10.). The Computational Propaganda Project. Retrieved February 3, 2021, from <https://blogs.oii.ox.ac.uk/comprop/research/russia-and-brexit/>
- Pacheco, D., Flammini, A., & Menczer, F. (2020). Unveiling Coordinated Groups Behind White Helmets Disinformation. *Companion Proceedings of the Web Conference 2020*, 611–616. <https://doi.org/10.1145/3366424.3385775>
- Ramsay, G. (2019). How Fake Stories Fuel Propaganda. *British Journalism Review*, 30(2), 45–51. <https://doi.org/10.1177/0956474819855547>
- Ramsay, G., & Robertshaw, S. (2019). *Weaponising news: RT, Sputnik and targeted disinformation*. King's College London. <https://www.kcl.ac.uk/policy-institute/research-analysis/weaponising-news>
- Robinson, O., & Sardarizadeh, S. (2020, February 14). Facebook removes “foreign interference” operations from Iran and Russia. *BBC News*. <https://www.bbc.com/news/blogs-trending-51493172>
- Schiffrin, A. (2017). Disinformation and Democracy: The Internet Transformed Protest but Did not Improve Democracy. *Journal of International Affairs*, 71(1), 117–126.
- Timberg, C., & Romm, T. (2019, June 25). It's not just the Russians anymore as Iranians and others turn up disinformation efforts ahead of 2020 vote. *Washington Post*. <https://www.washingtonpost.com/technology/2019/07/25/its-not-just-russians-anymore-iranians-others-turn-up-disinformation-efforts-ahead-vote/>
- Twitter Election Integrity Hub. (2021). *Civic integrity positions and policies*. <https://about.twitter.com/en/our-priorities/civic-integrity>
- Statista (2020). *Twitter: Most users by country*. (2021). Retrieved February 1, 2021, from <https://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/>
- Starbird, K., Arif, A., & Wilson, T. (2019). Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 127:1-127:26. <https://doi.org/10.1145/3359229>
- Mejias, U. A., & Vokuev, N. E. (2017). Disinformation and the media: The case of Russia and Ukraine. *Media, Culture & Society*, 39(7), 1027–1042. <https://doi.org/10.1177/0163443716686672>
- Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking*. Council of Europe. <https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html>
- Warminsky, J. (2020, October 8). Takedown of 92 Iran-owned domains includes 4 used for disinformation in US, feds say. *CyberScoop*. <https://www.cyberscoop.com/iran-propaganda-domains-takedown/>