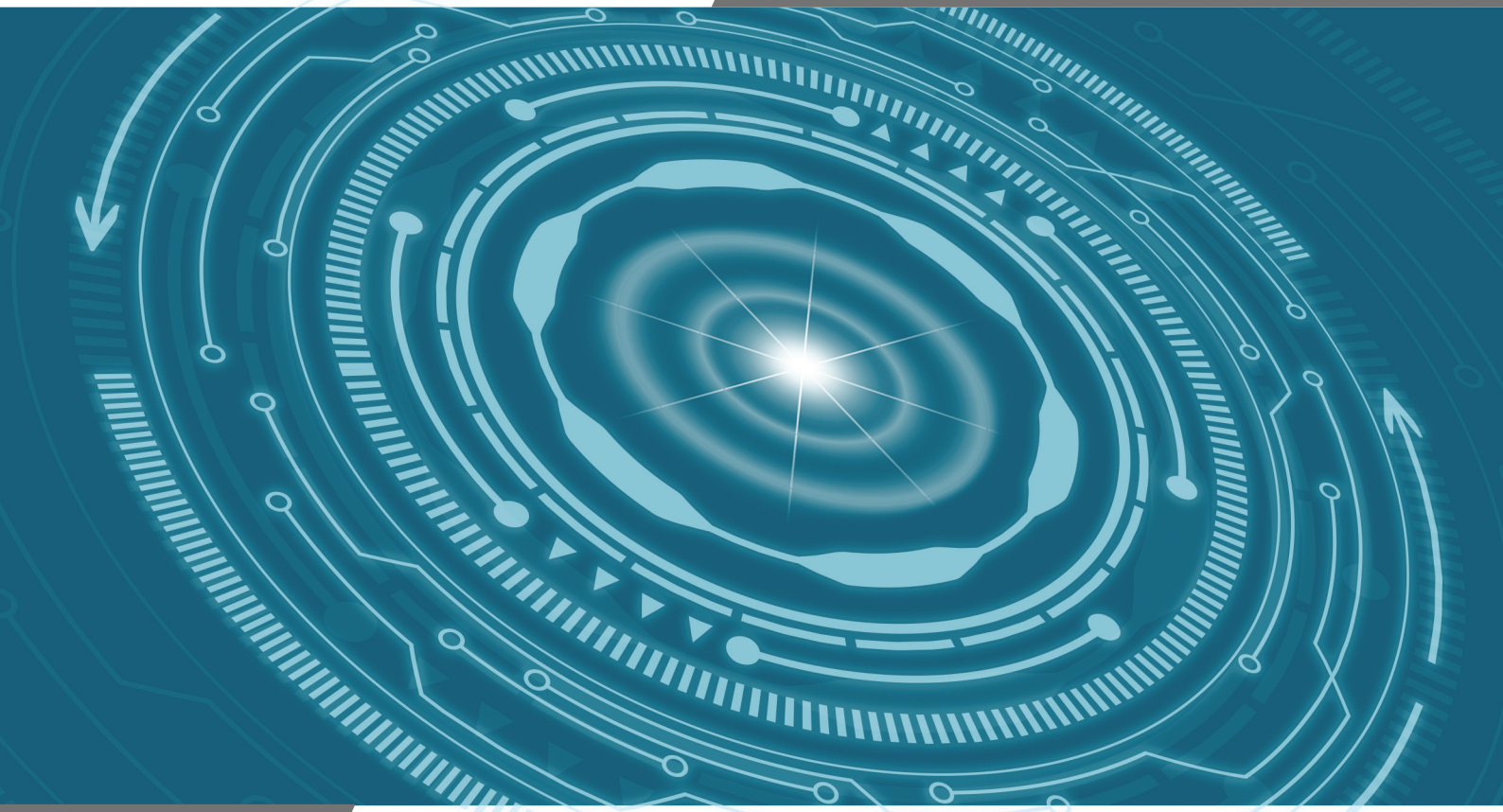
Centre for Economics and Foreign Policy Studies

edam

Cyber Governance and Digital Democracy 2019/1



March 2019

Russian Digital Media and Information Ecosystem in Turkey

H. Akın Ünver | EDAM, Oxford CTGA & Kadir Has University

Russian Digital Media and Information Ecosystem in Turkey

H. Akın Ünver | EDAM, Oxford CTGA & Kadir Has Üniversitesi

INTRODUCTION

In recent years, Russian digital information operations, including disinformation, fake news, and election meddling have assumed prominence in international news and scholarly research outlets. A simple Google Trends query shows us that 'fake news' as a term enters into global mainstream lexicon starting with October 2016, peaking in the immediate aftermath of the US Presidential Election in November. Since then, disinformation has been largely synonymous with Russian digital information operations in the West, and a number of empirical research projects have begun focusing on the impact of information warfare on elections and political behavior.

Russian media ecosystem in Western democracies, including information and dis-information dynamics, are quite well-documented[1]. This focus owes largely to increased awareness of election meddling, fake news and digital spoilers such as trolls and bots that often have real-life effects. In addition to other digital contestation types, including cyber warfare, Russian information operations are not confined to the country's official communication policy. These strategies are part of the Russian military doctrine, most relevant of which has been the 2010 Military Doctrine of the Russian Federation, which sought to "escalate to de-escalate"[2] tensions encompassing the country's western borders. To achieve this, the document advised 'hybrid war', which is an umbrella term to define untraceable and largely non-violent tools and methods that complement conventional military efforts. The 2010 doctrine was further bolstered by the 2013 Gerasimov Doctrine, which, among other things, diagnosed the "blurring the lines between the states of war and peace", adding that "wars are no longer declared and having begun, proceed according to an unfamiliar template"[3]. Hybrid war is not a Russian invention, nor is Russia the first state to use non-military measures to complement military efforts. Rather, the 2010 doctrine was an acknowledgment of the term 'hybrid war', officially coined first by the USCENTCOM in its analysis of the 2006 Israel-Hezbollah War[4]. The use of conventional and unconventional tactics, coupled with the new advances

CHREST FOUNDATION

This research has been made possible by funding obtained from the US-based Chrest Foundation for the project "Turkey and Russia: Context and Prospects".

1 Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," Working Paper (National Bureau of Economic Research, January 2017), https://doi.org/10.3386/w23089; Meital Balmas, "When Fake News Becomes Real: Combined Exposure to Multiple News Sources and Political Attitudes of Inefficacy, Alienation, and Cynicism," Communication Research 41, no. 3 (April 1, 2014): 430–54, https://doi.org/10.1177/0093650212453600; Michael C. Dorf and Sidney Tarrow, "Stings and Scams: 'Fake News,' the First Amendment, and the New Activist Journalism," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, January 26, 2017), https://papers.ssrn.com/abstract=2906444; David M. J. Lazer et al., "The Science of Fake News," Science 359, no. 6380 (March 9, 2018): 1094–96, https://doi.org/10.1126/science.aao2998.

2 "Text of Newly-Approved Russian Military Doctrine," Carnegie Endowment for International Peace, February 5, 2010, https://carnegieendowment.org/2010/02/05/text-of-newly-approved-russian-military-doctrine-pub-40266.

3 Henry Foy, "Valery Gerasimov, the General with a Doctrine for Russia," Financial Times, September 15, 2017, https://www.ft.com/content/7e14a438-989b-11e7-a652-cde3f882dd7b.

4 Matt M. Matthews, "We Were Caught Unprepared: The 2006 Hezbollah-Israeli War" (Fort Leavenworth, Kansas: US Army Combined Arms Center, 2007), https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/we-were-caught-unprepared.pdf.

in communication technology, widened the battlefield and forced the sides to fight along a broad spectrum of ideas, images and appearances, all floating in digital space. In the words of Timothy Thomas, Russian high command was deeply influenced by the 2006 USCENTCOM report and that analysis had led Moscow's transition into a new thinking in terms of how to merge new communication technologies with strategic thinking: "*a real cognitive war underway in the ether and media for the hearts and minds of its citizens at home and abroad*"[5].

In many ways, the Internet has become a force domain, just like land, sea and air. In January 2019, the world has attained 51% Internet penetration, meaning more than half of the world is now online and digitally interconnected[6]. Foreseeing an inevitable mass global interconnectivity, most major countries have already set up long-term strategies in place to situate themselves into a more favorable strategic position in the digital domain. For the rest of the state actors, there have been two real wake-up calls to adapt to the digital medium. The first was the Arab Spring movement that rocked the MENA capitals through 2010-12 and the second was the Occupy-inspired or related movements that did the same in the West[7]. Both movements demonstrated the disruptive capacity of social media platforms to circumvent and bypass state surveillance and repression. It is during this period that social media has begun to transform. Instagram was launched in October 2010, following Facebook's politically important geotag function via 'Places' app in August 2010. Facebook bought Instagram in April 2012 and WhatsApp in February 2014, turning itself into the biggest heavyweight in social media. In tandem, Twitter emerged as a more important political communication alternative to Facebook, as the Arab Spring and Occupy movements used primarily Twitter to organize and disseminate messages[8]. The publicly visible 140-character platform architecture of Twitter, combined with its fast media upload system, rendered it the primary venue for critical information flows during emergencies, protests and civil wars. The Syrian Civil War, conflict in Ukraine and war against ISIS have all substantially contributed to the rise of Twitter as the primary emergency-related social media platform[9].

Both the NATO Bi-Strategic Capstone Concept[10] and the 2010 Russian Military Doctrine[11] document have underlined the threat of an adversary "with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives". These means were fairly identical in both NATO and Russian military documents: nuclear proliferation, terrorism, cybercrime and cyberwar, organized crime and its role in drugs, arms and human trafficking, migration, ethnic and religious conflicts, population conflicts due to resource scarcity and globalization. Both documents also emphasized the digital medium as an emerging frontier of political contestation. NATO followed-up with a 2011 'Countering Hybrid Threats' experiment to develop a unified alliance strategy against disinformation and media manipulation efforts. This was ultimately abandoned due to uneven interest and commitment by the constituent countries[12]. Compared to NATO, however, Moscow was quicker to embrace the uncertainty of the new information revolution, the hybrid nature of social media and how its intricate twists and turns could be deployed to support what would later be defined as the 'sub-threshold warfare strategy'.

5 Timothy Thomas, "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations" (Riga: NATO STRATCOM, 2015), https://www.stratcomcoe.org/timothy-thomas-russias-21st-century-information-war-working-undermine-and-destabilize-populations.

6 Abdi Latif Dahir, "Half the World's Population Used the Internet in 2018 - ITU — Quartz Africa," Quartz, December 11, 2018, https://qz.com/africa/1490997/more-than-half-of-worlds-population-using-the-internet-in-2018/.

7 Philip N. Howard et al., "Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2011), https://papers.ssrn.com/abstract=2595096.

8 Alexandra Segerberg and W. Lance Bennett, "Social Media and the Organization of Collective Action: Using Twitter to Explore the Ecologies of Two Climate Change Protests," The Communication Review 14, no. 3 (July 1, 2011): 197–215, https://doi.org/10.1080/10714421.2011.597250; W. Lance Bennett and Alexandra Segerberg, "Digital Media and the Personalization of Collective Action," Information, Communication & Society 14, no. 6 (September 1, 2011): 770–99, https://doi.org/10.1080/1369118X.2011.579141.

9 Markus Rohde et al., "Out of Syria: Mobile Media in Use at the Time of Civil War," International Journal of Human–Computer Interaction 32, no. 7 (July 2, 2016): 515–31, https://doi.org/10.1080/10447318.2016.1177300.

10 For full text, see: http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

11 For full text English translation, see: https://carnegieendowment.org/files/2010russia_military_doctrine.pdf

12 Michael Aaronson et al., "NATO Countering the Hybrid Threat," PRISM 2, no. 4 (2011): 111–24.

Sub-threshold warfare strategy is a sub-strand within the wider umbrella term of 'hybrid warfare', which seeks to conduct confrontational and combative operations without triggering the NATO Article 5 obligations or a direct military retaliation by a NATO country[13]. This strategy builds upon the late-Soviet strategy of 'active measures', which deployed a combination of informatics and political framing mechanisms to divert, distract and mislead institutions and agencies in Western countries[14]. As outlined by former KGB Director of Foreign Counterespionage Oleg Kalugin, 'active measures' worked by creating several layers of separation between the perpetrating agency or figures, rendering the operation virtually untraceable back to Moscow[15]. Following decades of iterations, 'active measures strategy' has evolved into its modern form - sub-threshold warfare – which defines the sum of non-violent and obstructionist tactics of Russia's hybrid warfare operations within NATO countries.

Russia did not invent the sub-threshold warfare, however. It is the Russian response to the American 'offset strategy', which seeks to alter the balance of power in an unfavorable standoff through creating a new standoff in a more favorable contestation area[16]. The first American offset strategy was proclaimed during the early 1950s to deter the Soviet Union through nuclear means, without spending excessively on conventional forces. The second offset strategy was during the 1975-89 period when the United States attempted to pursue technological deterrence against the Warsaw Pact to mask NATO's comparative conventional disadvantage in Eastern Europe. Finally, the third US offset strategy, which Russia is currently challenging in direct terms, was announced in 2014 to bolster US capabilities against anti-access, area-denial (A2-AD) systems developed by Russia and China[17]. This implied bolstering US cyber surveillance, intelligence, digital media and stealth platforms to preserve its informatics upper hand in Eastern Europe, especially along the Russian border. From Russia's point of view, such US-origin measures targeted ethnic and religious fault lines in former Soviet countries, to uproot pro-Russian governments and leaders from power[18]. In the same vein, Russia's sub-threshold strategy is a mirror image of US offset strategies. By using digital media and informatics tools, Russia seeks to offset NATO's technological and military strength, driving wedges within and around NATO countries without triggering their conventional defense mechanisms[19].

13 Alexander Lanoszka, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe," International Affairs 92, no. 1 (January 1, 2016): 175–95, https://doi.org/10.1111/1468-2346.12509.

14 Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," Connections 15, no. 1 (2016): 5–31.

15 Evan Osnos, David Remnick, and Joshua Yaffa, "Trump, Putin, and the New Cold War," February 24, 2017, https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war.

16 Daniel Fiott, "Europe and the Pentagon's Third Offset Strategy," The RUSI Journal 161, no. 1 (January 2, 2016): 26–31, https://doi.org/10.1080/03071847.2016.1152118.

17 Luis Simón, "The 'Third' US Offset Strategy and Europe's 'Anti-Access' Challenge," Journal of Strategic Studies 39, no. 3 (April 15, 2016): 417–45, https://doi.org/10.1080/01402390.2016.1163260.

18 Daniel Fiott, "A Revolution Too Far? US Defence Innovation, Europe and NATO's Military-Technological Gap," Journal of Strategic Studies 40, no. 3 (April 16, 2017): 417–37, https://doi.org/10.1080/01402390.2016.1176565.

19 Bettina Renz, "Russia and 'hybrid Warfare,'" Contemporary Politics 22, no. 3 (July 2, 2016): 283–300, https://doi.org/10.1080/13569775.2016.1201316; Sascha Dov Bachmann and Hakan Gunneriusson, "Russia's Hybrid Warfare in the East: The Integral Nature of the Information Sphere," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, October 7, 2015), https://papers.ssrn.com/abstract=2670527.

Major Cases of Disinformation and Countermeasures in the West

The highest-profile accusations of Russian meddling in the West came after the 2016 US General Election. The US Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) have stated that Russian President Vladimir Putin had personally ordered a large-scale and high-level 'influence campaign' to increase the chances of Donald Trump's victory in the election[20]. This was done, according to US security agencies, through a Russian military intelligence (GRU) led effort in hacking the Democratic National Committee servers, as well as John Podesta's – the director of the Hillary Clinton campaign[21] - account. Later in January 2017, Director of the US National Intelligence James Clapper asserted in a testimony that Russia was also involved in a coordinated and state-led 'fake news campaign', disseminated across web-based news and social media platforms. All of this led to the well-known 'Mueller investigation', conducted by the US Department of Justice Special Counsel Robert Mueller since May 2017, exploring the extent to which Russia and pro-Russian networks have been involved in the 2016 election[22]. A major sub-thread of the investigation concerns the extent of Russian digital media operations in the United States that go beyond more direct attacks such as hacking.

In mid-December 2018, two major empirical studies were submitted to the US Senate Intelligence Committee that explored the measurable impact of Russian disinformation operations in the US elections[23]. One of these reports, conducted by the Oxford Internet Institute's (OII) Computational Propaganda Project, outlines the extent to which the Russian Internet Research Agency (IRA) has used targeted disinformation, bots and trolls to divide the US public opinion into politically polarized interest groups for targeted manipulation[24]. Specifically, the report outlines how Russian efforts pinpointed and exacerbated existing social, racial and religious tensions and fears among the American right-wing voters, and fed both inaccurate and fabricated content to channel those tensions and grievances into pro-Trump electoral behavior. According to the report, not only did this targeted disinformation effort contribute substantially to Donald Trump's victory, but also continued to bolster his digital popularity during contested decision phases of his Presidency.

What is interesting from the researcher's point of view, is that Russian disinformation ecosystem in the US is extremely easy to spot and map-out, as the OII report demonstrates how 99% of all engagement related to the pro-Russian and Russian content (likes, shares, retweets, comments) originated from only 20 accounts on Twitter and Facebook, all controlled by the IRA, containing account names such as "Being Patriotic," "Heart of Texas," "Blacktivist" and "Army of Jesus". An overwhelming majority of these accounts share links from explicitly Russian news websites such as Russia Today, Sputnik and RIA Novosti, making web domain tracking one of the most common analytical tools to identify a pro-Russian network in a large data cluster. In other words, Russia hasn't spent much effort in trying to conceal its digital influence operations in the United States, and most of these accounts still exist in the American information ecosystem with different names, continuing to shape opinion within the far-right information networks. In analytical terms, all of these factors render the US one of the easiest cases to study Russian disinformation, as influence networks and content are still very much 'out there' and can be extracted through a very small sample. Even more interesting from the researcher's point of view, Russian disinformation operations have become even more brazen, direct and identifiable after they were spotted by the Mueller investigation, rendering their identification and network far

20 Karen Yourish and Troy Griggs, "8 U.S. Intelligence Groups Blame Russia for Meddling, but Trump Keeps Clouding the Picture," The New York Times, July 16, 2018, sec. U.S., https://www.nytimes.com/interactive/2018/07/16/us/elections/russian-interference-statements-comments.html, https://www.nytimes.com/interactive/2018/07/16/us/elections/russian-interference-statements-comments.html.

21 David E. Sanger and Charlie Savage, "U.S. Says Russia Directed Hacks to Influence Elections," The New York Times, December 21, 2017, sec. U.S., https://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html.

22 Jason Breslow, "All The Criminal Charges To Emerge So Far From Robert Mueller's Investigation," NPR.org, December 9, 2018, https://www.npr.org/2018/12/09/643444815/all-the-criminal-charges-to-emerge-so-far-from-robert-muellers-investigation.

23 Scott Shane, "Five Takeaways From New Reports on Russia's Social Media Operations," The New York Times, December 18, 2018, sec. U.S., https://www.nytimes.com/2018/12/17/us/politics/takeaways-russia-social-media-operations.html.

24 Philip N. Howard et al., "The IRA and Political Polarization in the United States, 2012-2018," Computational Propaganda Research Project (Oxford, UK: Oxford Internet Institute, December 2018), https://comprop.oii.ox.ac.uk/research/ira-political-polarization/.

easier to map out[25]. As this research report will show, this is quite 180-degrees the opposite of what we observed in Turkey, where pro-Russian information network is elusive, withdrawn and largely dormant, leading to excruciating research difficulties in mapping out the true extent of similar information operations.

Given the influence and success of Russian information operations in the United States, most analysts have turned to other NATO countries to see whether Russian-affiliated individuals or networks are involved in elections or contested political episodes. Russian information footprint is more visible in some European countries than others and came in two major waves[26]. The first wave, 1991-2004, focused primarily on former Soviet states and Cold War frontier countries to promote pro-Moscow political candidates and shift the public debate into a form more palatable to Kremlin[27]. As demonstrated in Way (2015), where the anti-Russian candidate is a democrat, Russia promoted more autocratic messaging and information in digital media channels, whereas if the anti-Russian candidate was authoritarian, Russian messaging promoted pluralism, change, and democracy[28]. The first wave also had a generally low level of success. The second wave of Russian information operations began in 2014, right after the United States declared its Third Offset Strategy in November 2014, and continues until today. The second wave directly targeted core NATO countries with two priorities in mind; a) retaliate against NATO-led ethnic and religious division strategies in and around Russia, by dividing Western nations electorally and socially through information warfare, without triggering Article #5, and b) to ride the wave of rising far-right and left-wing populism to maximize the effect of polarization operations[29]. Compared to the first wave, the second wave has been far more successful in terms of its goal of incapacitating NATO countries' collective defense mechanisms and strategic coherence. Beginning with 2014, Russia has specifically targeted political parties and movements that contributed to the polarization in European countries and also those that posed a more existential criticism of the political system, rather than individual political parties[30].

In France, Kremlin has partnered with Front National and has verifiably conducted a range of digital warfare attempts, including the hacking and leakage of Emmanuel Macron's campaign team data[31]. In the UK, pro-Russian accounts were heavily involved in the Brexit referendum through cyber-attacks, digital disinformation campaigns and targeted political advertisements to steer the direction of the vote in favor of the 'Leave' campaign[32]. In Germany, Russia has been involved with phishing attacks against political parties and campaigns that are pro-EU, including a 2015 hacking of the German Bundestag, stealing 16 gigabytes of emails (although these emails weren't leaked)[33]. Similar digital disinformation, phishing and campaign hacking cases are

25 Jane Mayer, "How Russia Helped Swing the Election for Trump," The New Yorker, September 24, 2018, https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump.

26 Naja Bentzen, "Foreign Influence Operations in the EU - Think Tank" (Brussels: European Parliament, 2018), http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282018%29625123.

27 Charlotte Wagnsson and Maria Hellman, "Normative Power Europe Caving In? EU under Pressure of Russian Information Warfare," JCMS: Journal of Common Market Studies 56, no. 5 (2018): 1161–77, https://doi.org/10.1111/jcms.12726.

28 Lucan A. Way, "The Limits of Autocracy Promotion: The Case of Russia in the 'near Abroad,'" European Journal of Political Research 54, no. 4 (2015): 691–706, https://doi.org/10.1111/1475-6765.12092.

29 Peter Pomerantsev, "Authoritarianism Goes Global (II): The Kremlin's Information War," Journal of Democracy 26, no. 4 (October 19, 2015): 40–50, https://doi.org/10.1353/jod.2015.0074.

30 Alina Polyakova, "Strange Bedfellows: Putin and Europe's Far Right," World Affairs 177, no. 3 (2014): 36–40.

31 Alex Hern, "Macron Hackers Linked to Russian-Affiliated Group behind US Attack," The Guardian, May 8, 2017, sec. World news, https://www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack.

32 Patrick Wintour, "Russian Bid to Influence Brexit Vote Detailed in New US Senate Report," The Guardian, January 10, 2018, sec. World news, https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report.

33 Paul Carrel and Andrea Shalal, "Germany Says Its Government Computers Secure after 'Isolated' Hack," Reuters, February 28, 2018, https://www.reuters.com/article/us-germany-cyber-russia-idUSKCN1GC2HZ.

also documented in Italy[34], Netherlands[35] and Sweden[36]. By December 2018, the European Union has declared a belated 'War Against Disinformation' in preparation for renewed Russian meddling efforts in a series of upcoming elections across Europe in 2019 (including the European Parliament election)[37]. Some of the proposed Europe-wide efforts are the establishment of a rapid warning system to recognize, isolate and remove fake or manipulated digital content, establishment of a new 'digital contract' with the main social media platforms Twitter, Facebook, YouTube and Instagram to 'get serious' about tackling disinformation during key events and set up a European fact-checking network of local verifiers to spot disinformation attempts in real-time. At the national level, countries have begun formulating largely converging strategies to combat external information operations.

France mobilized its intelligence agencies in the run-up to its 2017 elections. The National Cybersecurity Agency of France (ANSSI) has produced a cybersecurity handbook, including a beginner's introduction to DDoS (Distributed Denial of Service) attacks, with follow-up briefings for all political parties[38]. According to Carnegie Endowment, Marine Le Pen's Front National was the only party to be absent from all of these briefings[39]. This strategy worked, because 2017 French elections became one of the best-documented cases of failed Russian election meddling. Expecting a hack, Emmanuel Macron's campaign team hired an IT team specializing in digital disinformation and generated a digital file storage system that is designed to feed Russia its own medicine: deliberately fabricated false campaign documents to mitigate the value of 'real' documents that Russia may have extracted through its hacks. Macron team also hired three IT lawyers, each tasked with handling different aspects of disinformation campaigns during the election. Le Monde has published a list of news websites before the election day, ranking them according to their reliability[40]. Also, 30 media outlets in France partnered with Google to build a networked fact-checking initiative called CrossCheck. All of this meant that Russian meddling in French efforts failed, because France launched a truly national, trans-partisan, inclusive and heavily institutionalized framework to minimize the damage caused by Russian digital information operations. It also used a hybrid strategy of both autonomous, citizen-led fact-checking efforts and strategically deployed deliberate disinformation against Russian hackers.

Because the United Kingdom had already suffered from Russian disinformation attempts during the Brexit Referendum, its current strategy is structured to learn from those mistakes retrospectively. Like France, Britain's National Cyber Security Center (NCSC) is bringing British political parties together to brief them about the potential vulnerabilities of digital information systems and how to secure their networks against phishing attacks[41]. NCSC also published technical primers for politicians on more advanced topics in cybersecurity, disinformation and digital leaks[42]. Because voting in Britain is complex due to the absence of electronic voting and the responsibility of organizing voting at the district level, Britain is relatively more immune to direct digital election meddling. Rather, Britain is more exposed to digital disinformation and opinion

34 Stephanie Kirchgaessner, "Russia Suspected over Hacking Attack on Italian Foreign Ministry," The Guardian, February 10, 2017, sec. World news, https://www.theguardian.com/world/2017/feb/10/russia-suspected-over-hacking-attack-on-italian-foreign-ministry.

35 Patrick Wintour and Andrew Roth, "Russia Summons Dutch Ambassador over Hacking Revelations," The Guardian, October 8, 2018, sec. World news, https://www.theguardian.com/world/2018/oct/08/russia-summons-dutch-ambassador-over-hacking-revelations.

36 Erik Brattberg and Tim Maurer, "How Sweden Is Preparing for Russia to Hack Its Election," May 31, 2018, sec. World, https://www.bbc.com/news/world-44070469.

37 Daniel Boffey, "EU Raises Funds to Fight 'Disinformation War' with Russia," The Guardian, December 5, 2018, sec. World news, https://www.theguardian.com/world/2018/dec/05/eu-disinformation-war-russia-fake-news.

38 Heather A. Conley and Jean-Baptiste Jeangène Wilmer, "Successfully Countering Russian Electoral Interference," CSIS Briefs (Washington DC: Center for Strategic and International Studies, June 21, 2018), https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.

39 Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks" (Washington DC: Carnegie Endowment for International Peace, May 23, 2018), https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

40 Laura Daniels, "How Russia Hacked the French Election," POLITICO, April 23, 2017, https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/.

41 Oscar Williams, "Russia Is Targeting UK Infrastructure through Supply Chains, NCSC Warns," New Statesman, April 6, 2018, https://tech.newstatesman.com/business/russia-uk-critical-infrastructure.

42 "UK Political Parties Warned of Russian Hacking Threat: Report," Reuters, March 12, 2017, https://www.reuters.com/article/us-britain-russia-cybercrime-idUSKBN16J0OE.

manipulation attempts, than a direct hack. Thomas Rid's US Senate hearing demonstrated that both hacking and disinformation operations from Russia and China during the Brexit vote favored no particular candidate, but rather sought to exacerbate existing divisions and polarization over the refugee problem, immigration and the political power balance between London and Brussels[43]. Like the US, Russian-origin disinformation in the UK has been easy to spot and map-out. University of Edinburgh researchers have discovered that 3000 types of unique content can be traced to the Russian Internet Research Agency, with around 150,000 unique accounts created by pro-Russian networks to post specifically on the Brexit referendum[44]. These accounts were generally involved in anti-NATO and anti-EU content dissemination and focused on the British far-right audience through nationalist and isolationist content.

Germany on the other hand, has been targeted from a multitude of vulnerabilities, including its Bundestag network, Ministry of Finance digital accounts, Ministry of Foreign Affairs records and the Christian Democratic Union (CDU) party infrastructure. Like France, Germany has been primarily targeted by the APT28 hacker team, a GRU cyber-extension, as well as carefully curated and targeted disinformation attempts[45]. A number of such disinformation attempts involving the immigrants and immigrant-related violence have become popular among German far-right digital circles, perhaps the best-known case being the 'Lisa' story[46]. Even after the exposure of the 'Lisa story' as a disinformation case, Russian-origin disinformation campaigns on immigration and integration still remain popular among the German far-right[47]. To defend against such attempts, political sides in Germany have entered into a trans-partisan agreement before the September 2017 election to refrain from exploiting each other's' leaked political data and significantly limit the use of Twitter bots to boost the spread and engagement of their online political messages[48]. Facebook contributed to the training of the political parties in securing digital infrastructure systems, as well as how to deal with digital disinformation as fast as possible, with the help of the voters and national fact-checking initiatives[49]. German domestic intelligence agency BfV and Federal Office for Information Security, BSI, both took an active part in training political parties against a number of vulnerabilities[50]. BSI even offered its cyber defense services to all parties[51]. Like France, Germany also set up a large network of citizen-led, autonomous fact-checking networks to widen its disinformation defense capabilities.

43 Thomas Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns," Pub. L. No. 33017, § Select Committee on Intelligence (2017).

44 Robert Booth et al., "Russia Used Hundreds of Fake Accounts to Tweet about Brexit, Data Shows," The Guardian, November 14, 2017, sec. World news, https://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets.

45 Carrel and Shalal, "Germany Says Its Government Computers Secure after 'Isolated' Hack."

46 "The 'Lisa Case': Germany as a Target of Russian Disinformation," NATO, 2016, http://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm.

47 Constanze Stelzenmüller, "The Impact of Russian Interference on Germany's 2017 Elections," Brookings (blog), June 28, 2017, https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

48 Michael Schwirtz, "German Election Mystery: Why No Russian Meddling?," The New York Times, January 20, 2018, sec. World, https://www.nytimes.com/2017/09/21/world/europe/german-election-russia.html.

49 Sara Germano, "Facebook, Germany to Collaborate Against Election Interference," Wall Street Journal, January 20, 2019, sec. Business, https://www.wsj.com/articles/facebook-germany-to-collaborate-against-election-interference-11548004995.

50 Sumi Somaskanda, "The Cyber Threat To Germany's Elections Is Very Real," The Atlantic, September 20, 2017, https://www.theatlantic.com/international/archive/2017/09/germany-merkel-putin-elections-cyber-hacking/540162/.

51 "German Cyber Defense Blends Military and Commerce," Deutsche Welle, 09 2018, https://www.dw.com/en/german-cyber-defense-blends-military-and-commerce/a-45636325.

Charting the Pro-Russian Information Ecosystem in Turkey

With such direct and easily identifiable Russian meddling in some of the most powerful nations of the West, researchers have recently begun exploring how Russia-origin disinformation efforts shape the political debate in the rest of the world. Turkey is a natural case study. After all, Turkey has been a Cold War buffer country, lies right at the intersection of Western and Eastern security ecosystems and is adjacent to three major civil wars – Iraq, Syria and Ukraine. It has long been a strategically important country and lies adjacent to some of the most problematic politically contested regions of the Balkans, Caucasus, Middle East and North Africa. According to International Telecommunication Union (ITU), around 70% of the population has access to the Internet[52] and according to the UK-based media analytics company WeAreSocial, Turkey is one of the top countries in terms of social media usage[53]. Despite restrictions, Turkey is still one of the most active countries in terms of discussion and dissemination of political information online[54], and ranks among the most active countries in terms of using social media for political communication purposes[55]. Yet, it is also one of the most vulnerable countries to disinformation, bot usage and cyber-attacks[56]. Therefore, if there is an ideal country to study the impact of disinformation on politics, Turkey comes very close to that definition.

Yet, Turkey is also a difficult country to study in terms of disinformation, because it is already plagued by high-levels of fake news contamination[57]. The overall poor state of the information environment in the country renders disinformation a norm, not an exception, which makes it harder to isolate the researched anomaly within a wider pool of other anomalies. There is also the critical question of causality. Following the popularized cases in the US, UK, France and Germany, more countries have begun reporting cases of disinformation, even when such cases have no measurable effect on any political outcome[58]. This availability bias is plaguing the field with an enormous volume of contextually irrelevant cases of fake news that don't spread beyond a very small network and/or have no political or social implication[59]. More importantly, an excessive focus on Russian disinformation generate myopia that overlooks the agency of domestic players in making their countries vulnerable to disinformation in general[60]. Today, it is possible to locate Russian disinformation in a large number of countries, although Russia is by no means the only player that weaponizes digital information or systematically hacks international political actors. This creates an availability bias in the field, which distorts the extent to which Russia matters in digital space and substantially downplays the agency of the pre-existing political and media actors and institutions, analytically reducing them into non-entities.

This is a problematic way to approach disinformation, because its conceptual root – propaganda – is certainly not new to political communication. States have been deploying propaganda for centuries through the most recent and widespread media outlets they could access in any given era. Digital media is simply another step in the long history of propaganda and political diversion, spread in the past

52 "Measuring the Information Society Report 2018," International Telecommunications Union, 2018, https://www.itu.int/en/ITU-D/Statistics/Pages/publications/misr2018.aspx.

53 "Digital in 2018: World's Internet Users Pass the 4 Billion Mark," We Are Social, January 30, 2018, https://wearesocial.com/blog/2018/01/global-digital-report-2018.

54 Erkan Saka, "Social Media in Turkey as a Space for Political Battles: AKTrolls and Other Politically Motivated Trolling," Middle East Critique 27, no. 2 (April 3, 2018): 161–77, https://doi.org/10.1080/19436149.2018.1439271.

55 "Reuters Institute Digital News Report" (Oxford, UK: Reuters Institute, Oxford University, 2018), http://www.digitalnewsreport.org/.

56 Barçın Yinanç, "Poor Media Literacy 'making Turks Vulnerable to Fake News' - Turkey News," Hürriyet Daily News, December 10, 2018, http://www.hurriyetdailynews.com/poor-media-literacy-making-turks-vulnerable-to-fake-news-139582.

57 Mark Lowen, "Hunting for Truth in a Land of Conspiracy," BBC News, November 15, 2018, sec. Europe, https://www.bbc.com/news/world-europe-46137139.

58 Herman Wasserman, "Fake News from Africa: Panics, Politics and Paradigms," Journalism, December 17, 2017, 1464884917746861, https://doi.org/10.1177/1464884917746861; Marco Visentin, Gabriele Pizzi, and Marco Pichierri, "Fake News, Real Problems for Brands: The Impact of Content Truthfulness and Source Credibility on Consumers' Behavioral Intentions toward the Advertised Brands," Journal of Interactive Marketing 45 (February 1, 2019): 99–112, https://doi.org/10.1016/j.intmar.2018.09.001; Edson C. Tandoc Jr, Zheng Wei Lim, and Richard Ling, "Defining 'Fake News,'" Digital Journalism 6, no. 2 (February 7, 2018): 137–53, https://doi.org/10.1080/21670811.2017.1360143.

59 Dominic Spohr, "Fake News and Ideological Polarization: Filter Bubbles and Selective Exposure on Social Media," Business Information Review 34, no. 3 (September 1, 2017): 150–60, https://doi.org/10.1177/0266382117722446; Tim Groeling, "Media Bias by the Numbers: Challenges and Opportunities in the Empirical Study of Partisan News," Annual Review of Political Science 16, no. 1 (2013): 129–51, https://doi.org/10.1146/annurev-polisci-040811-115123.

60 Samantha Bradshaw and Philip N. Howard, "The Global Organization of Social Media Disinformation Campaigns," Journal of International Affairs 71, no. 1.5 (2018): 23–32.

through word of mouth, sealed envelopes, telegram, radio, television and motion picture. Success of propaganda through all of these periods relied primarily on two factors: the perpetrator's understanding of the media system, and the perpetrator's successful diagnosis of the social divisions in a target country. Propaganda therefore, always depends on how well its wielder understands the social impact of the delivery mechanism, be it telegram, motion picture or Twitter, and how well it understands what makes its audience tick. From this perspective, a propagandist's success relies largely on the pre-existing information environment and the extent of grievances within the audience.

In light of the growing criticism in the disinformation literature against studies that merely state that 'disinformation exists' or focus solely on Russian disinformation diffusion without any political and media environment context, this report aims to go one step further. Rather than only looking at whether there is Russian disinformation in Turkey (there is), this study seeks to explore whether Russian information operations in Turkey matter, and have any influence on Turkey's wider information landscape. Do they influence any mainstream conversation and have a measurable effect such as polarization and/or shifting election results, or do they merely exist in isolation, without any substantial engagement and relevance?

To do that, this study dissects 3 of the most important events in recent Turkish-Russian bilateral relations (downing of the SU24 jet, assassination of the Russian ambassador and the S400 negotiations) and arguably 2 of the most important domestic events in recent Turkish politics (2016 coup attempt and 24 June 2018 general elections) and aims to measure the impact of Russian-origin information campaigns against the wider Turkish information network in these most critical episodes. This method yields a more accurate perspective to evaluate the severity of Russian information efforts in Turkey compared to isolating low-engagement or marginally relevant content types that have no measurable effect on the general information network.

Mainstream pro-Russian information ecosystem in Turkey is fairly straightforward. Russia's primary mainstream Turkish language media outlet is *Sputnik-Türkiye*, which was one of the first foreign language branches of the agency after it replaced all previous Russian foreign-language services in November 2014. Around the same time, *Rusya'nın Sesi* – the primary pro-Russian news radio in Turkey – was named *RSFM* and continued under the aegis of the Sputnik News Agency. Aydınlık is a well-known pro-Russian outlet, that regularly reports events directly related to Turkish-Russian relations with an emphasis on the Russian view. There is also a pro-Turkish-Russian relations website called TurkRus.com, run by journalist Suat Taşpınar, where news and opinion on Turkish-Russian relations are shared frequently. Outside Sputnik-Türkiye, RSFM and Aydınlık however, what constitutes a pro-Russian outlet in Turkey is a highly contested and often a context-specific designation. Being considered 'pro' any foreign country, be it Russia, United States or otherwise, is generally considered libelous in Turkey. To that end, being called pro-Russian, like being called pro-American, is usually an external allegation to defame an actor and is also usually denied by the target(s). This complicates an analyst's job, especially when the study is empirical, because the outlining the 'pro-Russian media environment' becomes a moving target. Regardless, and as demonstrated in this research report, all shades of the Turkish media spectrum have published news reports and analyses that could be considered as 'pro-Russian' or 'close to Putin's position', under different contexts and content. In other words, the mainstream media in Turkey measurably shifts into a pro-Russian narrative on issues directly related to Turkish-Russian relations.

Prominent studies[61] that explore Russian disinformation in the US or EU have so far identified 'pro-Russian' accounts in three ways: a) URL/domain root tracking to see if they lead to Sputnik, RT or other Russian-language media or website link, b) location information of the account(s) involved (most US and UK disinformation studies traced pro-Russian networks based on their stated physical location within Russian territory), and c) dominant language of the text shared by the account (whether it is mostly in Russian). A combination of these methods usually yield a fairly reliable network of Russian influence actors in an information ecosystem. The first method can be applied to the Turkish case, as pro-

61 Savvas Zannettou et al., "Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web," arXiv:1801.09288 [Cs], January 28, 2018, http://arxiv.org/abs/1801.09288; Michael Jensen, "Russian Trolls and Fake News: Information or Identity Logics?," Journal of International Affairs 71, no. 1.5 (2018): 115–24; Yevgeniy Golovchenko, Mareike Hartmann, and Rebecca Adler-Nissen, "State, Media and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation," International Affairs 94, no. 5 (September 1, 2018): 975–94, https://doi.org/10.1093/ia/iiy148; Denis Stukal et al., "Detecting Bots on Russian Political Twitter," Big Data 5, no. 4 (December 1, 2017): 310–24, https://doi.org/10.1089/big.2017.0038; Emilio Ferrara et al., "The Rise of Social Bots," Communications ACM 59, no. 7 (June 2016): 96–104, https://doi.org/10.1145/2818717.

Russian opinion actors in Turkey do share Sputnik or Russia Today news frequently. The other two however, are not very reliable in the Turkish context, because they can be easily faked. Like the well-known attribution problem in cyber-attacks (i.e. who really conducted the attack), location and language-based attribution of information operations can be masked, leading to false attribution. Furthermore, in our study, less than .0001% of the content (14 tweets only out of 183 million) was sent by accounts that contains location information in Russia, or had Russian-language text in their content data.

Further complications arise from separating a pro-Russian media outlet from an anti-Western media outlet. A range of Turkish outlets have been designated as 'pro-Russian' due to their anti-NATO and anti-EU reporting bias, although some of these outlets sometimes reject this designation, defining themselves as 'nationalist'. From an analyst's perspective it becomes further difficult to separate NATO, EU and Russia news reports of a nationalist or an Islamist outlet, given both forms of reporting are heavily against Western institutions and report Turkish-NATO and Turkish-EU cooperation in overwhelmingly critical terms. This doesn't necessarily make them pro-Russian, as most of those outlets are also often critical of Moscow. Even further complicating the picture, and as demonstrated empirically in this research report, in the last 3 years, most mainstream, high-circulation pro-government and opposition news outlets alike have begun, at different times, reporting content that is aligned with Russia's position. As the mainstream media environment shifts gradually into a more pro-Russian tone, identifying pro-Russian outlets and networks become even harder. The only exceptions, of course are Sputnik-Türkiye, RSFM, because they are explicitly Russian-owned and funded. The closest domestic political outlet that comes closest to being an indigenous pro-Russian player is Aydınlık, given its frequent explicit support for Russian policy. However, in light of the new data presented in this study, it is more accurate to track 'pro-Russian content', rather than an outright 'pro-Russian outlet', as the former can be traced across all shades of the Turkish media environment, whereas the latter becomes a subjective designation, open to debate.

From a methodological standpoint, all of this makes a truly objective computational, large-volume study on Russian information operations in Turkey tricky. Instead of following the best-known mainstream studies that focus on Russian disinformation in the West through focusing on follower networks and most commonly shared news domains, we had to go a step further. In this study, we use the follower network and web URL tracing approaches, while adding a third dimension: sentiment. We have trained our topic modelling algorithm in Turkish political text to identify positive and negative sentiment digital content related to events and topics on Russian-Turkish relations. This three-layered strategy was necessary, as Russian information domain is not nearly as explicit, straightforward and brazen as we observe in other Western cases.

Methodology

Data source. The data used in this study is generated via the Twitter streaming API. Our research group has built a crawler that live-scrapes all tweets and their metadata since 24 November 2015 (SU-24 downing incident) that contain the n-grams 'Rus_', 'Putin_' and 'Moskova_'. These n-grams are derived from the keyword analysis tool KWFinder and topic-wise allow us to extract 99.998% of all Twitter content related to Turkish-Russian relations in Turkish-language. We don't call our approach 'stemming', which is mostly understood as an acronym for n-grams. Stemming works better with inflecting languages like English, whereas has a low reliability in agglutinative languages like Turkish. In the latter, n-gram approach yielded a more reliable result compared to 'stemming'. We primarily use Twitter in this study, with periodic robustness checks on Facebook. In comparison to our scraping effort on public accounts on Facebook, which yielded a total of 1,163,856 words over 3 years, Twitter gave us 486,052,996 words in total through the same time period, rendering Twitter a far better venue for this type of research. In our study on Turkish elections, we have pre-designated 6 of the most-shared proven disinformation cases that emerged during the election period. To explore disinformation during the failed 2016 coup attempt, we similarly analyzed 5 of the most prominent cases of fake news. These disinformation types have been exposed by Teyit.Org, a major Turkish fact-checking initiative.

Case selection. Our cases are selected due to their significant digital popularity compared to other cases in Turkish-Russian relations, and their political impact on bilateral relations. 24 June elections were picked, as these were arguably the most important political election in

Turkey, with the higher stakes and acute rivalry compared to previous elections. Most importantly, 24 June elections inaugurated the new political system in Turkey, and has a regime-shift component. The importance of 24 June elections is evidenced by their popularity on social media.

Selected Cases	Percentage of Dirty Data	Clean Data
S400 negotiations (5 benchmarks – longitudinal)	3.937	44,394,129
2016 Coup attempt	21.593	27,459,214
Assassination of the Ambassador	11.353	18,667,492
SU24 downing incident	9.825	13,560,108
Discarded Cases	**Percentage of Dirty Data**	**Clean Data**
Russia's annexation of Crimea (Mar 2014)	15.024	1,901,403
TurkStream Negotiations + Signing (longitudinal)	2.079	871,031
White Helmets (longitudinal)	46.492	139,059
Akkuyu Nuclear Power Plant (longitudinal)	1.291	84,493
Selahattin Demirtaş visit to Moscow (Dec. 2015)	11.938	37,381

Table 1 - Selected and discarded cases based on the proportion of cleaned data and post-cleaning data size

Selected Robustness Check	Percentage of Dirty Data	Clean Data
24 June 2018 Elections (Presidential + General)	17.884	79,823,491
Discarded Robustness Check Alternatives	**Percentage of Dirty Data**	**Clean Data**
2017 referendum	21.091	24,043,032
1 November 2015 Elections (General)	14.726	18,129,491
June 2015 Elections (General)	11.958	14,939,251
2014 Presidential elections	8.083	7,249,219
2014 local elections	6.179	3,140,402

Table 2 - Selected robustness check case and discarded alternatives based on the proportion of cleaned data and post-cleaning data size

Data cleaning. In this study, we clear out a type of bot-driven content commonly observed in Turkey: gibberish, randomly-selected words that don't contain any meaning. This type of automated content is easy to automatically detect and remove because The First Letters Of All Words In Such Tweets Are Capitalized. Often, bots that have nothing to do with Turkish-Russian relations (such as sports-related or advertiser bots) are programmed to auto-select n-grams based on their popularity, with no relation to any political incident. This results in quite a large volume of meaningless data that skews the results of Turkey-based disinformation research, and thus, have to be cleaned. We don't clean out tweets that are bot-driven, but have a meaningful sentence structure. The total number of tweets we study in this report is 183,904,434 post-cleaning. Percentages of dropped tweets during the cleaning phase in each case are listed in Tables 1 and 2.

Bot designation. We use a bot-detection algorithm that auto-identifies suspected bot accounts by employing four of the most established methods in the methodological literature: a) friend-to-follower ratio (Wang et. al., 2010[62]), number of tweets (Howard and Kollanyi, 2016[63]), account creation date (Jones, 2017[64]) and text duplicates (Thieltges et. al. 2018[65]). Only if an account posts content that meets one of these criteria, we do a second robustness check through a) the use of URL shorteners (a main indicator of automation, because URL shorteners, like trib.al, bit.ly or tinyurl.com, track traffic to a link), b) its tweet history of using more than 3 languages (bot accounts post automated messages in an average of 5-6 different languages to push a particular narrative in multiple linguistic and time-zone domains), c) follower-to-like ratio (an account that contains too many posts with disproportionate likes and retweets compared to its follower count, there is a high likelihood that it is a bot).

Automated Content/Sentiment Analysis. For automated text analysis we use ReadMe: Software for Automated Content Analysis[66], CEM: Coarsened Exact Matching Software and WhatIF: Software for Evaluating Counterfactuals, all of which we trained with Turkish-language official document, media text and news website comments text specifically related to Turkish-Russian relations and Turkish foreign policy over the course of 6 months. Through random selection semi-supervision tests, this heavy focus on texts related specifically Turkish-Russian political relations has allowed us to reach 98% reliability in detecting Turkish-language sentiment (including sarcasm) correctly[67]. In addition to specialized learning through focused text, we believe that this high level of reliability also owes to the linguistic properties of Turkish as an agglutinative language as opposed to English as an inflecting language.

Latent Dirichlet Allocation: LDA is a topic model type, which is a statistical text-mining method that auto-discovers relevant topic clusters in a large body of text. Its relevance algorithm is driven by Dirichlet distributions that are built as 'topic-per-document' and 'words-per-topic' classification. Our pre-processing routine includes tokenization, removing words fewer than 3 words, removing stopwords, lemmatizing words and reducing n-grams to their root form. In this study, we use the LDA approach defined by McCallum (et. al. 2007[68]).

62 Alex Hai Wang, "Detecting Spam Bots in Online Social Networking Sites: A Machine Learning Approach," in Data and Applications Security and Privacy XXIV, ed. Sara Foresti and Sushil Jajodia, Lecture Notes in Computer Science (Springer Berlin Heidelberg, 2010), 335–42.

63 Philip N. Howard and Bence Kollanyi, "Bots, #Strongerin, and #Brexit: Computational Propaganda During the UK-EU Referendum," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, June 20, 2016), https://papers.ssrn.com/abstract=2798311.

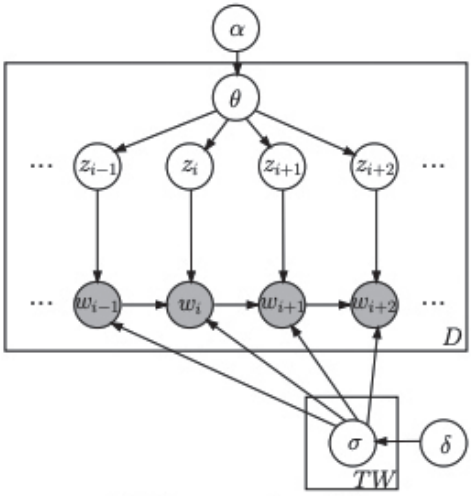
64 Marc Owen Jones, "Hacking, Bots and Information Wars in the Qatar Spat," Washington Post, June 7, 2017, https://www.washingtonpost.com/news/monkey-cage/wp/2017/06/07/hacking-bots-and-information-wars-in-the-qatar-spat/.

65 Andree Thieltges et al., "Effects of Social Bots in the Iran-Debate on Twitter," arXiv:1805.10105 [Cs], May 25, 2018, http://arxiv.org/abs/1805.10105.

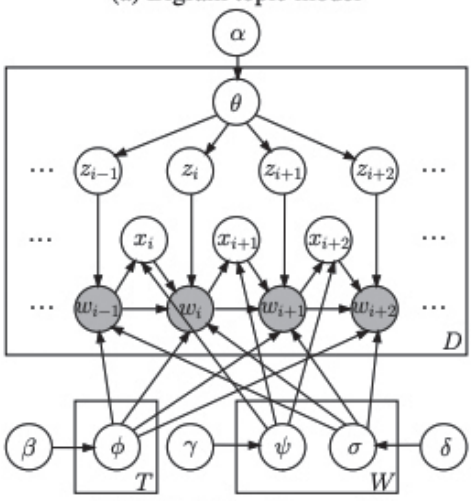
66 Daniel J. Hopkins and Gary King, "A Method of Automated Nonparametric Content Analysis for Social Science," American Journal of Political Science 54, no. 1 (2010): 229–47, https://doi.org/10.1111/j.1540-5907.2009.00428.x.

67 Peng Liu et al., "Sarcasm Detection in Social Media Based on Imbalanced Classification," in Web-Age Information Management, ed. Feifei Li et al., Lecture Notes in Computer Science (Springer International Publishing, 2014), 459–71.

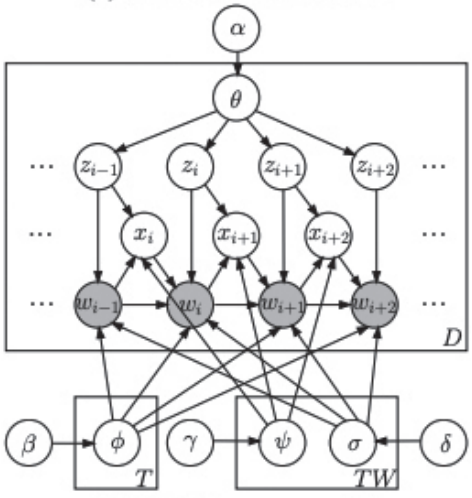
68 A. McCallum, X. Wei, and X. Wang, "Topical N-Grams: Phrase and Topic Discovery, with an Application to Information Retrieval," in Seventh IEEE International Conference on Data Mining (ICDM 2007)(ICDM), 2007, 697–702, https://doi.org/10.1109/ICDM.2007.86.



(a) Bigram topic model



(b) LDA-Collocation model



(c) Topical n-gram model

Figure 1 - N-gram text discovery and topic model approach used in this research report, as described in McCallum et. al. (2007): "The graphical model presentation of this model is shown in Figure 1(c). Its generative process can be described as follows: 1. draw Discrete distributions ϕ_z from a Dirichlet prior β for each topic z; 2. draw Bernoulli distributions ψ_{zw} from a Beta prior γ for each topic z and each word w; 3. draw Discrete distributions σ_{zw} from a Dirichlet prior δ for each topic z and each word w; for each document d, draw a Discrete distribution $\theta^{(d)}$ from a Dirichlet prior α; then for each word $w_i^{(d)}$ in document d: (a) draw $x_i^{(d)}$ from Bernoulli $\psi_{z\,(d)\,i-1 w\,(d)\,i-1}$; (b) draw $z_i^{(d)}$ from Discrete $\theta^{(d)}$; and (c) draw $w_i^{(d)}$ from Discrete $\sigma_{z\,(d)\,i\,w\,(d)\,i-1}$ if $x_i^{(d)} = 1$; else draw $w_i^{(d)}$ from Discrete $\phi_{zi}^{(d)}$."

Case-1: SU24 Downing Incident

The 24 November 2015 downing of the Russian SU-24 in Syria is a major flashpoint between Turkey and Russia and offers a good case study for longitudinal digital misinformation research. Predicting that the incident would change Turkish-Russian relations to a great extent, our research cluster has begun scraping social media data soon after the news broke out. Initially, we scraped Twitter, Facebook and web pages, but given the vast analytical size of the former, we decided to go with Twitter only. Ultimately, the decision to begin scraping relevant data that date became an auspicious one, as we are still continuing with the same corpus and keywords that have been building up since then.

The Russian Sukhoi-24 was shot down by a Turkish F-16 after the Russian aircraft violated the Turkish airspace by about 2.19 kilometers. Two Russian pilots had ejected, but the main pilot was shot down and killed by a band of Syrian rebels on the ground, while Russian troops ultimately rescued the second pilot. Russia contested Turkey's decision to shoot down the SU-24, asserting at the highest level that the craft remained within Syrian territory and never strayed into Turkish airspace. Turkey, on the other hand, released a number of audio recordings, including the radio communications between the Turkish air base and the F-16. In addition, Ankara argued that the Russian SU-24 was unidentified (meaning its electronic radar identification was marked as 'unknown' craft) and the airbase command thought the jets belonged to the Syrian government. The contested narratives between the two sides continued for months and could only be diffused following intense diplomatic cushioning. The event was also highly internationalized as all NATO countries, including the United States, entered the fray through diplomatic de-escalation moves.

Initial hours of the incident on social media are marked mostly by objective statements, with a substantial presence of retweets from main news outlets, rather than organic new content. The severity of the crisis was generating an unexpectedly cautious response from the digital audiences on both sides; rather than making assertive statements, content focused mainly on the technicalities: how far the SU24 penetrated Turkish air space, what were the engagement rules and the exact location of the shooting down. It is after Day-1 that the first cases of sentiment-relevant content start to emerge. Our group fed the collected tweets into both ReadME and SentiStrength – two popular text analysis tools. Ultimately, we decided to go ahead with semi-supervised ReadME as it provided greater reliability in Turkish-language political text. Eventually, our algorithm has discovered two main topic clusters, that correspond to two narrative ecosystems: one pro-Russian and one pro-Turkish:

Narrative-A: the topic cluster of tweets that blame Russia for violating Turkish airspace,
Narrative-B: the topic cluster of tweets that blame Turkey for shooting down the jet outside of Turkish airspace.

Narrative-A was disseminated quite centrally by pro-government news outlets, closely supported by government members' accounts, ultimately reaching hegemonic status within the Turkish Twitter ecosystem by the end of Day-1. This narrative orbited around legalistic arguments and emphasis on international law over airspace violations, and asserted that the decision was correct. Narrative-B on the other hand primarily relied on Sputnik Türkiye, Aydınlık, and RT-domain content, yet received less support in the Turkish Twitter ecosystem. Narrative-B followed Russian defense establishment view that the SU24 was shot down outside Turkish airspace, while it was still cruising within Syrian territory. Furthermore, Narrative-B contained early radar screen images disseminated by the Russian high command to support the claim that the jet was shot down within Syrian airspace. However, Narrative-A quickly monopolized the frame and the narrative in Turkish information ecosystem, and Narrative-B lingered on with diminishing popularity and eventually got marginalized in the ecosystem by Day-8.

Narrative-A Top Keywords	Occurrence	Narrative-B Top Keywords	Occurrence
Uça_	4,180,868	Uça_	1,628,426
Rus_	4,012,673	Rus_	1,574,634
Savaş	3,963,145	Suriye	1,506,418
Sınır_	3,461,369	SU24	1,469,765
İhlal	3,405,951	Dışı_	1,369,748
Havasaha_	3,208,413	Havasaha_	1,267,932
Türk_	2,794,486	Gir_	1,134,662
Suriye	2,408,018	Devriye	1,068,484
Taraf_	2,097,666	Sınırın_	1,097,255
Savunma	1,468,234	F-16	1,031,320
Düşür_	1,168,989	Savunma	947,824
Alçak_	896,725	Moskov_	864,768
Haber_	711,266	Düşür_	845,250
Sputnik_TR	702,431	Düştü	764,318
İçerisinde	626,482	RT	745,326
Güneyinde	554,936	Sputnik_TR	741,255
RIA	524,864	Dışarı_	645,262
F-16	464,629	Kuzey_	468,598

Table 3 - Most frequently occurring n-grams in LDA-designated Narrative-A and Narrative-B content and engagement clusters

Narrative-A Domain	Diffusion Share %	Narrative-B Domain	Diffusion Share %
Sabah.com.tr	17.593	tr.sputniknews.com	88.931
Yenisafak.com.tr	16.394	aydinlik.com.tr	6.394
Hurriyet.com.tr	16.014	Rt.com	4.675
HaberTurk.com.tr	13.931		
Milliyet.com.tr	11.293		
aa.com.tr	9.429		
Cnnturk.com.tr	6.291		
Ntv.com.tr	4.485		
Ahaber.com.tr	4.570		

Table 3 - Top domains included in tweets from LDA-designated Narrative-A and Narrative-B*

* Domain popularity indicates how much users prefer to share content that contains these URLs. It doesn't mean that these accounts publish more content. It is a sign of how frequently that domain is referred to, not how much that domain publishes on a given topic. This is an important disclaimer that is also relevant for other domain popularity tables in this report.

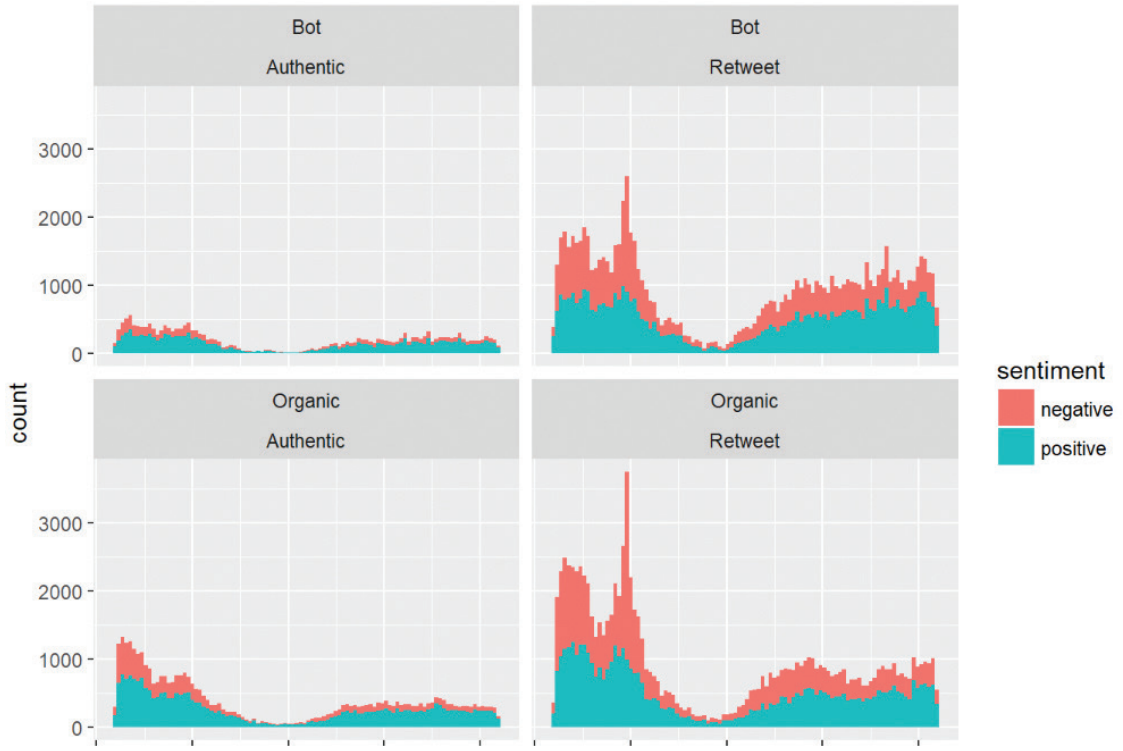


Figure 2 - 24-hour time-series analysis of LDA-designated Narrative-A and Narrative-B engagement metrics, sorted by organic/bot and authentic/retweet designation. Count value in 000s.

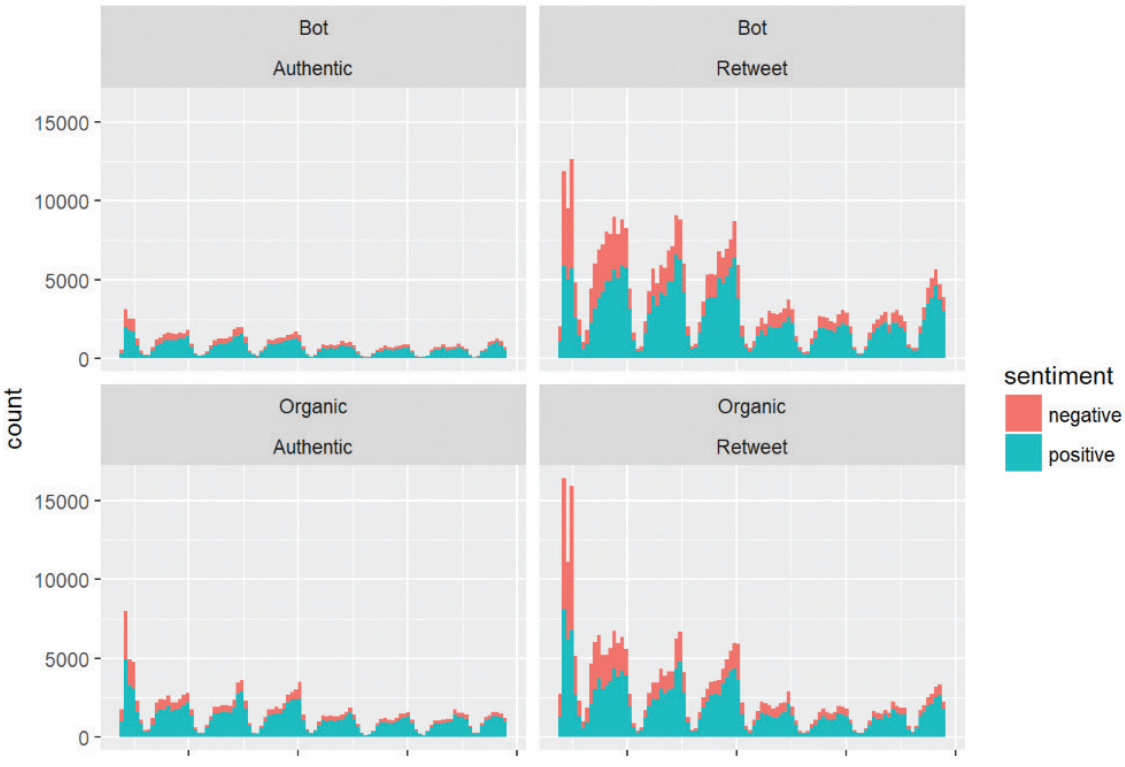


Figure 3 - 7-day time-series analysis of LDA-designated Narrative-A and Narrative-B engagement metrics, sorted by organic/bot and authentic/retweet designation. Count value in 000s.

After Day-8 (2 December 2015) however, a new pro-Russian line emerges. This line [Narrative-C] mounted a centralized challenge against the Turkish government for aiding and supporting the Islamic State (ISIS), specifically by purchasing crude oil from the areas controlled by the group via tankers[69]. This new line was also heavily disseminated through Sputnik-Türkiye and a number of Turkish-language anonymous accounts and became more successful in terms of its spread and staying power, compared to Russia's early narrative that the SU-24 was shot down outside Turkish airspace. In all of our cases, this is the most successful, high-impact and lasting Russian information operation, and arguably, Russia's success with this narrative has put Turkey on the defensive from a digital standpoint. This new pro-Russian criticism of Turkey suggests heavy centralized message control owing to the Russian Defense Ministry statement on 2 December 2015, that it had satellite images offering proof that Turkish tankers were involved in oil smuggling from ISIS-controlled territory[70]. Beginning with January 2016, this narrative substantially proliferated in the Turkish Twitter ecosystem, and becomes a more dominant line of argument, compared to Turkey's narrative-A (that Russian jet was shot down within Turkish airspace). Furthermore, the Russian line was frequently retweeted and shared by Western media outlets as well[71], perhaps as an expression of frustration towards Turkey in general, or its Syria policy in particular. Regardless, pro-Russian information operations on Turkey-ISIS link went beyond Turkish information ecosystem and became truly global, with substantial engagement in all NATO countries. In terms of diplomatic messaging and signaling, Russia has demonstrated to Ankara that it could easily draw a wedge between Turkey and its Western allies and create a very large rift within NATO if it tried. Arguably, the success of Narrative-C has been one of the digital drivers, along with more immediate physical drivers related to Syria, of Turkey's growing distancing from NATO and its slide into the Russian orbit. The main evidence on this can be found with the other cases studied in this report: after Narrative-B, Turkey never officially challenged a Russian digital narrative on social media in a significant way.

Narrative-C	Occurrence	Narrative-D	Occurrence
Türk_	6,216,826	FET_	4,136,193
IŞİD	5,120,631	Rus	3,849,679
Petrol	4,597,623	Cemaa_	3,426,716
Yasadışı	2,236,641	Uçağı_	3,201,329
Tanker	1,619,374	NATO	2,797,634
Suriye	1,396,417	Talimat_	2,643,418
Erdoğan	946,674	Tarafı_	2,325,824
Militan_	863,219	ABD	1,946,264
Ticareti_	634,546	Güle_	1,245,357
Görüntü_	422,279	Pilot_	904,526
Sınır_	316,748	Moskov_	843,145
Haftada	201,367	Gizli	751,422
Bakanl_	102,267	Emir	526,214

Table 5 - Most frequently occurring n-grams in Narrative-C and Narrative-D content and engagement cluster

69 "Russia Presents Proof of Turkey's Role in ISIS Oil Trade," RT International, December 2, 2015, https://www.rt.com/news/324263-russia-briefing-isis-funding/.

70 Ben Taub, "The ISIS Oil Trade, from the Ground Up," December 4, 2015, https://www.newyorker.com/news/news-desk/the-isis-oil-trade-from-the-ground-up.

71 Tom Brooks-Pollock, "Russia Releases 'Proof' Turkey Is Smuggling Isis Oil over Its Border," The Independent, December 2, 2015, http://www.independent.co.uk/news/world/europe/russia-releases-proof-turkey-is-smuggling-isis-oil-over-its-border-a6757651.html; Maria Tsvetkova and Lidia Kelly, "Russia Says It Has Proof Turkey Involved in Islamic State Oil Trade," Reuters, December 2, 2015, https://www.reuters.com/article/us-mideast-crisis-russia-turkey-idUSKBN0TL19S20151202; Greg Botelho, "Russia, Turkey Trade Charges: Who Bought Oil from ISIS?," CNN, December 2, 2015, https://edition.cnn.com/2015/12/02/europe/syria-turkey-russia-warplane-tensions/index.html.

Narrative-C Domain	Diffusion Share %	Narrative-D Domain	Diffusion Share %
tr.sputniknews.com	47.493	Sabah.com.tr	22.193
Cumhuriyet.com.tr	12.328	Yenisafak.com.tr	20.594
Odatv.com	11.387	Ahaber.com.tr	17.603
Aydinlik.com.tr	9.395	Sozcu.com.tr	13.491
Evrensel.net	7.203	Haberler.com	10.839
Diken.com.tr	6.382	Aksam.com.tr	9.394
Miscellaneous blogs/websites	5.812	Ahaber.com.tr	5.886

Table 6 - Top domains within Narrative-C and Narrative-D content and engagement clusters

The 'ISIS oil' information strategy has been demonstrably successful from the Russian perspective. Although the information ecosystem in Turkey still discussed and debated that Ankara was correct in deciding to shoot down the Russian jet, the pro-Russian ecosystem has managed to widen the information battlefront and distract substantially from Ankara's main argument. Through 2 December 2015 till 6 August 2016 meeting between Presidents Erdoğan and Putin (around 8 months), the oil smuggling narrative has dominated the online agenda on Turkey-Russia relations and reframed the whole episode into Turkey's 'oil trade with ISIS'. Nothing Ankara did, either diplomatically or public relations-wise was enough to counter Russian narrative. As mentioned earlier, Russia was able to hack into Turkey's relations with NATO through this narrative as NATO country media outlets became some of the most prominent central hubs in the dissemination of this narrative. Even today, 'ISIS oil' narrative is shared widely through US-based far-right conspiracy theory outlets like Breitbart[72] and InfoWars[73]. This narrative ended quite sharply, however, following the first-ever meeting between Presidents Recep Tayyip Erdoğan and Vladimir Putin in St. Petersburg on 9 August 2016. Even before that, the failed coup attempt of 15 July 2016 seems to have made a mark on reducing Russia's weight behind Narrative-C.

The Turkish side has responded to Russia's Narrative-C, by both retaining its insistence on Narrative-A, and diverting gradually into a new narrative. Narrative-D asserted that the jet shooting was ordered by a military chain of command loyal to the exiled cleric Fethullah Gülen[74]. It is difficult to assess why this shift happened by purely computational tools. However, it is likely that this shift was a product of Turkey's realization that it didn't have much leverage against Moscow in strategic terms and had to de-escalate the situation, even though Turkish version of events ultimately proved to be correct and the allegations of Turkey's 'oil purchases from ISIS' have been played down by the US State Department itself[75]. Regardless, Russia's 'ISIS oil' information campaign had become too hard to challenge for Turkey, given its domestic and international diffusion rate, necessitating a diversion, rather than a direct challenge. According to the new Narrative-D, the decision to shoot down the Russian jet did not follow the regular chain of command but was deliberately put into play by a clandestine pro-Gülen and/or NATO military network. This line of reasoning shifts into two different but not mutually exclusive sub-narratives: that a) the order was given by a pro-Gulen commander, b) the decision was made autonomously by a pro-Gulen pilot, and c) decision was made by a much higher ranking general

72 Edwin Mora, "Report: Turkey, Syria Helped Keep Islamic State Alive by Buying Their Oil," Breitbart, July 3, 2018, https://www.breitbart.com/national-security/2018/07/03/report-turkey-syria-helped-keep-islamic-state-alive-by-buying-their-oil/.

73 Michael Snyder, "Obama Knows That Turkey Is Buying Oil From ISIS And He Isn't Doing Anything To Stop It," InfoWars (blog), November 28, 2015, https://www.infowars.com/obama-knows-that-turkey-is-buying-oil-from-isis-and-he-isnt-doing-anything-to-stop-it/.

74 "Rus Savaş Uçağının Fetö Tarafıdan Düşürüldüğü İddiası," Milliyet, October 7, 2017, http://www.milliyet.com.tr/rus-savas-ucaginin-feto-tarafidan-dusuruldugu-sivas-yerelhaber-2323116/.

75 "Oil Smuggled into Turkey Not Enough to Be Profitable: U.S. Official," Reuters, December 4, 2015, https://www.reuters.com/article/us-syria-oil-usa-idUSKBN0TN2P920151204.

operating with a hidden, pro-NATO agenda[76]. According to line-C, the decision to shoot down the jet was a NATO clandestine instigation, set in motion to create significant escalation in Turkey-Russia relations as Russia had recently entered the Syrian war. This line of reasoning suggested that a major diplomatic incident with Turkey would be a deterrent for Russia and that's why clandestine pro-Gülen and/or rogue pro-NATO cohort within the Turkish command structure sought to create an artificial crisis to cause military escalation between Ankara and Moscow. All three lines were nearly evenly distributed across the pro-government accounts, without any particular narrative becoming more popular than others. All of these different sub-narratives were intended to divert further from Russia's Narrative-C (ISIS oil) and tried to seek a digital narrative consensus that both sides could agree on; at least on paper. After the failed coup attempt in July 2016, Narrative-D became the mainstream narrative in Turkish-language Twitter.

Although Turkey prevailed over Russia in the first round (Days 1-8) over the framing of the jet downing incident, Russia's distraction strategy of widening the information battlefield in round-2 (2 December 2015 - 6 August 2016) has been more successful. This is a perfect example of how Russia adapted to and surpassed the inherent logic of the US 'offset strategy'. The extent of this success is evidenced both by the engagement and spread statistics in Figure-4, but also by the fact that although Turkey resumed its narrative-A, it has also shifted to an alternative narrative that the decision to shoot down was made outside regular decision-making channels. This may have had several goals in mind, from exporting the blame away from recently altered engagement rules against Syria, or giving Russia a backdoor reconciliation option, or a signal of de-escalation, or all of them. This shift of narratives has contributed to the de-escalation of the crisis, as Sputnik-Türkiye, Aydınlık, and OdaTV, along with regular pro-government newspapers like Yeni Safak, Sabah and Takvim too, have both gradually begun reporting on a possible 'Gülenist meddling'. By the end of August 2016, Russia had abandoned its line furthering 'Turkey-ISIS oil' narrative, and Turkish line had shifted from 'we were right', into 'the decision was made by conspirators'.

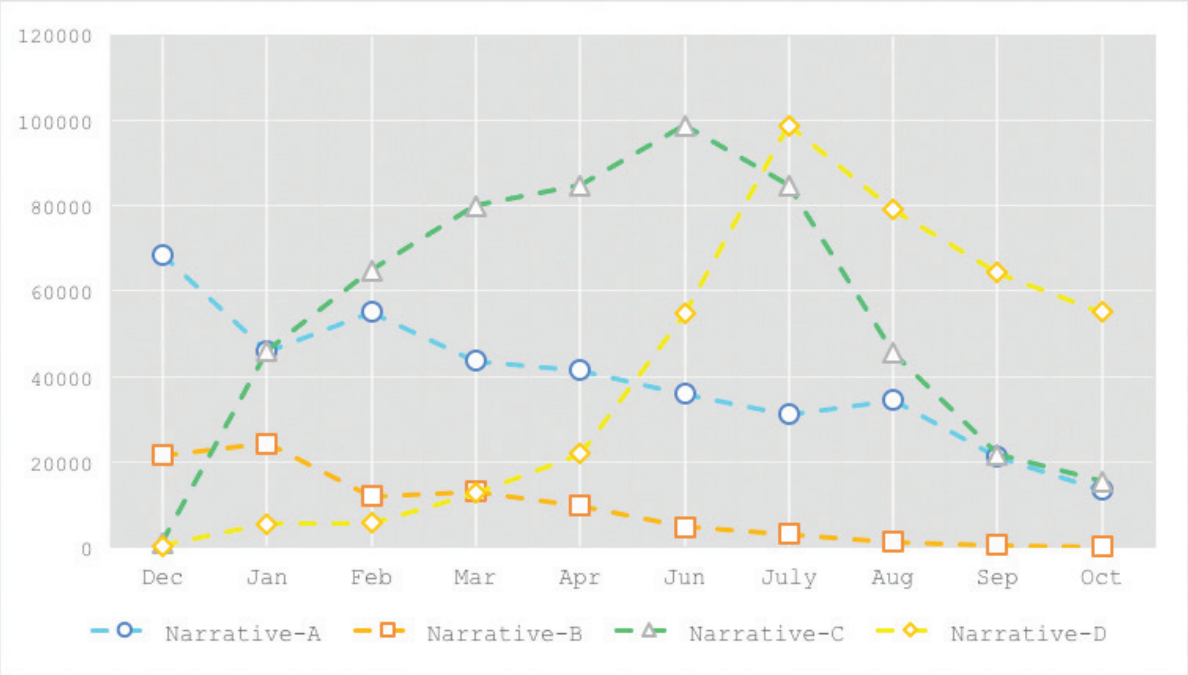


Figure 4 - Time-series engagement metrics of four main LDA-designated narrative clusters (December 2015 – October 2016)

[76] Fuad Safarov, "Rus uzman, Rus uçağını düşürme emrini kimin verdiğini açıkladı," Sputnik Türkiye, 12 2016, https://tr.sputniknews.com/rusya/201612041026128807-rus-uzman-gulen-ucak/; Elvan Alkaya, "Elvan Alkaya: FETÖ bağlantılı cinayetler ve şaibeli davalar (2)," Yeni Şafak, July 26, 2016, https://www.yenisafak.com/yazarlar/elvanalkaya/feto-baglantili-cinayetler-ve-aibeli-davalar-2-2030700; Mehmet Y. Yılmaz, "Davutoğlu bıçağın sırtında," Hürriyet, July 19, 2016, http://www.hurriyet.com.tr/yazarlar/mehmet-y-yilmaz/davutoglu-bicagin-sirtinda-40154956.

The jet downing incident has been the first and the last time that Moscow flexed its digital hybrid war muscles in dealing with Ankara. Most certainly with the addition of more immediate and 'real' factors related to Syria, growing Russian military capabilities in the Black Sea and widening rift between Turkey and NATO, Moscow's information demonstration has made a lasting mark on the Turkish information ecosystem. This was also the first, and the last time we have observed a direct digital information confrontation between Russia and Turkey and also the only time that we can conclusively assert from data that Russian information operations had a significant influence on Turkey's information ecosystem in a way that had a measurable effect on policy.

Case-2: July 2016 Coup Attempt

Disinformation during the coup attempt and in following days was rife. The uncertainty of the first few hours of the coup attempt produced a number of contextually important and potentially dangerous cases of disinformation that served to distract, confuse and mobilize people. In the days following the night of 15-16 July, the type of disinformation attempts changed, replacing mobilization-oriented content with cases of political disinformation that is harder to fact-check and verify.

1. ResulK vs. F-16 - By far, most widespread of these factually untrue types of popular content has been the man who allegedly tried to jump on a rogue F-16 as it was diving down into the Kızılay square in Ankara[77]. As unbelievable as it sounds in hindsight, the story of Resul K., the man who 'tried to jump on an F-16 and wanted to smash its windows with a crowbar', became the widest-spread false information on social media (Facebook, Twitter and Instagram combined). This disinformation type, featuring a photoshopped image of the Kızılay square, emerged within a cluster not affiliated either with the government, or the opposition, but based on our study, was generated and spread through the 'wisdom of the crowds', with no observable central node controlling the spread. However, after a day after the introduction of this particular disinformation case on social media, mainstream pro-government and nationalist outlets have picked up on this disinformation and began to share it on social media. Days later however, the Milliyet[78] newspaper reported that Resul Kaptancı was indeed killed during his attempt to attack the rogue troops taking over the General Staff headquarters in Ankara, but the F-16 story was wrong. Yet, digital content related to Resul Kaptancı was overwhelmingly shared as part of the disinformation related to the attempt to jump on an F-16 and remained that way. This disinformation content is still popular on Youtube and popular culture websites in Turkey.

77 "Şeytan taşladı," Takvim, 08 2016, https://www.takvim.com.tr/guncel/2016/08/16/seytan-tasladi.

78 "15 Temmuz Şehidi Resul Kaptancı'nın Ailesi İdam İstiyor," Milliyet, March 5, 2017, http://www.milliyet.com.tr/15-temmuz-sehidi-resul-kaptanci-nin-ankara-yerelhaber-1884645/.

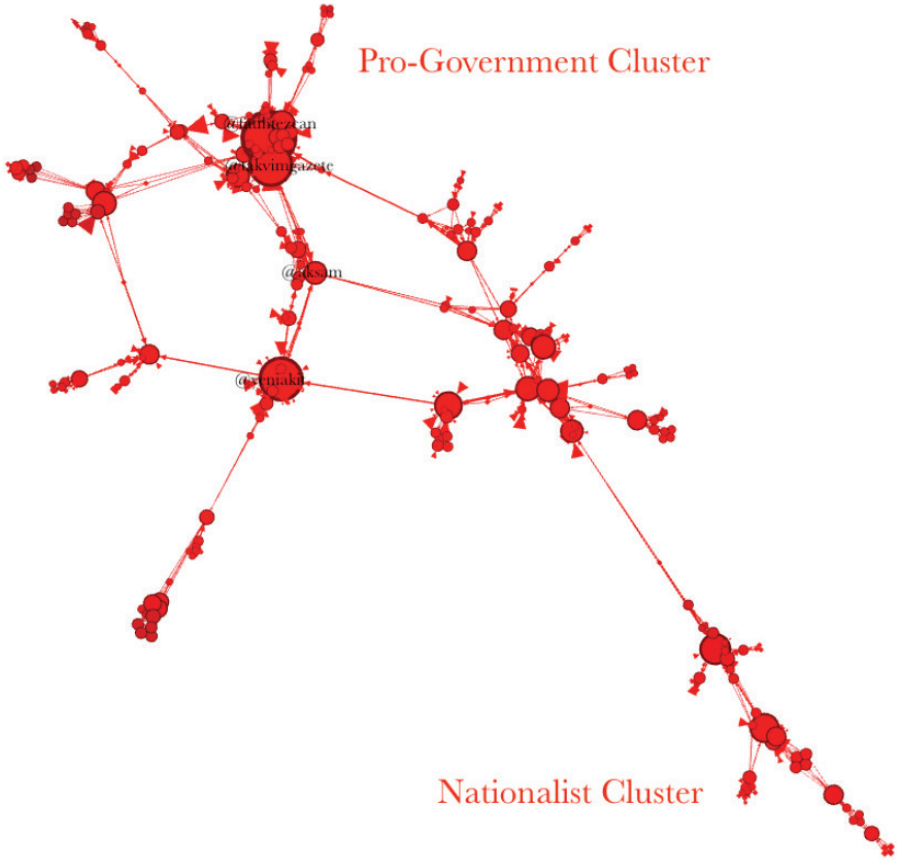


Figure 5 - Sample content and first-hour diffusion network of the ResulK vs. F-16 disinformation

2. Responsibility Waiver – The second most popular type of disinformation was in fact, a meta-disinformation. It sought to protect people against disinformation, but it was itself disinformation. It featured a fabricated message allegedly sent by, or on behalf of the Gendarmerie Headquarters calling on everyone on social media to post a legal waiver on their account pages, waiving their legal responsibility 'in case other malicious actors hacked into their accounts and posted disinformation or anti-government messages without their knowledge'. In the immediate post-coup environment, where disinformation and confusion were rife, this case of disinformation added fuel to the fire and led hundreds of thousands of Turks to post this disclaimer on their accounts. Another version of this disinformation type cited the Prime Ministry as the source. Regardless, neither the Turkish Penal Code nor the country's IT law contain any clause or requisite related to such waivers and the text message was fact-checked as essentially meaningless. This particular disinformation type is traceable back to the opposition news network and popular public figures, but later took on a non-political tint, shared by a large portion of the Turkish social media users. As demonstrated in Figure-6, this disinformation type was fact-checked within the first hour of its emergence, but still lingered on as one of the widest-shared disinformation types in the aftermath of the coup attempt.

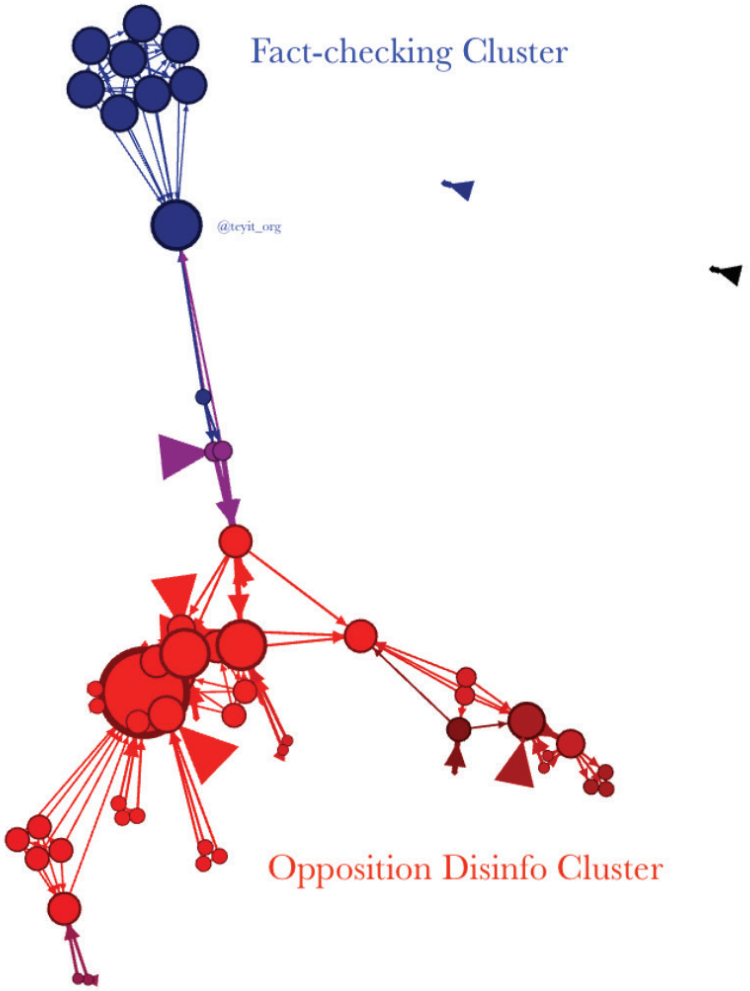


Figure 6 - Sample content and first-hour diffusion network of the 'Responsibility Waiver' disinformation

3. Fake Azerbaijan Incursion – The third most widespread disinformation type after the coup attempt was an alleged statement attributed to the President of Azerbaijan, Ilham Aliyev. According to the attributed quote, President Aliyev had declared his support for the Turkish people's resistance against the coup attempt and added that had the people's resistance failed, the Army of Azerbaijan would move into Turkey to help people quash the coup attempt. When traced back to its original quote, President Aliyev did declare his support for the resistance against the coup, but made no statement that would even remotely resemble ordering his army moving into Turkey[79]. Regardless, this disinformation originally emerges within the ultranationalist social media groups that have too few followers to make an impact. It became viral, when the JPEG image of this disinformation was shared on a popular Twitter account called @TuhafAmaGercek (2.25 million followers as of writing this report). This could have been a good candidate for pro-Russian information operation, given Russia's role in Turkish-Azerbaijani relations, but the account @TuhafAmaGercek has no connection to either Russia or the pro-Russian information ecosystem in Turkey and is a widely followed popular culture trivia account.

[79] "İlham Aliyev'den FETÖ Darbe Girişimine Kınama," TRT Haber, 07 2016, https://www.trthaber.com/haber/dunya/ilham-aliyevden-feto-darbe-girisimine-kinama-261298.html.

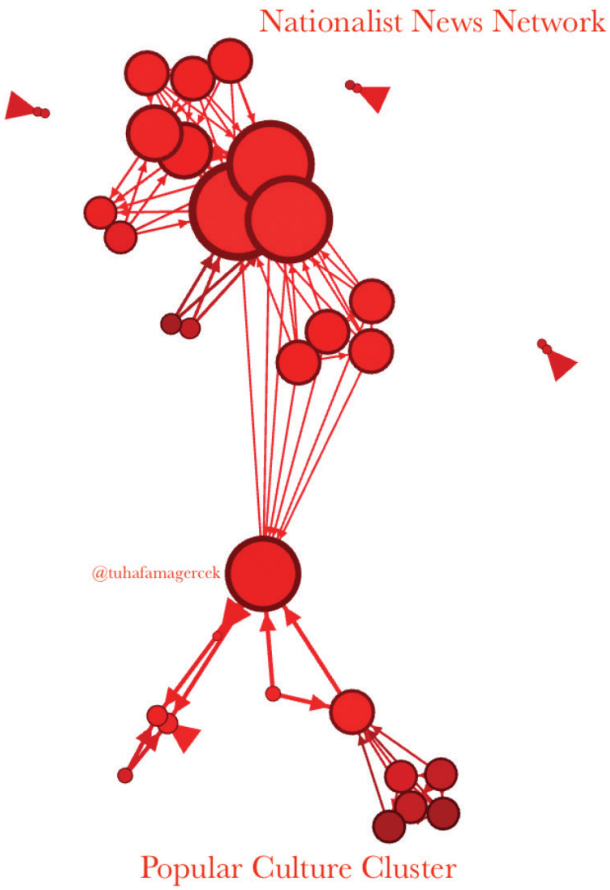


Figure 7 - Sample content and first-hour diffusion network of the 'Fake Azerbaijan incursion' disinformation

4. Rogue Soldiers – The fourth largest spread disinformation is a combination of distorted versions of a factually correct news about the violence against rogue troops following the failure of the coup attempt. The best-known and documented case was the surrender of the rogue troops on Istanbul's second bridge, during which six soldiers were lynched[80]. As one of the tensest flashpoints of the coup attempt, the 2nd Istanbul Bridge had witnessed rogue troops firing on the crowd killing several civilians. In return, and although loyalist troops and police were there to oversee the surrender, several rogue troops faced lynching, and one of those had died on the scene. This tense episode was portrayed on social media through a flurry of fake images and disinformation, and can be traced back to OdaTV and Haber.Sol.Org.Tr[81]. One of the most prominent cases was the spread of an image that belongs to an ISIS beheading in Syria, as if it was the image of the lynching in Istanbul. In addition, the images of several alive soldiers were disseminated on social media as the identity of the deceased soldier, adding further

confusion and anger to an already loaded situation. This type of disinformation had spread through both pro-government and opposition social networks and the involvement of accounts that can be traced to Russia is non-existent. This is one of the most contested disinformation types related to the coup attempt and the fake versions of the actual incident still circulate widely on Turkish-language social media platforms.

80 "6 askere linç," Hürriyet, 07 2016, http://www.hurriyet.com.tr/gundem/6-askere-linc-40150768.

81 "'Başı kesilen asker' haberine gelen yalanlama ve o haberin hikayesi," Sözcü, 07 2016, https://www.sozcu.com.tr/2016/gundem/basi-kesilen-asker-haberine-yalanlama-ve-o-haberin-hikayesi-1319809/.

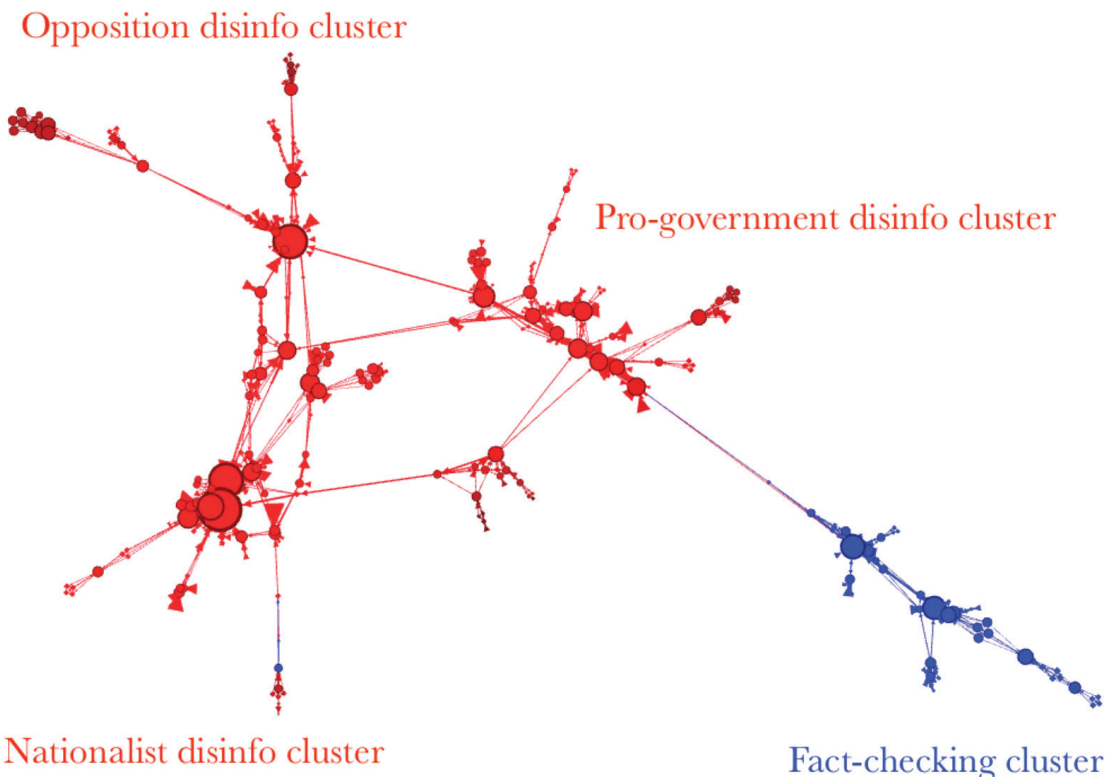


Figure 8 - Sample content and first-hour diffusion network of the 'Rogue Soldiers' disinformation

5. Police HQ Bombing – Another highly potent case of disinformation has been the video that some of the prominent media outlets shared as the 'bombing of the Ankara police headquarters'[82]. The headquarters building was indeed attacked during the coup night, but a doctored video belonging to 2014 Israeli airstrikes in Gaza became more widespread compared to the actual event footage. The fact that such an easily verifiable video (Google reverse video search function easily brings the original Youtube version[83]) was shared across prominent media outlets gives a good idea on how crisis episodes render even trained journalists into sharing unverified false information. This has been by far the most problematic type of fake news to verify. The video is a doctored version of Russia Today's live coverage of the 2014 Israeli bombardment and thus, most links shared on social media contain the 'rt.com' domain extension. However, it is impossible to verify who really doctored the video and the central nodes in the dissemination of this video in its very early hours are all Turkish accounts.

82 A recording of the video on CNN-Turk can be accessed here: https://twitter.com/t24comtr/status/754384016657289217

83 For the video link, please visit: https://www.youtube.com/watch?v=8pffdijUI1U

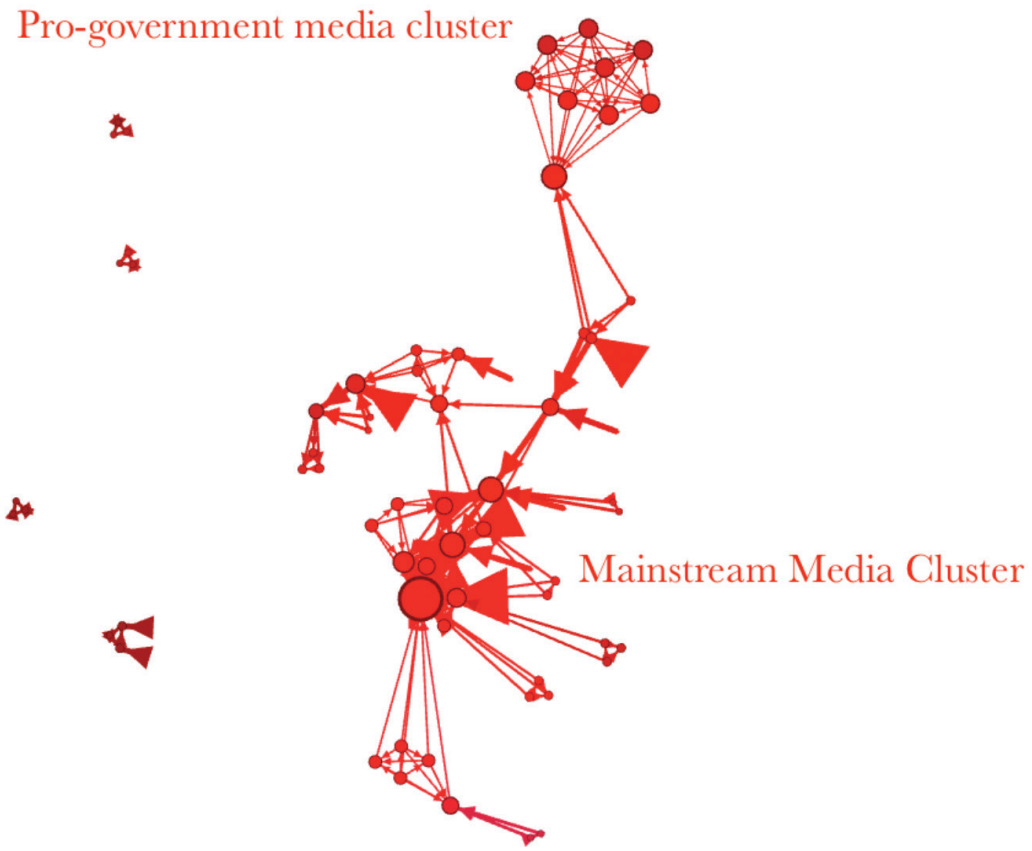


Figure 9 - The original RT video, which was doctored and used as a disinformation footage and the first-hour diffusion network of the 'Ankara bombing' disinformation

A final word about the Russian role in disseminating news on NATO and/or US involvement or negligence/apathy during the coup attempt. Sputnik-Türkiye and a number of other pro-Russian accounts in Turkey did push this line during and after the coup attempt. However, this line was already a mainstream view in the Turkish information ecosystem in the immediate aftermath of the coup attempt and dominantly disseminated by the pro-government news networks. Our survey found 5 such content types by Sputnik-Türkiye, but discovered that their reach was below 800 aggregate engagements. In contrast, however, digital content originating from mainstream Turkish accounts blaming the US or NATO had already reached around 100,000 aggregate engagements by the end of 17 July 2016.

Case-3: Assassination of the Russian Ambassador in Ankara

The second major crisis after the SU24 incident and months of diplomatic rebalancing was the assassination of the Russian Ambassador to Ankara, Andrey Karlov. Already tense and mutually distrustful from the damage caused by the SU-24 incident, the assassination of Ambassador Karlov on 19 December 2016 in Ankara, during a public event, threatened to hamper reconciliation efforts. The assassination followed a cautious improvement in Turkish-Russian relations ongoing since the Erdogan-Putin meeting in August. The assassination had profound implications, given the assassin was an off-duty police officer, who sneaked into Ambassador Karlov's security detail using his police ID[84]. The weeks that ensued were marked by significant noise in digital information flows, mostly regarding the allegiances of the attacker, as well as the motivations that led to the assassination. Turkey's official line has been that the attacker was a member of the Fethullah Gülen network; a point that was personally made by President Recep Tayyip Erdoğan[85]. Other alleged allegiances of the attacker were to ISIS, and Jabhat Fatah al-Sham[86] - a jihadi group active in north-western Syria. Recently in late-2018, a new theory emerged that the attacker belonged to another Islamic congregation – an allegation made none other than by Sputnik-Türkiye itself[87].

The sentiment scores of the aggregate data in the first 3 hours of the assassination are mixed (positive and negative) and display significant confusion. Hostile-designated content are those that either a) question whether the assassination really happened or whether it was 'staged', and b) expressed opinion that the assassination was a Russian 'inside job' that attempted to further embarrass Turkey by exposing its internal security deficit, or that c) it was a 'Western instigation' aimed to disrupt ongoing Turkish-Russian rapprochement. This confusion owes largely to the fact that there has been no centrally-coordinated messaging in Turkish information ecosystem within the first hour, and all major information brokers tried to weave a narrative on their own. It is with the 2-hour mark that the Presidency and government accounts begin to assert a positive narrative to end the confusion in the digital domain. With the identification of the attacker as a police officer another wave of confusion ensues, trying to contextualize this security deficit. But this flurry of negative-sentiment content also dies down by the 9-hour mark as the official narrative settles in and defines the act officially as a terrorist attack and declares solidarity with Moscow. Indeed, by the 12-hour, both organic and bot-driven engagement begins to revolve around keywords related to terror/terrorism, and also condolences and sympathies towards Russia and the Ambassador's family, revealing that the Turkish-speaking Twitter ecosystem largely accepted the government narrative. By the end of Day-1, two additional negative-sentiment peaks emerge, following the official denouncement of the attack by President Erdoğan and Prime Minister Binali Yıldırım. By Day-2, a new influx of negative-sentiment content is observable, both at the organic and bot-driven-level, blaming the Gülen network for its involvement in the assassination. This line of narrative is similar to the one in the jet downing incident, as three distinct plot lines emerge: a) the assassin was directed by a rogue police chief, b) the assassin himself was a rogue operator, and c) decision was made by a clandestine network operating with a hidden, pro-NATO agenda.

84 "Karlov suikastı iddianamesi mahkemede," NTV, November 23, 2018, https://www.ntv.com.tr/turkiye/karlov-suikasti-iddianamesi-mahkemede,pG6plihRcUaQQcbvWqgpEg.

85 "Erdoğan: Suikastçı FETÖ'ye Mensup," December 21, 2016, sec. Türkiye, https://www.bbc.com/turkce/haberler-turkiye-38394837.

86 "Karlov suikastını, eski adı El Nusra olan Fetih el Şam üstlendi," Sputnik Türkiye, December 21, 2016, https://tr.sputniknews.com/ortadogu/201612211026428039-karlov-fetih-el-sam/.

87 "Karlov suikastı sanığı: Menzil tarikatına bağlıyım," Sputnik Türkiye, January 11, 2019, https://tr.sputniknews.com/turkiye/201901111037037495-karlov-suikasti-sanigi-menzil-tarikatini-bagliyim/.

Positive-Sentiment Top Keywords	Occurrence	Negative-Sentiment Top Keywords	Occurrence
Karlov	12,954,371	Karlov	3,917,394
Rus_	11,720,845	Büyükelçi_	3,742,197
Suikast_	9,384,054	Öldü_	3,248,492
Büyükelçi_	7,920,581	Provok_	2,928,915
Üzü_	6,183,401	Tehdit_	2,271,601
Putin_	5,193,932	Ankara_	1,293,857
Başsağlı_	4,910,356	Oyun_	1,104,381
Dost_	3,291,603	Suriye_	958,398
Andrey	2,869,039	Halep_	769,271
Kın_	1,958,204	FET_	481,293
Halkı_	984,812	NATO	385,926
İşbirli_	750,386	Amerika_	204,385

Table 7 - Most frequently occurring n-grams in positive and negative-sentiment content and engagement clusters

We measure the centrality of actors, sentiment and content in dedicated network clusters based on the following function (Saxena et. al. 2017[88])

$$R_{rev}(u) = n + \frac{1-n}{1+\left(\frac{C(u)}{c_{mid}}\right)^{p}},$$

Where C_{mid} denotes closeness centrality of the best-connected node in the cluster, n is the aggregate number of nodes, p is the degree of the logistic curve at median.

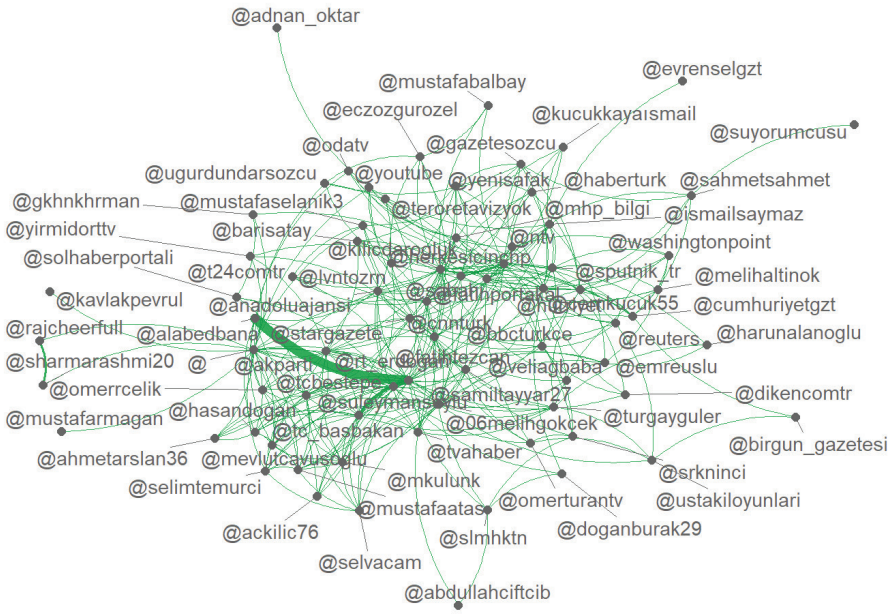


Figure 10 - Weighted centrality network of inter-account engagement within the Positive-Sentiment cluster (first 4 hours)

88 Akrati Saxena, Ralucca Gera, and S. R. S. Iyengar, "A Faster Method to Estimate Closeness Centrality Ranking," ArXiv:1706.02083 [Physics], June 7, 2017, http://arxiv.org/abs/1706.02083.

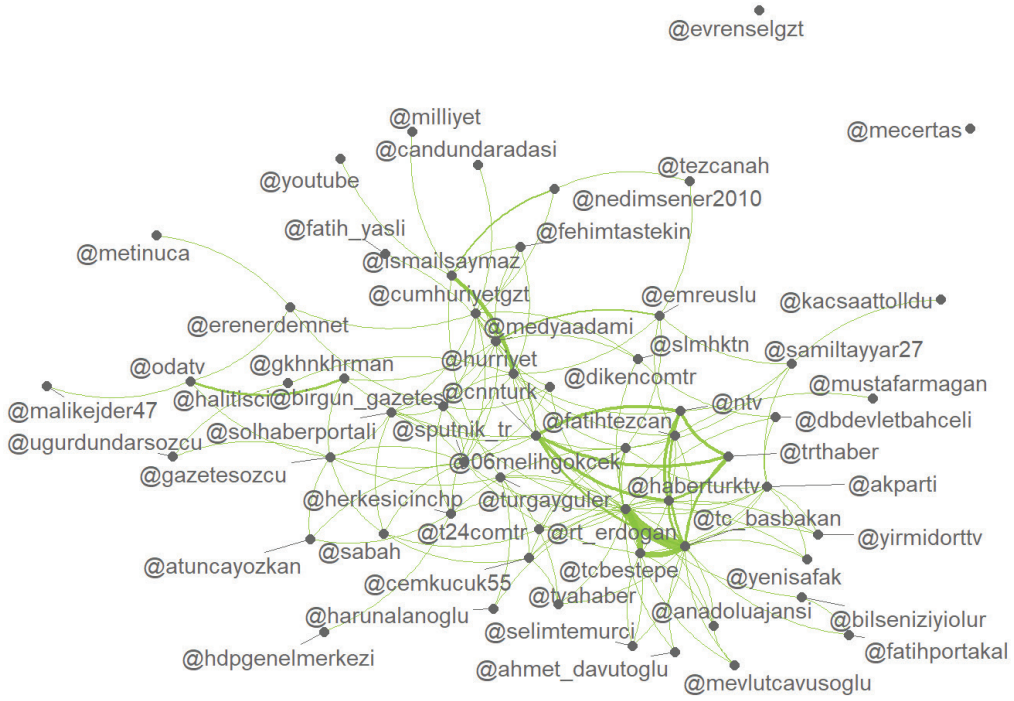


Figure 11 - Weighted centrality network of inter-account engagement within the Negative-Sentiment cluster (first 4 hours)

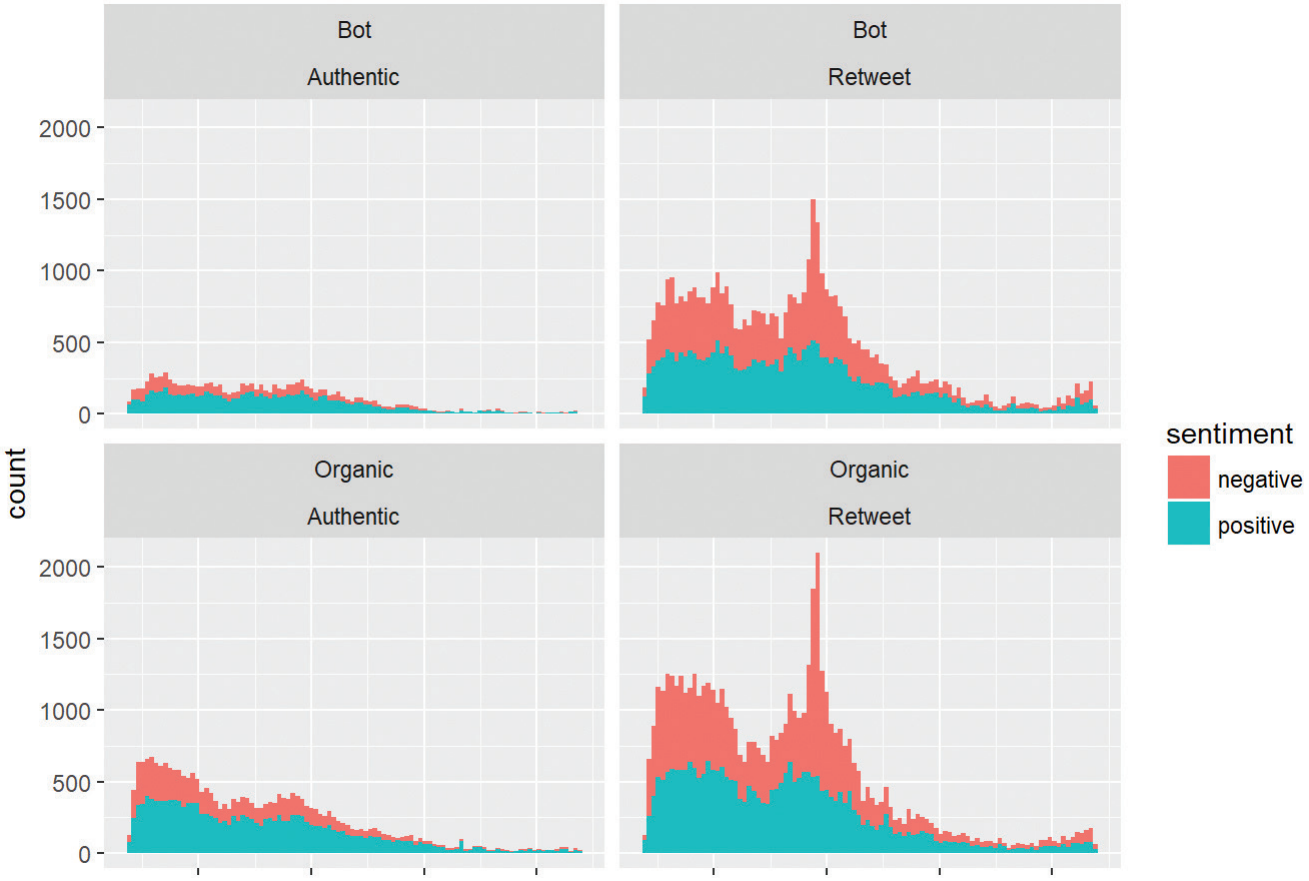


Figure 12 - 24-hour time-series analysis of LDA-designated Positive and Negative-sentiment engagement metrics, sorted by organic/bot and authentic/retweet designation. Count value in 000s.

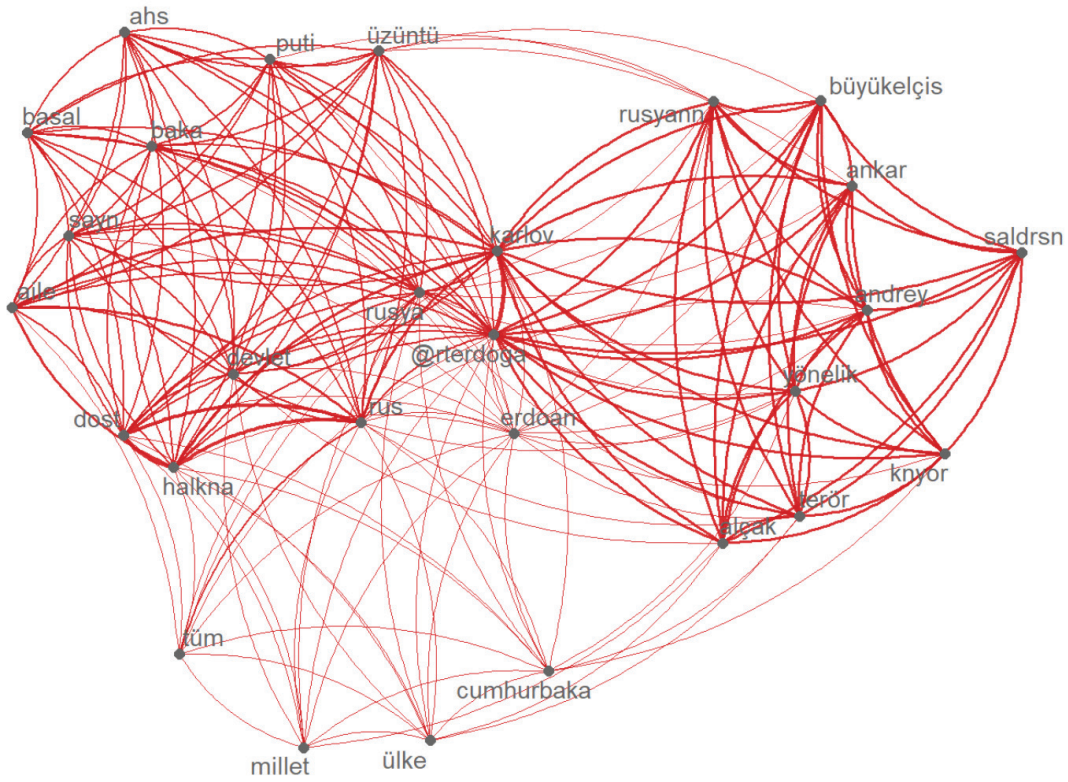


Figure 13 - Weighted centrality measures of the most frequently appearing words in organic positive sentiment tweets (first 2 hours)

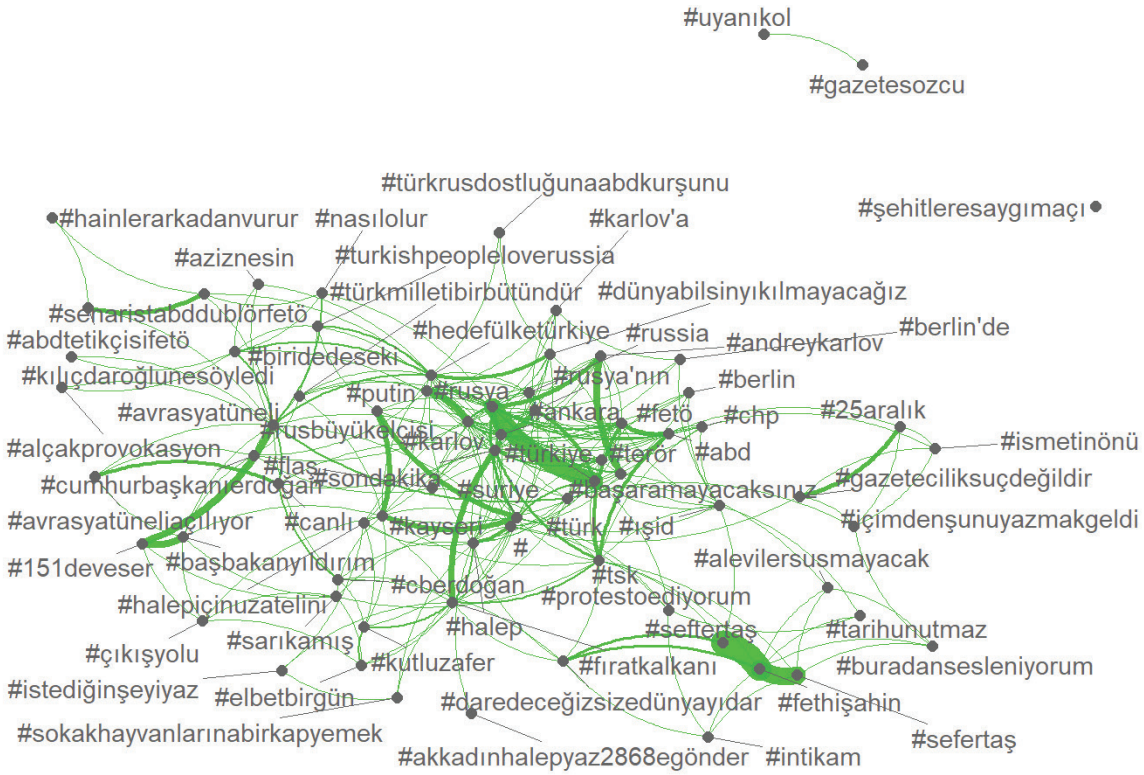


Figure 14 - Weighted centrality measures of the most frequently appearing words in bot-driven negative sentiment tweets (first 2 hours)

While the positive-sentiment mention network measures of the first 3-4 hours demonstrate convergence, negative-sentiment mention network is more fragmented. This means that tweets designated as 'positive' by our algorithm indicate greater centralized control (i.e., government-led framing attempts), whereas negative sentiment tweets originate from accounts that are either loosely tied to the government or the opposition network. This is equally valid for both organic and bot-driven content. The negative-sentiment ecosystem on the other hand (again, both organic and bot-driven) is greatly fragmented in terms of discussed topics and topic weights. Although positive sentiment score topics contain mostly organic sentiments of sadness, sorrow and solidarity between Turkey and Russia, negative sentiment score topics contain a variety of narratives driven primarily by hashtags. These are namely a) assassination being a 'provocation', b) an 'external game played on Turkey', c) a 'successful revenge' against Russian military role in Aleppo, or d) an incident aiming to pressure Turkey internationally. Also in the first 3-hours, there are occasional bot-driven negative sentiment spikes dominated by implications of US and NATO involvement in the assassination attempt. Although by the 6th hour these suggestions are eliminated from the information ecosystem as there have been sporadic resurfacing of NATO and US involvement allegations within the same ecosystem that makes such blames through the Gülen organization. The NATO and US-related blame eventually disappear from the ecosystem by the 12th hour as the most frequent negative sentiment mentions become 'terror/terrorism', 'treason/traitor' and 'FETÖ'. By the end of the first week and the return of Ambassador Karlov's body back to Moscow, the information ecosystem settles into a generally positive equilibrium as content frequency and substance both reveal mutual understanding, sympathy and condolences. Through all time frames observed (1, 3, 6 12-hour, 1-day intervals) the pro-Russian information ecosystem in Turkey has been remarkably silent. Sputnik-Türkiye and accounts that regularly lie within the Sputnik network have resorted to very few content shares. Those that they did share were mainly quotes directly attributed to the Presidency, government, and security officials.

In digital terms, this particular episode in Turkish-Russian relations has demonstrated substantial restraint on the part of the pro-Russian information apparatus in Turkey, given the silence and direct reliance on official sources in its news. Especially when compared to the aftermath of the SU24 downing incident, pro-Russian media behavior in Turkey has been significantly toned-down, asserting Moscow's confidence in the way Turkish authorities dealt with the situation. This suggests high-level coordination and confidence-building at play that would force Moscow to refrain from the kind of media assault it did with the 'ISIS oil' strategy.

Another important observation is that both positive and negative sentiment diffusion clusters orbit the same high-level official sources. Regardless of whether a network represents negative or positive sentiment content, its constituent accounts retweet and follow the same key ministries, security agencies and the Presidential office. This is an interesting finding, since all of the widely-shared content types overwhelmingly reference official organs, but interpret the statements of these official organs completely differently. This finding is especially visible within the first hour of the assassination, as negative-sentiment bots and organic accounts represent official statements in a way that fits their own agenda. It is only after the first two hours and a more explicit assertion of the official view through Presidency and ministerial accounts that these negative sentiment clusters switch to a more conciliatory and de-escalating tone.

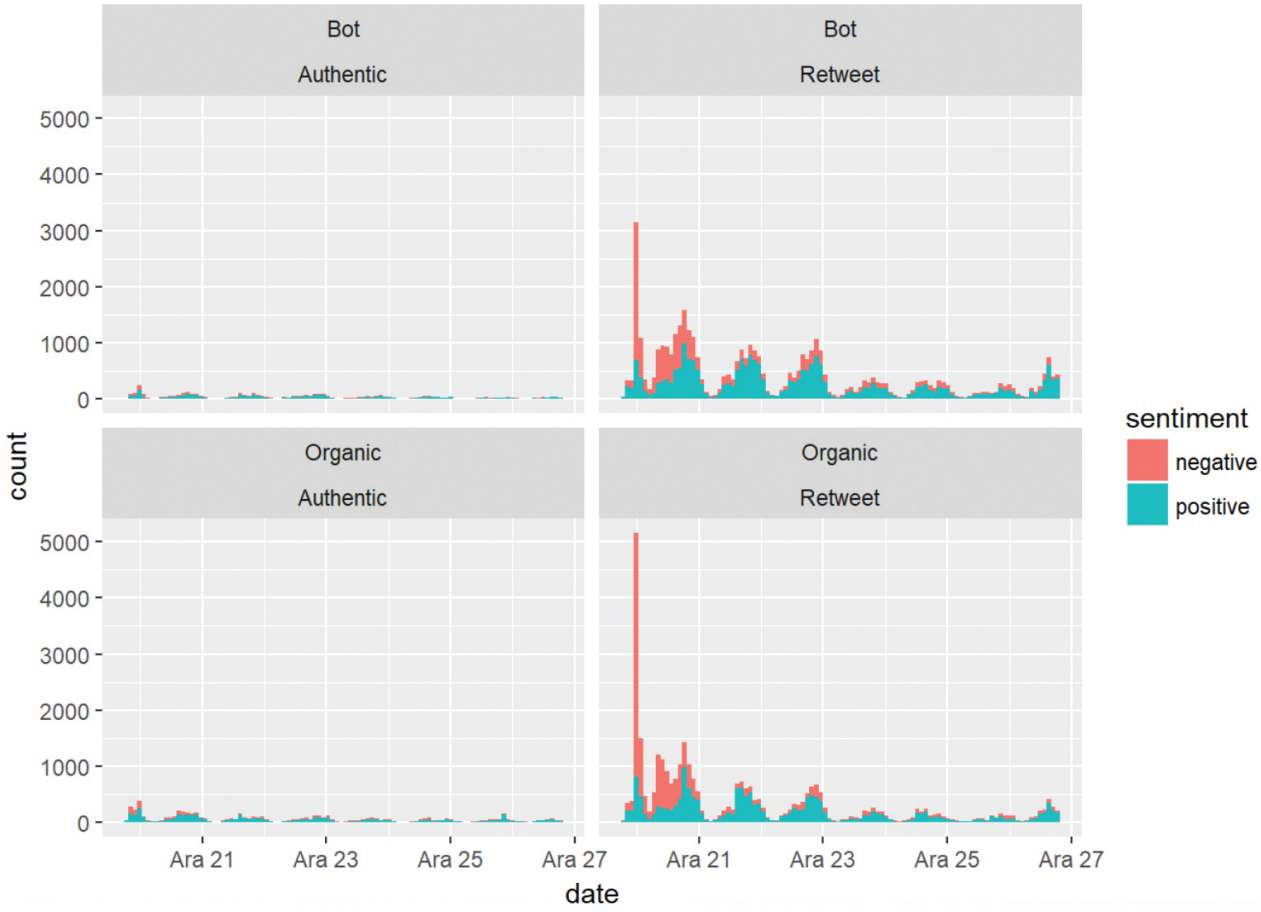


Figure 15 - 7-day time-series analysis of LDA-designated Positive and Negative-sentiment engagement metrics, sorted by organic/bot and authentic/retweet designation. Count value in 000s.

Case-3: Potential Election Meddling

Perhaps the most researched aspect of Russian involvement in digital space has been election meddling in Western democracies. While Russia's involvement in Western elections is relatively well documented, there is virtually no substantive and empirical research on similar election interference beyond these countries - and definitely no data-driven research on Turkey. This is important, since checking Russian involvement in any election meddling in Turkey would serve as a good robustness check of our findings related to the most significant crises in relations.

Although a separate, longitudinal analysis on disinformation in all Turkish election since 2010 is necessary, that would lie beyond the scope of this project. There is an endless debate in Turkish political science literature on the question of which recent election(s) were 'really' the most important for Turkey. Presenting this research in multiple occasions, we observed an acute disagreement among the attendees, all offering a different combination of elections as 'the most important'. To that end, we decided to go only with the 24 June 2018 elections for two reasons. First, it has the largest volume of data compared to all other Turkish elections with nearly 80 million tweets containing solely disinformation-related content, after data cleaning (the total volume of election data is much larger). Second, it had the largest turnout (87%[89]) among recent Turkish elections since the 1999 general elections and it was the Turkish election with the largest ever nominal votes cast (51,183,729[90]), including the 2017 referendum. To that end, it is a better robustness check compared to the alternatives.

89 "Voter Turnout in Turkey Elections Was 87 Percent: State Broadcaster," Reuters, June 24, 2018, https://www.reuters.com/article/us-turkey-election-turnout-idUSKBN1JK0SP.

90 "Son dakika: YSK, 2018 kesin seçim sonuçlarını açıkladı," Hürriyet, July 4, 2018, http://www.hurriyet.com.tr/gundem/son-dakika-ysk-2018-kesin-secim-sonuclarini-acikladi-40886560.

To trace Russian involvement in Turkish digital disinformation ecosystem during the election, this study focuses on 6 of the most popular of such cases (measured by more than 50,000 engagements within the first day) on or before 24 June. These cases are exposed as disinformation and were fact-checked by Teyit.org.

1. Allegation that Erdogan called Meral Aksener 'zilli' (1,492,493 combined engagement): One of the odder, yet significant disinformation types was the allegation that President Erdoğan had called a major opposition leader Meral Aksener 'zilli'[91] - a slang word that has a wide spectrum of meanings, closest in this context being 'shrewish'. Originally appearing in a public Facebook page called 'İzci', the disinformation attempt lashed out at President Erdoğan for his lack of tact during his party's convention, by referring to Meral Akşener in slang terms. In reality, there never was such a statement, evidenced by President Erdoğan's full speech, available on Youtube[92]. The content spread quite rapidly across opposition-nationalist information ecosystem, also spreading to the pro-government network within the same day. Similar to other disinformation cases, although the correction and fact-checking content appeared on social media outlets within the a few hours of its dissemination, this disinformation type took on a life of its own and it was shared frequently until the election day on 24 June. There is no node or network in this disinformation ecosystem that could be traced to pro-Russian sources.

91 "Erdoğan'ın Meral Akşener hakkında 'Zilli Meral Kemal'in eteklisi' dediği iddiası," teyit.org (blog), May 7, 2018, https://teyit.org/erdoganin-meral-aksener-hakkinda-zilli-meral-kemalin-eteklisi-dedigi-iddiasi/.

92 Full video can be accessed at: https://www.youtube.com/watch?v=FKpQ0irG6aE

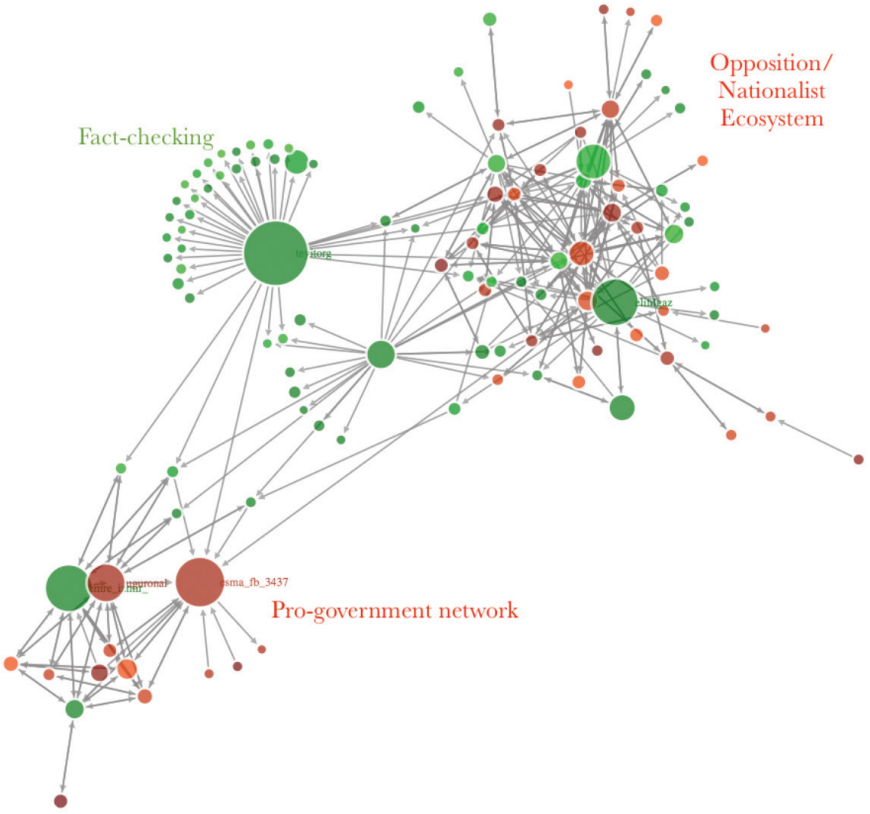


Figure 16 - Sample content and first 2-hour diffusion network of the 'zilli' disinformation

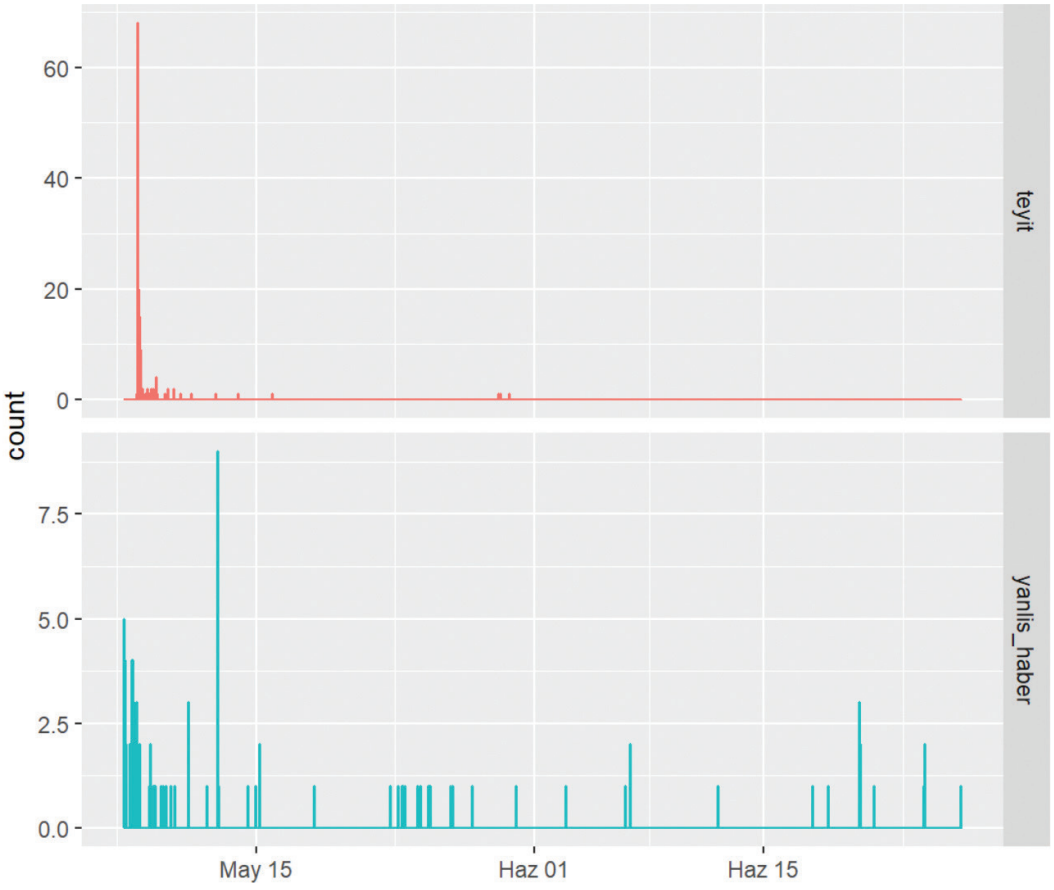
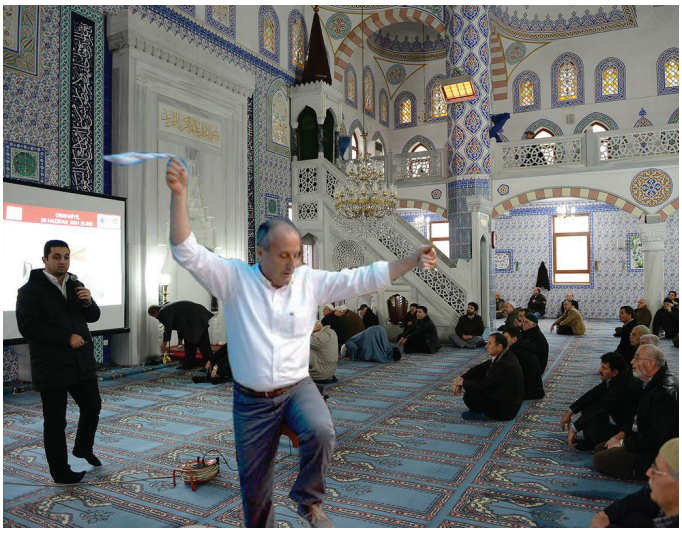


Figure 17 - Time-series engagement graph showing the popularity of the fake news(below) and fact-checked (above) content

2. Muharrem Ince dance (2,491,385 combined engagement): The widest-shared disinformation regarding the main opposition candidate Muharrem Ince was a photoshopped image of him, dancing in a mosque[93]. As absurd as the statement sounds, the doctored image of a dancing Muharrem Ince overlaid into a mosque interior became one of the most shared digital content types of the election. The content can be traced back to a very distinct pro-government network, in which former Ankara mayor, Melih Gokcek appears to be the overwhelmingly central node based on the function we import from Saxena (et. al. 2017[94]). There is also a distinct bot network involved in the initial spread. Rather than any pro-Russian ecosystem, this disinformation type can be traced into a distinctly pro-government media and opinion network.



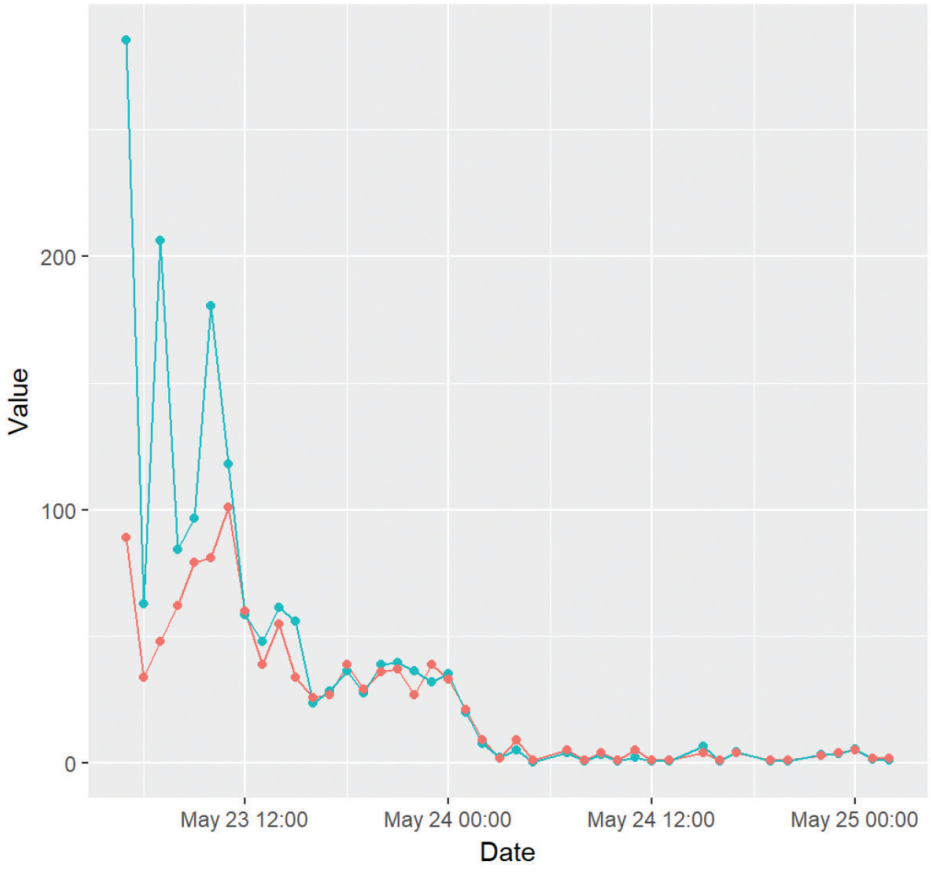


Figure 18 - Time-series engagement with the fake news (first 1.5 days).
Blue: Engagement through popular (high follower count) accounts, Red: Nominal value of engagement

93 "Fotoğrafın Muharrem İnce'nin camide halay çektiğini gösterdiği iddiası," teyit.org (blog), May 9, 2018, https://teyit.org/fotografin-muharrem-incenin-camide-halay-cektigini-gosterdigi-iddiasi/.

94 Saxena, Gera, and Iyengar, "A Faster Method to Estimate Closeness Centrality Ranking."

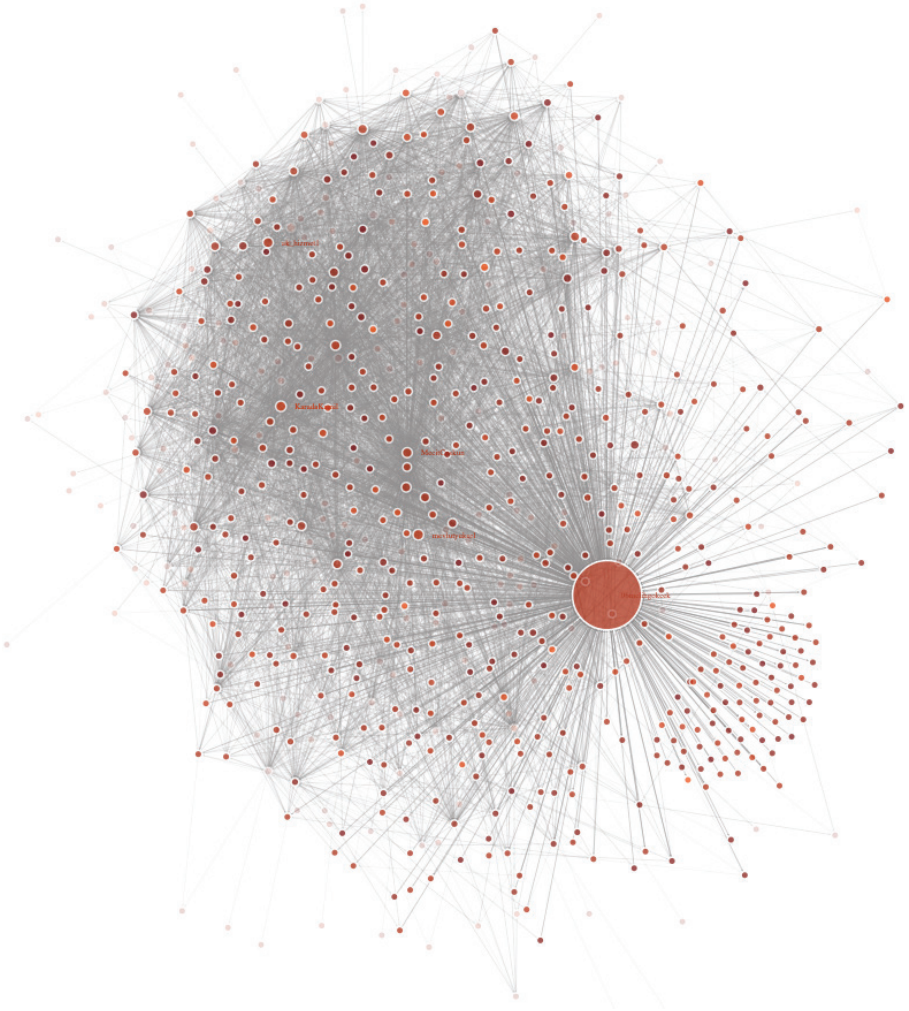


Figure 19 - The diffusion network (overwhelmingly pro-government) of the fake news. The large red dot represents @06melihgokcek – which assumes disproportionate centrality in the diffusion network.

3. Alleged Election Fraud in Diyarbakır (1,375,482 combined engagement): Another major disinformation case that proliferated on the day of the election was the allegation that a voting site (Mesut Yilmaz primary school building) in Diyarbakır was visited by three members of the Higher Electoral Board (YSK)[95]. These officials, according to rumors, looked suspicious and tried to force ballot box administrators and observers to agree to fraudulent behavior. Shared by a local district official from the People's Democracy Party (HDP), the image of the YSK members accompanied by police officers circulated far and wide on social media, creating widespread upheaval in an already-tense city. After multiple inquiries, it was revealed that the YSK team was sent to the voting site following an additional envelope request by the voting site scrutineers and had ultimately reached an agreement with the HDP officials[96]. Although the verified version of events was also disseminated on social media, the misunderstood image and the content became shared far more across social media venues, warning all observers and voters to 'be careful against YSK officials'. This predictably caused substantial problems in a number of voting sites during regular and scheduled YSK observer visits.

95 "Diyarbakır Mesut Yılmaz İlkokulu'nda boş zarflarla dolaşan kişiler kim?," teyit.org (blog), June 24, 2018, https://teyit.org/diyarbakir-mesut-yilmaz-ilkokulunda-bos-zarflarla-dolasan-kisiler-kim/.

96 "Emniyet Müdürü: YSK'dan zarf talep etmiş," HaberTurk, June 24, 2018, https://www.haberturk.com/diyarbakir-da-muhurlu-bos-zarflarda-yanlis-anlasilma-2029291.

This particular case of disinformation invalidates an important theory of communication, which in essence, argues that strengthening local news is the best way to combat fake news at the national level[97]. Proponents of this argument posit that if local journalism is supported and strengthened, on-the-ground reporters would do a much faster job in validating false claims before they could reach the national level. In our particular case however, the opposite happened. Local news agencies have been the main sources from which disinformation emerged, spread and picked up by national news. Although HDP officials later clarified the situation, most local news agencies did not share the fact-checked version of events, creating around 6-8 hours' time lag until engagement with this content declined visibly. The weighted centrality of this disinformation case is clustered around local news outlets in Diyarbakır. In addition, there are a number of marginally important anonymous organic accounts that are unidentifiable in terms of their political allegiances, either from their profile information, or text analysis of their tweets. These accounts cannot be traced to any pro-Russian network in Turkey and remain outside of the central pro-Kurdish news network diffusion mechanics (see Fig. 21).

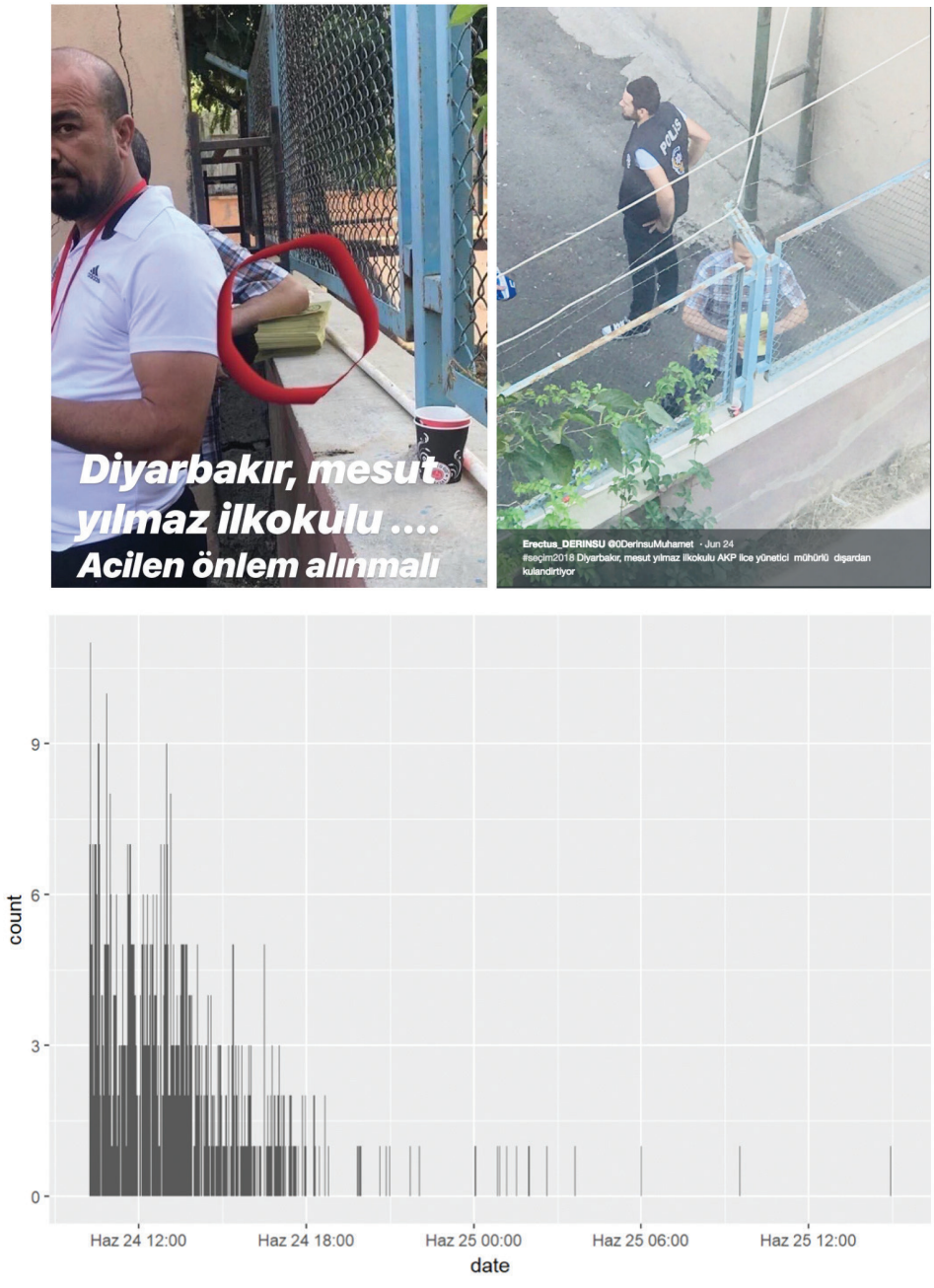


Figure 20 - Sample content types and time-series engagement with the Diyarbakır fake news case

97 Damian Radcliffe, "How Local Journalism Can Upend the 'fake News' Narrative," The Conversation, November 27, 2018, http://theconversation.com/how-local-journalism-can-upend-the-fake-news-narrative-104630.

Figure 21 - Spread network of the disinformation. Starting from local news sources, the fake news was ultimately nationalized through Twitter

4. Alleged Erdoğan Rally Mistake (1,371,964 combined engagement): This case of disinformation alleged that President Erdoğan, in an election rally in Bursa, mistakenly addressed the crowd as 'the people of Sakarya', confusing which city he was in[98]. This disinformation type was shared frequently with other minor attempts that pointed to the old age of the President and his slip ups and mistaken statements, questioning whether he was fit to rule the country. In reality, Erdoğan was citing a folk song, which contains the words 'Sakarya', but did not confuse his audience[99]. Originating within the opposition network cluster more aligned with the Republican People's Party (CHP) this was one of the fastest-spreading fake news cases we encountered (See. Fig.21). The role of bots is minimal in this case, as the organic opposition network has contributed heavily to the dissemination of such content. Despite the fast fact-checking of Teyit.Org, the fact-checked version of events was marginalized by the vast wave of accounts involved in the disinformation effort, willingly or unwillingly. No pro-Russian network is observable in this case.

98 For a popular example, see: https://twitter.com/avcimucahit/status/1006221787846324225

99 "Cumhurbaşkanı Erdoğan'ın Bursa mitingindeki kalabalığa 'Sakarya' diye seslendiği iddiası," teyit.org (blog), June 12, 2018, https://teyit.org/cumhurbaskani-erdoganin-bursa-mitingindeki-kalabaliga-sakarya-diye-seslendigi-iddiasi/.

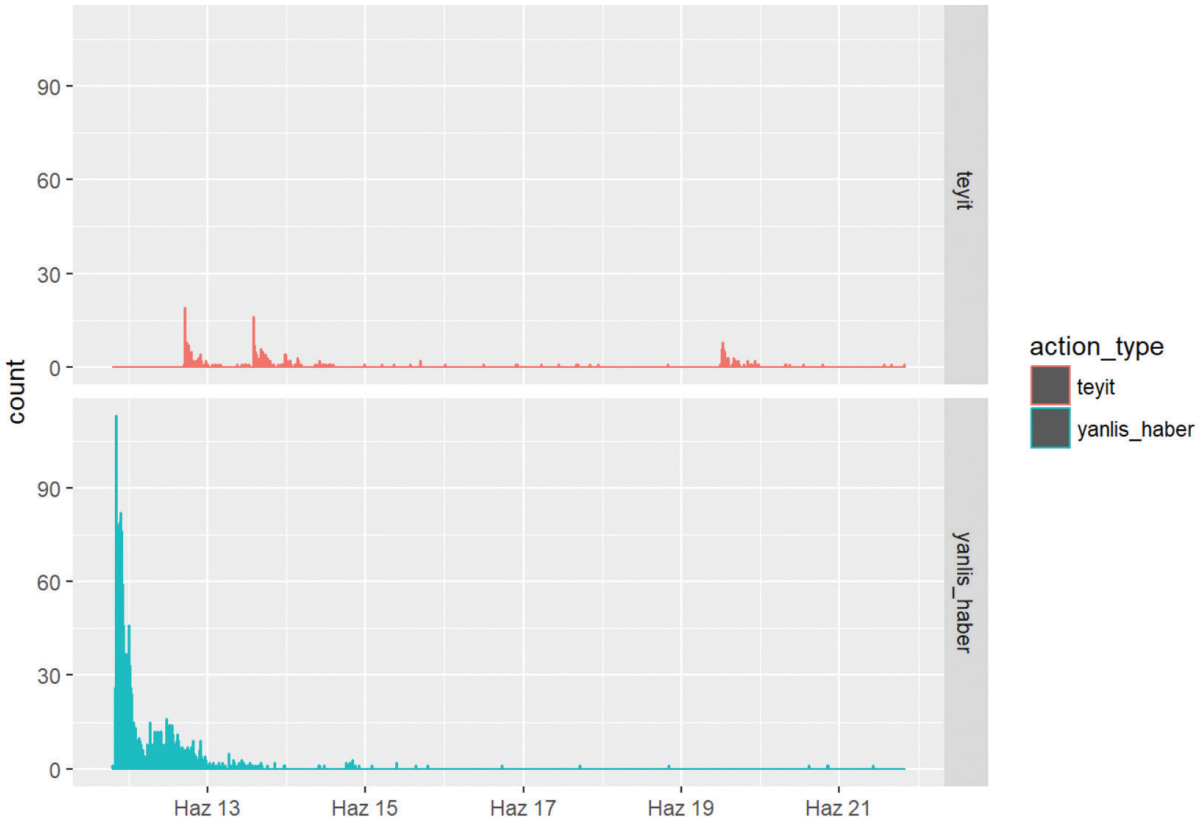


Figure 22 - Time-series diffusion and engagement patterns of the fake news (blue) and its fact-checked version (red)

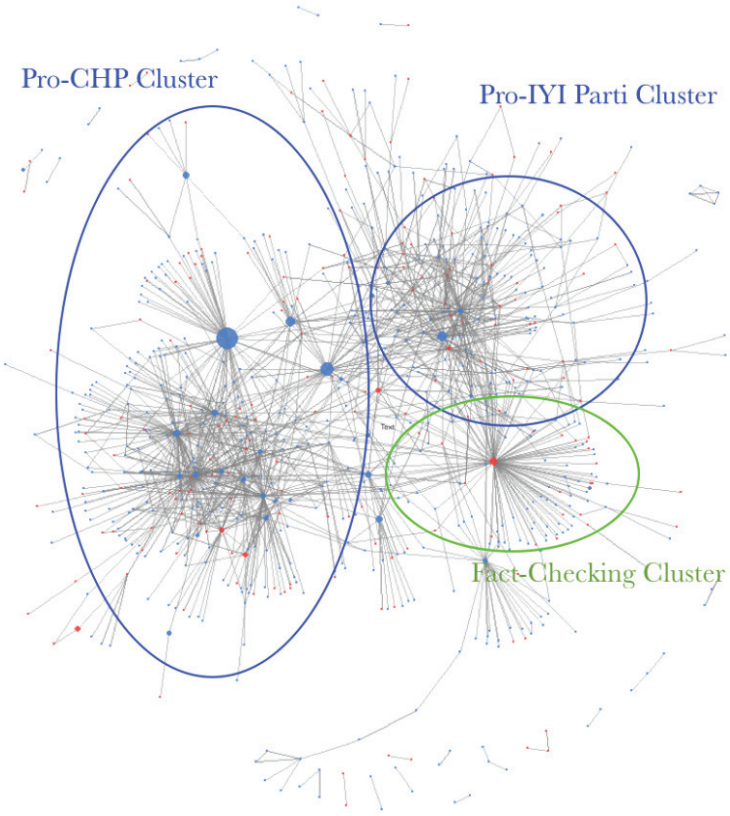


Figure 23 - Despite fact-checks (red), the overwhelming majority of the engagement with the fake news (blue) demonstrates wide reach and dissemination. Politically, the cluster is overwhelmingly made up of opposition politicians, journalists and celebrities that are politically highly engaged with each other. In other words, the network represents an overwhelming opposition network.

5. Allegation that Ince was in a coffeehouse during the coup attempt: The allegation that Muharrem Ince, the main opposition candidate was in a coffeehouse, playing *rummikub* during the night of the coup was disseminated widely by the pro-government conventional news accounts like Yeni Akit, A Haber and Takvim[100]. Using a photo from December 2014, these news outlets began circulating the disinformation attempt online. This was one of many similar disinformation styles of the pro-government media ecosystem blaming senior members of the opposition parties for not 'doing enough' during the coup attempt. The interesting point with this particular case of disinformation is that the opposition network is equally active in disseminating it as the pro-government network. Of further interest is the fact that it was another pro-government account (@Ankara_Kusu) that eventually spearheaded the fact-checking effort in the first hours of the spread.[101] There are no pro-Russian accounts observable in the early impact network of this

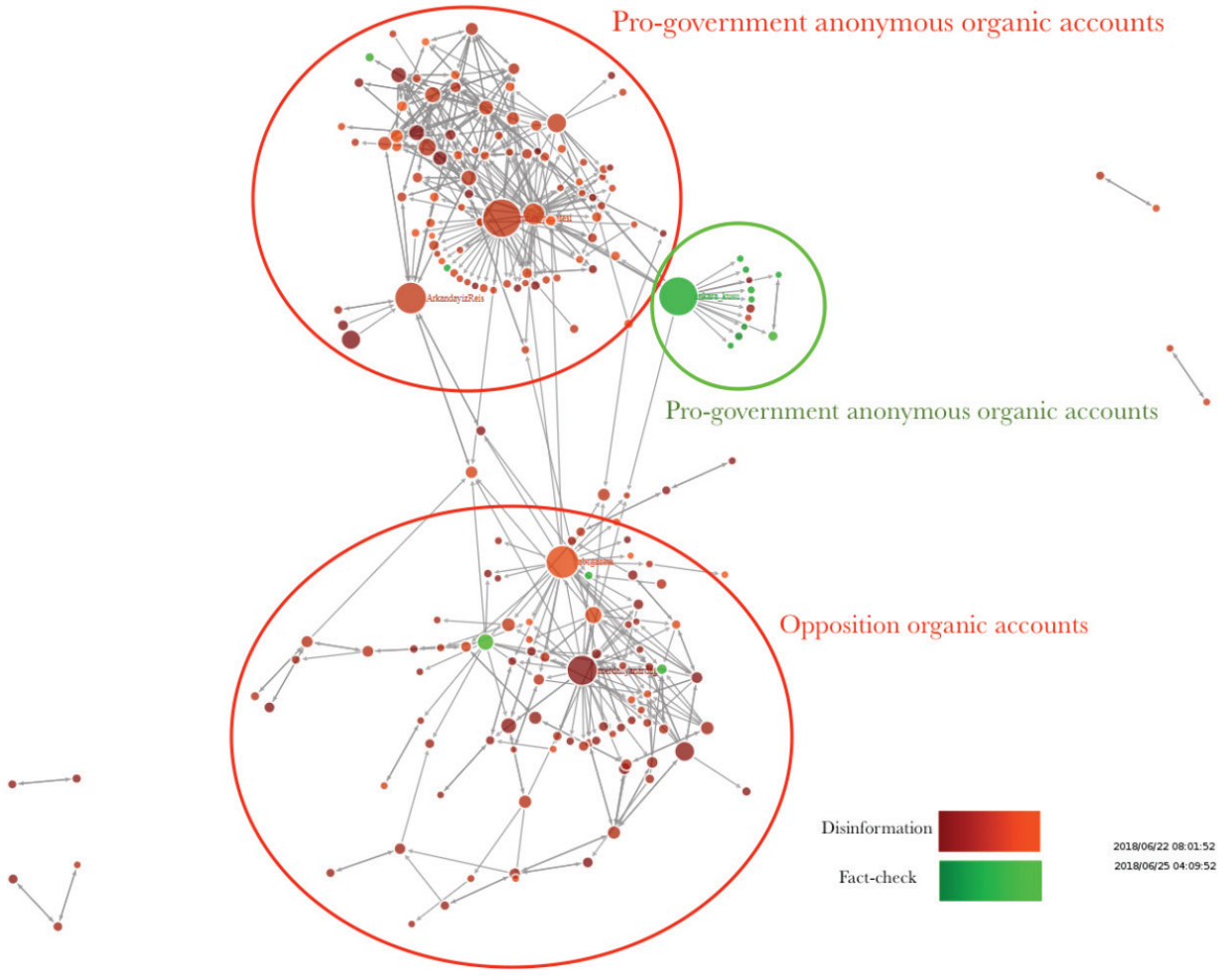


Figure 24 - Muharrem Ince-related disinformation content example and diffusion network

[100] "Darbe gecesi tavla partisindeymiş," Sabah, June 22, 2018, https://www.sabah.com.tr/gundem/2018/06/22/darbe-gecesi-tavla-partisindeymis.

[101] See: https://twitter.com/ankara_kusu/status/1010272819073179649

6. Disappearing ink: By noon on the election day, Ruhat Mengi - a Turkish journalist - warned her 62.5k followers that a friend's relative had spotted a tampered ballot stamp. According to the allegation, a 'special ink' was distributed by the government to voting sites that regularly vote against the ruling AKP and Erdoğan, and was an elaborate plan to render all votes in opposition districts 'null'. This message was retweeted and shared across media platforms within minutes and became shared by some of the most influential journalists and politicians online.

Our analysis shows that the tweet was actually shared much earlier in the morning (06:26am) by a university student in Ankara[102], and spread across several other platforms and social chat channels before reaching Ruhat Mengi by noon. Evidently, there was no verified report in any medium regarding any 'disappearing ink'; this allegation was later fact-checked and corrected. Still, the tweet retained its potency and got shared online for hours to come. This was a truly cross-platform disinformation example, as tracing its course solely through Twitter yields insufficient results. Several examples on Facebook, Whatsapp, Eksisozluk and Instagram were spotted by our research team, although establishing a clear causal cross-platform linkage is very difficult.

Diffusion patterns reveal that although the fake news originally emerged within the opposition network, it was later picked up by a number of highly influential ultranationalist anonymous accounts to fact-check and stop its diffusion. After its fact-checked versions appeared online, pro-government accounts spread both the fake news and the fact-checked version in order to mock the opposition network due to the strangeness of their claim. Although the opposition network originated the content, it was mostly the pro-government networks mocking the claim that contributed to the widest diffusion of this disinformation type. We haven't encountered any accounts in this network that could be connected to the pro-Russian information ecosystem.

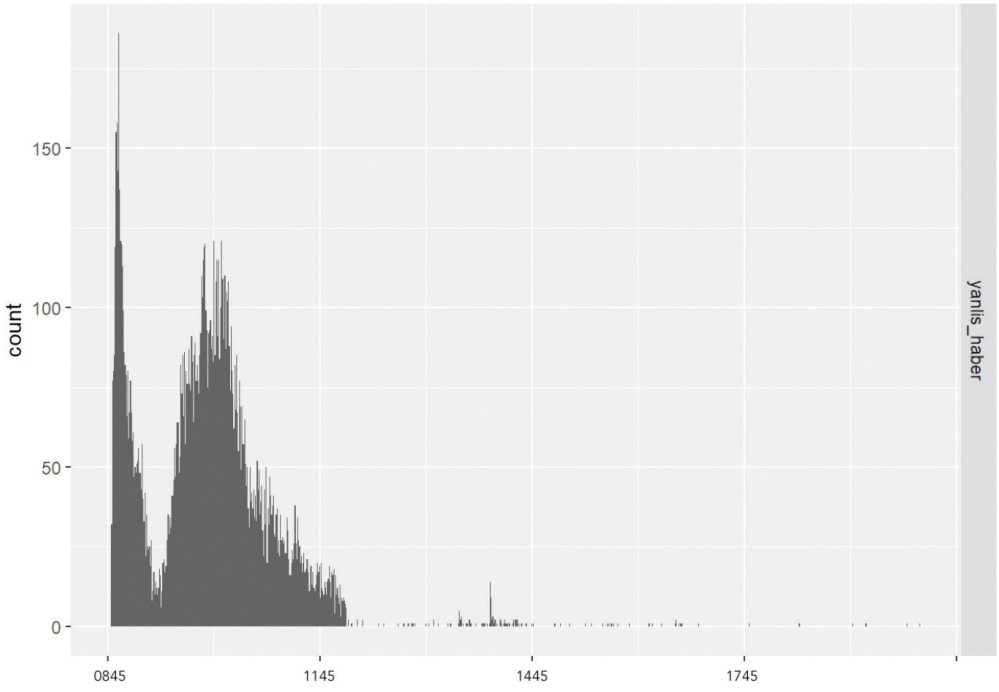


Figure 25 - Sample content type engagement metrics of the 'disappearing ink' fake news

[102] Tweet link: https://twitter.com/MazharCoban/status/1010786264944128001

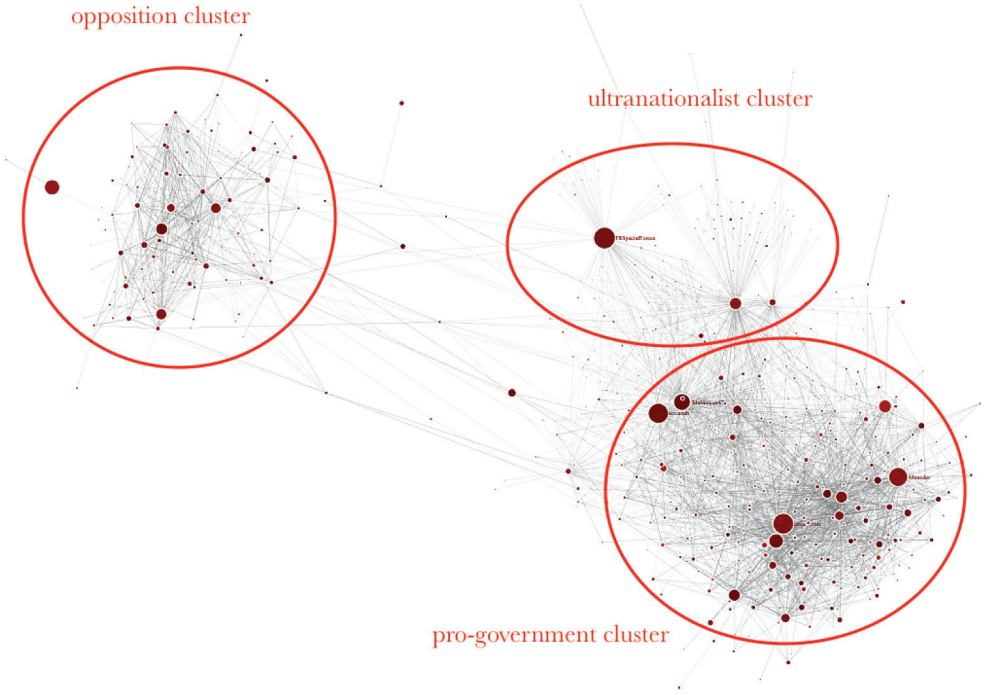


Figure 26 - Diffusion network of the fake news (first 6 hours)

Case-4: S400 Procurement Process

Another critical case study for Russian information ecosystem in Turkey is the S400 saga. Syrian Civil War had heightened Turkey's threat perceptions and made the country's long-term dependence on NATO for aerial defense more glaring. Although Patriot missile batteries were deployed along the border, operated by American, German, Dutch and Spanish crews in turns, Turkey viewed the delays in the arrival of these batteries as highly problematic to its immediate national security concerns. Eager to become more self-sufficient and prevent such critical delays in the future, Turkey sought resident anti-air batteries. Initially reaching out to Chinese anti-air systems, this move was abandoned due to China's reluctance to fulfill Turkey's technology transfer criteria[103]. Then, Turkey showed interest in Russian S400 systems, seeking to secure a better technology transfer and co-production deal. Ultimately, an agreement was reached in September 2017, when President Erdoğan stated that the deal with Russia was a foregone conclusion, leading to the 2.5 billion US Dollar signing in December. Yet, this deal has no technology transfer or co-production clause as well. The first S400s systems were then announced to be delivered in 2019.

In a search for pro-Russian information flows through this period, this study has benchmarked five events:

a. 10 October 2016 when Turkey and Russia declared that serious Presidential-level negotiations were underway over S400 sales,
b. Erdoğan's 10 March 2017 visit to Moscow to assert Turkey's commitment to S400,
c. 29 December 2017 commercial agreement between the two sides,
d. 3 April 2018 President Erdoğan's statement on Turkey's 'point of no return' on S400 purchase,
e. 19 August 2018 President Putin's statement that deliveries could be made a year earlier than planned.

In these periods, we have measured pro-Russian and anti-Russian sentiments on Turkish-language Twitter, as measured by our topic modeling algorithm that we trained on Turkish political text. It is interesting to observe the gradual transition of the sentiment scores related to S400s from mixed (negative and positive) to mostly positive through these five cases we observed. The October 2016

[103] "Turkey Confirms Cancellation of $3.4 Billion Missile Defence...," Reuters, November 18, 2015, https://www.reuters.com/article/us-turkey-china-missile-idUSKCN0T61OV20151118.

declaration was mostly met with mixed views by the Turkish-language Twitter. Digital opinions shared on the matter split between whether S400s are ultimately good (positive sentiment) or bad (negative sentiment) for Turkey. Due to the technical nature of S400 negotiations, we observe a general restraint by users to post authentic tweets, and rather their preference for retweeting reports on the deal published by familiar media outlets. The even split between positive and negative sentiments gradually eases down and positive sentiment scores prevail at an increasingly greater margin across five benchmarked events, ultimately becoming the mainstream consensus in Turkish-language Twitter. Especially with the August 2018 statement by Putin, the overall interest in S400s both decline and converge on a generally positive sentiment.

As shown on Table-8, some of the main words designated as 'negative-sentiment' topic cluster contain interoperability issues with existing NATO equipment, commitment to NATO regarding the deployment of Patriot missile batteries, and to what extent S400 acquisitions will influence Turkey's bid to buy F-35 jets from the United States. Such content viewed S400s not as diversification, but strategic confusion as it brought operational problems with potentially real-life consequences. Positive-sentiment topic cluster words, on the other hand, contain n-grams that belong to digital content that question the relevance of NATO, importance of Turkey's security autonomy, and technical information about S400s (such as its range and capabilities) largely interwoven with Erdoğan's supportive statements about the missile systems. Because we look at the longitudinal changes in sentiment scores, S400 deal is an overall good way to observe the gradual shift of the Turkish information ecosystem from an ambivalent view towards Russia, into a mostly pro-Russian view. The topic clusters show, however, that this pro-Russian sentiment is less about Turks 'liking' Russia, and more about their views about converging strategic interests in a limited pool of issue areas.

Long-term sentiment scores also add substantial depth to our previous findings. In terms of the domain roots of positive and negative-sentiment content, we clearly observe that the pro-Russian opinions have been quite well-integrated into the pro-government mainstream (Table-9). Because S400s have largely been framed within the context of strategic autonomy and greater self-sufficiency in anti-air defensive capabilities, both nationalist anti-government and pro-government media clusters (that are usually non-converging) are mostly converging in unison support. Negative sentiment clusters appear to have converged along the mainstream center-right and centrist media outlets, although their share gradually declines as positive-sentiment content becomes the main expression regarding the S400s.

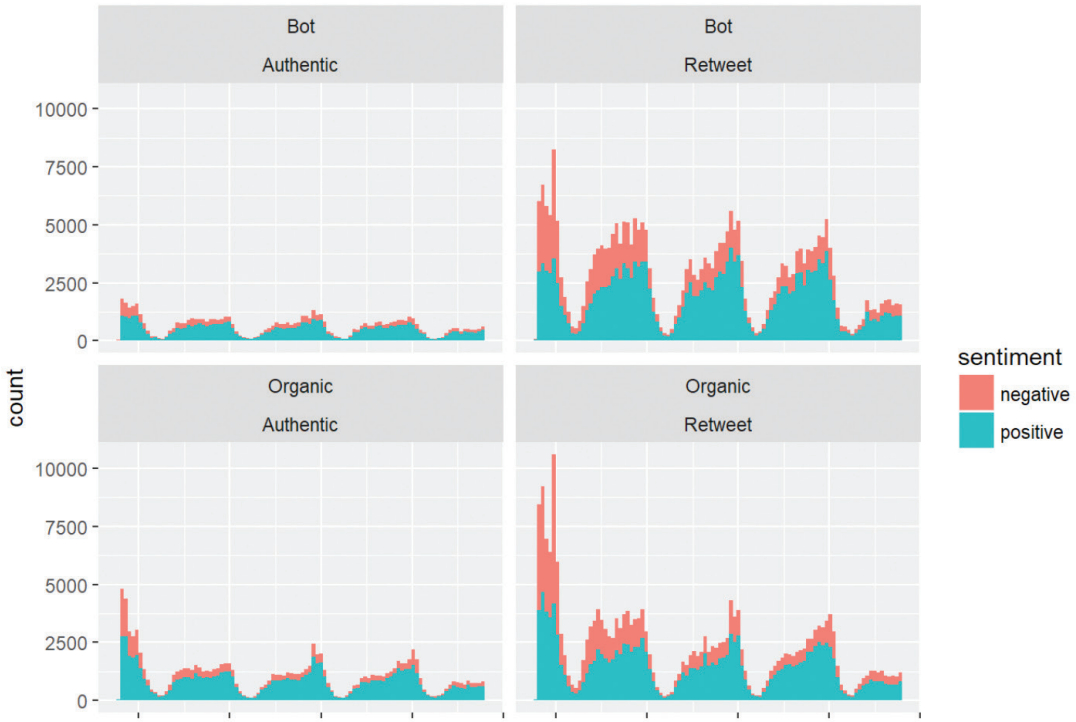


Figure 27 - - Time-series diffusion of positive and negative sentiment scores towards S400 missiles based on organic/bot and authentic/retweet clusters. Date range 1 October 2016 – 1 September 2018. Peaks represent engagement during five benchmarked events.

Negative Sentiment Top Keywords	Occurrence	Positive Sentiment Top Keywords	Occurrence
S400	1,382,385	S400	6,492,695
Füze_	1,294,016	Türkiye	6,329,593
Birlikte_	1,184,603	Savunma	5,938,149
NATO	1,035,596	Hava	5,394,014
F16	939,503	Karşı	4,205,699
Patriot	929,458	Erdoğan	4,144,923
Entegre	837,814	Bağımsız_	3,948,391
Savunma	742,559	Yüksek	3,854,553
Altyapı	693,941	Kapasite_	3,469,319
Kullanılabi_	491,394	Menzil_	3,194,966
Türkiye	443,644	Füze	2,847,471
Kongre_	385,193	Güvenli_	2,638,383
F35	293,004	Sınır	2,385,993

Table 8 - Most frequently occurring n-grams in positive and negative-sentiment content and engagement clusters

Negative Sentiment Domain	% Share of Aggregate Tweets	Positive Sentiment Domain	% Share of Aggregate Tweets
Hurriyet.com.tr	22.382	Sabah.com.tr	27.294
CnnTurk.com.tr	19.504	Yenisafak.com	21.953
Sozcu.com.tr	17.828	HaberTurk.com.tr	19.144
Cumhuriyet.com.tr	15.382	Ahaber.com.tr	13.048
T24.com.tr	13.449	Star.com.tr	8.032
bbc.com (Turkish)	6.486	OdaTV.com	5.392
DW.com (Turkish)	3.291	Tr.Sputniknews.com	5.019

Table 9 - Top domains within positive and negative-sentiment content and engagement clusters

CONCLUSION

This report sought to explore the impact and relevance of pro-Russian information operations in Turkey. To do this, it traced pro-Russian information flows on Twitter across some of the most important events in Turkish-Russian relations and two of the most important cases for Turkey individually to act as an analytical robustness check. In doing so, this study has become one of the largest longitudinal digital information studies ever conducted. This study has discovered that with the exception of the Russian allegation that Turkey was selling oil to ISIS, accounts or content traceable to Russia with a high degree of certainty have close to zero influence on Turkey's digital information ecosystem. Compared to Russian disinformation and opinion manipulation efforts in most of the Western countries that are both easy to map out and have a visible impact on politics, similar activities in Turkey are both less explicit, and also overwhelmingly insignificant. This doesn't mean Russian disinformation or information operations don't exist in Turkey. Rather, this means that they don't have any measurable impact on the wider Turkish-language information ecosystem, whereas distinctly pro-Russian views are disseminated by mainstream pro-government and opposition media networks.

This finding is important. Given the scale and directness of both disinformation and election meddling in Western democracies, Russian digital media presence in Turkey is minimal. This begs the obvious question: Why?

The first answer that this research can provide directly through the empirical evidence is that pro-Russian opinion is well-embedded within the existing Turkish information sphere. In that, pro-Russian sentiments and opinion are already integrated into the media mainstream without any need for pro-Russian information operations. This doesn't mean that criticism of Russia has completely disappeared from the ecosystem; rather, in cases most directly relevant and important for Russia (Syria, Ukraine, natural gas partnership, defense deals or nuclear energy) the pro-government media apparatus visibly follows a pro-Russian line. When the pro-Russian content pressures the government, it is picked by the opposition network. In contrast, when the pro-Russian content validates the government's position, it is picked by the pro-government network. This bandwagoning behaviour can be viewed as a by-product of the strategic alignment (or entrapment, depending on one's point of view) between the two countries that could be observed in tangible strategic/security policy areas.

The second answer is that the Turkish information ecosystem is already so plagued with disinformation and domestically-generated fake news, that bits and pieces of cases traceable to Russia end up getting suffocated within the larger ecosystem. In two highly important cases for Turkey, the failed 2016 coup attempt and 24 June 2018 elections, domestic and indigenous disinformation attempts completely overwhelm the information ecosystem, rendering (dis) information content traceable to Russia highly insignificant. This shouldn't come as a surprise, as Turkey is already one of the most bot-infected countries in the world and have one of the lowest resistance to fake digital news. Yet, this evidence connects to the popular theoretical debate on whether pre-existing disinformation ecosystem renders further external disinformation easier or harder to make an impact. The general consensus in the political communication literature is that a free press, open media environment and freedom of expression render disinformation less effective and easier to spot, as the 'marketplace of ideas' is expected to quickly verify fake information and remove it quickly. This is what we have seen in France during the 2017 election, for example. Yet, the evidence presented in this report doesn't support this theory; it actually supports the exact opposite.

This leads to a second question: are Russian information attempts insignificant because of Turkey's pre-existing information landscape, or, bluntly put, is Russia not trying? Based on the sustained damage Russia wreaked with the 'ISIS oil' information campaign, it is possible to argue that in most cases, Russia has so far refrained from flexing its digital informatics muscles. This could be a direct result of changing strategic prerogatives in Ankara and Moscow, and the resultant convergence of short-term security interests. To that end, after Ankara's gradual strategic shift that began with Russia's entry into the Syrian Civil War in the summer of 2015, and especially following the first Erdogan-Putin meeting in August 2016, Russia appears to have followed a different 'sub-threshold' protocol for Turkey compared to other NATO countries. This is best exemplified by the general silence of the pro-Russian accounts in Turkey following what could have become a near-ideal exploitation point: the assassination of the Russian Ambassador. Yet, instead of launching an information campaign similar to those observed in other major NATO countries, pro-Russian accounts have chosen to share direct quotes from Turkish officials and stuck to the facts. The S400 negotiations are also indicative of the gradual transition of the Turkish information

ecosystem from a divided sentiment on Russia to a generally positive equilibrium. Evidenced by the high shares of pro-Russian content shared across mainstream Turkish media outlets, a major Moscow-led effort to establish a separate large-scale pro-Russian outlet or network in Turkey doesn't seem necessary. In other words, there seems to be no logic in destabilizing an already pro-Russian information network through further disinformation. Furthermore, Turkey's native information ecosystem is already highly contaminated with regular fake news that surmounting the pre-existing disinformation hurdles would probably require a great deal of financial and human-resource investment on Russia's part.

On a closing note, disinformation in Turkey in general and external information operations in particular (pro-Russian or otherwise) are gradually becoming better observable in the 'dark social media' (i.e., comments sections of hidden or restricted pages). Instead of the open and easily observable medium of Twitter and Facebook, newer forms of opinion manipulation are emerging in restricted pages on Facebook, Instagram and Turkey's own Reddit: EkşiSözluk. These outlets are the next emerging frontier in disinformation research; although at their current state, they are not very significant or able to influence the mainstream debate. Future studies interested in disinformation research in Turkey could benefit from an extended digital ethnography work on several of these restricted/hidden pages to see to what extent discussion there influences the wider debate. Another potentially important avenue would be communication apps like WhatsApp, Signal or Telegram, although these avenues bring their own data availability challenges. Yet, the most promising line of research seems to compare Russian information operations in Turkey with other countries where Russia is expected to meddle in, but doesn't. Bulgaria, Hungary, Poland or Romania could offer important comparative insight.

Furthermore, there is a strong case for looking into Russian disinformation about Turkey, in other NATO countries. It is by now common knowledge that Russian disinformation campaigns are aimed to polarize and distract public opinion within NATO. It is also known that in almost all NATO countries, immigration, Turkey's role in the EU refugee deal and Turkey' EU membership bid have all been used to fuel the rising far-right and contribute substantially to issue-specific polarization. The most obvious case would be the impact of the well-known Brexit referendum fake news, which asserted that Turkey would be joining the EU and also suggesting that Turkish migrants would come to the UK in large numbers if the voters chose to remain in the Union[104]. Given the success of Russian-origin immigration and refugee disinformation in the European Union (on Syrian refugees[105]) and the United States (on Mexican immigrants[106]), dividing NATO further by pushing anti-Turkish agenda in native-language digital domains in the West would fit well with wider Russian plans. After all, the 'ISIS oil' information operation demonstrated how well Russia could turn NATO against Turkey when it wants to. Further research on how Turkey-related disinformation content is shared within European and US information ecosystem would be a natural next step to follow up after this study.

Yet, in exploring both 'dark social media' or Turkey-related information operations among NATO countries studies have to look beyond the availability bias of 'disinformation exists' and try to explain whether such attempts matter or have any impact on either the mainstream information ecosystem. Most importantly do Turkey-related disinformation efforts generate any measurable outcome such as mobilization or alter electoral behaviour like it did during the Brexit referendum campaign. Most recently, Grinberg et. al. (2019[107]) article in Science has demonstrated how, despite an avalanche of attention and deep-dive into Russian disinformation operations during the 2016 US Election, disinformation (both Russian and indigenous) has accounted for only 6% of aggregate cumulative digital media consumption before, during and after the vote. Furthermore, it was only less than 1% of the American digital media audience that was exposed to 80% of the fake news disseminated around the

104 Anoosh Chakelian, "Facebook Releases Brexit Campaign Ads for the Fake News Inquiry – but What's Wrong with Them?," New Statesman America, July 27, 2018, https://www.newstatesman.com/politics/media/2018/07/facebook-releases-brexit-campaign-ads-fake-news-inquiry-what-s-wrong-them.

105 Thomas Brey, "Fake News and Alternative Facts Target EU's Core," Deutsche Welle, December 29, 2018, https://www.dw.com/en/opinion-fake-news-and-alternative-facts-target-eus-core/a-46889022.

106 Donie O'Sullivan, "Newly Released Facebook Ads Show Russian Trolls Targeted Mexican-Americans after Trump Election," CNNMoney, May 10, 2018, https://money.cnn.com/2018/05/10/technology/russian-facebook-ads-targeted-mexican-americans/index.html.

107 Nir Grinberg et al., "Fake News on Twitter during the 2016 U.S. Presidential Election," Science 363, no. 6425 (January 25, 2019): 374–78, https://doi.org/10.1126/science.aau2706.

election campaign period. That study is a good reminder of the necessity of contextualizing disinformation within the wider information sample and establish some degree of explanatory authority on the tangible and measurable effects of digital propaganda. The impromptu Twitter debate[108] between Gary King and other prominent disinformation researchers is highly instructive in this context.

Ultimately, it is possible to argue with a great degree of certainty that Russia has so far did not follow the same kind of information strategy in Turkish-language digital domain that it does in well-known cases in the West. This is a result of the convergence in security/strategic relations between Ankara and Moscow, and the heavy dose of pre-existing indigenous disinformation environment in Turkey raising the barriers of entry for external information meddling. This state of affairs, of course, is dependent on the continuation of converged strategic interests between the two sides, and shouldn't be interpreted as a structural explanation of why Russian information operations in Turkey are largely dormant.

[108] The link to the debate can be accessed here: https://twitter.com/kinggary/status/1079503260657041408

REFERENCES

"6 askere linç." *Hürriyet*, 07 2016. http://www.hurriyet.com.tr/gundem/6-askere-linc-40150768.

"15 Temmuz Şehidi Resul Kaptancı'nın Ailesi İdam İstiyor." *Milliyet*, March 5, 2017. http://www.milliyet.com.tr/15-temmuz-sehidi-resul-kaptanci-nin-ankara-yerelhaber-1884645/.

Aaronson, Michael, Sverre Diessen, Yves De Kermabon, Mary Beth Long, and Michael Miklaucic. "NATO Countering the Hybrid Threat." *PRISM* 2, no. 4 (2011): 111–24.

Abrams, Steve. "Beyond Propaganda: Soviet Active Measures in Putin's Russia." *Connections* 15, no. 1 (2016): 5–31.

Alkaya, Elvan. "Elvan Alkaya: FETÖ bağlantılı cinayetler ve şaibeli davalar (2)." *Yeni Şafak*, July 26, 2016. https://www.yenisafak.com/yazarlar/elvanalkaya/feto-baglantili-cinayetler-ve-aibeli-davalar-2-2030700.

Allcott, Hunt, and Matthew Gentzkow. "Social Media and Fake News in the 2016 Election." Working Paper. National Bureau of Economic Research, January 2017. https://doi.org/10.3386/w23089.

Bachmann, Sascha Dov, and Hakan Gunneriusson. "Russia's Hybrid Warfare in the East: The Integral Nature of the Information Sphere." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, October 7, 2015. https://papers.ssrn.com/abstract=2670527.

Balmas, Meital. "When Fake News Becomes Real: Combined Exposure to Multiple News Sources and Political Attitudes of Inefficacy, Alienation, and Cynicism." *Communication Research* 41, no. 3 (April 1, 2014): 430–54. https://doi.org/10.1177/0093650212453600.

"'Başı kesilen asker' haberine gelen yalanlama ve o haberin hikayesi." *Sözcü*, 07 2016. https://www.sozcu.com.tr/2016/gundem/basi-kesilen-asker-haberine-yalanlama-ve-o-haberin-hikayesi-1319809/.

Bennett, W. Lance, and Alexandra Segerberg. "Digital Media and the Personalization of Collective Action." *Information, Communication & Society* 14, no. 6 (September 1, 2011): 770–99. https://doi.org/10.1080/1369118X.2011.579141.

Bentzen, Naja. "Foreign Influence Operations in the EU - Think Tank." Brussels: European Parliament, 2018. http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282018%29625123.

Boffey, Daniel. "EU Raises Funds to Fight 'disinformation War' with Russia." *The Guardian*, December 5, 2018, sec. World news. https://www.theguardian.com/world/2018/dec/05/eu-disinformation-war-russia-fake-news.

Booth, Robert, Matthew Weaver, Alex Hern, Stacee Smith, and Shaun Walker. "Russia Used Hundreds of Fake Accounts to Tweet about Brexit, Data Shows." *The Guardian*, November 14, 2017, sec. World news. https://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets.

Botelho, Greg. "Russia, Turkey Trade Charges: Who Bought Oil from ISIS?" CNN, December 2, 2015. https://edition.cnn.com/2015/12/02/europe/syria-turkey-russia-warplane-tensions/index.html.

Bradshaw, Samantha, and Philip N. Howard. "The Global Organization of Social Media Disinformation Campaigns." *Journal of International Affairs* 71, no. 1.5 (2018): 23–32.

Brattberg, Erik, and Tim Maurer. "How Sweden Is Preparing for Russia to Hack Its Election," May 31, 2018, sec. World. https://www.bbc.com/news/world-44070469.

———. "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks." Washington DC: Carnegie Endowment for International Peace, May 23, 2018. https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

Breslow, Jason. "All The Criminal Charges To Emerge So Far From Robert Mueller's Investigation." *NPR.Org*, December 9, 2018. https://www.npr.org/2018/12/09/643444815/all-the-criminal-charges-to-emerge-so-far-from-robert-muellers-investigation.

Brey, Thomas. "Fake News and Alternative Facts Target EU's Core." *Deutsche Welle*, December 29, 2018. https://www.dw.com/en/opinion-fake-news-and-alternative-facts-target-eus-core/a-46889022.

Brooks-Pollock, Tom. "Russia Releases 'proof' Turkey Is Smuggling Isis Oil over Its Border." *The Independent*, December 2, 2015. http://www.independent.co.uk/news/world/europe/russia-releases-proof-turkey-is-smuggling-isis-oil-over-its-border-a6757651.html.

Carrel, Paul, and Andrea Shalal. "Germany Says Its Government Computers Secure after 'isolated' Hack." *Reuters*, February 28, 2018. https://www.reuters.com/article/us-germany-cyber-russia-idUSKCN1GC2HZ.

Chakelian, Anoosh. "Facebook Releases Brexit Campaign Ads for the Fake News Inquiry – but What's Wrong with Them?" *New Statesman America*, July 27, 2018. https://www.newstatesman.com/politics/media/2018/07/facebook-releases-brexit-campaign-ads-fake-news-inquiry-what-s-wrong-them.

Conley, Heather A., and Jean-Baptiste Jeangène Wilmer. "Successfully Countering Russian Electoral Interference." CSIS Briefs. Washington DC: Center for Strategic and International Studies, June 21, 2018. https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.

"Cumhurbaşkanı Erdoğan'ın Bursa mitingindeki kalabalığa 'Sakarya' diye seslendiği iddiası." *teyit.org* (blog), June 12, 2018. https://teyit.org/cumhurbaskani-erdoganin-bursa-mitingindeki-kalabaliga-sakarya-diye-seslendigi-iddiasi/.

Dahir, Abdi Latif. "Half the World's Population Used the Internet in 2018 - ITU — Quartz Africa." *Quartz*, December 11, 2018. https://qz.com/africa/1490997/more-than-half-of-worlds-population-using-the-internet-in-2018/.

Daniels, Laura. "How Russia Hacked the French Election." POLITICO, April 23, 2017. https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/.

"Darbe gecesi tavla partisindeymiş." *Sabah*, June 22, 2018. https://www.sabah.com.tr/gundem/2018/06/22/darbe-gecesi-tavla-partisindeymis.

"Digital in 2018: World's Internet Users Pass the 4 Billion Mark." We Are Social, January 30, 2018. https://wearesocial.com/blog/2018/01/global-digital-report-2018.

"Diyarbakır Mesut Yılmaz İlkokulu'nda boş zarflarla dolaşan kişiler kim?" *teyit.org* (blog), June 24, 2018. https://teyit.org/diyarbakir-mesut-yilmaz-ilkokulunda-bos-zarflarla-dolasan-kisiler-kim/.

Dorf, Michael C., and Sidney Tarrow. "Stings and Scams: 'Fake News,' the First Amendment, and the New Activist Journalism." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, January 26, 2017. https://papers.ssrn.com/abstract=2906444.

"Emniyet Müdürü: YSK'dan zarf talep etmiş." *HaberTurk*, June 24, 2018. https://www.haberturk.com/diyarbakir-da-muhurlu-bos-zarflarda-yanlis-anlasilma-2029291.

"Erdoğan: Suikastçı FETÖ'ye Mensup," December 21, 2016, sec. Türkiye. https://www.bbc.com/turkce/haberler-turkiye-38394837.

"Erdoğan'ın Meral Akşener hakkında 'Zilli Meral Kemal'in eteklisi' dediği iddiası." *teyit.org* (blog), May 7, 2018. https://teyit.org/erdoganin-meral-aksener-hakkinda-zilli-meral-kemalin-eteklisi-dedigi-iddiasi/.

Ferrara, Emilio, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini. "The Rise of Social Bots." *Communications ACM* 59, no. 7 (June 2016): 96–104. https://doi.org/10.1145/2818717.

Fiott, Daniel. "A Revolution Too Far? US Defence Innovation, Europe and NATO's Military-Technological Gap." *Journal of Strategic Studies* 40, no. 3 (April 16, 2017): 417–37. https://doi.org/10.1080/01402390.2016.1176565.

———. "Europe and the Pentagon's Third Offset Strategy." *The RUSI Journal* 161, no. 1 (January 2, 2016): 26–31. https://doi.org/10.1080/03071847.2016.1152118.

"Fotoğrafın Muharrem İnce'nin camide halay çektiğini gösterdiği iddiası." *teyit.org* (blog), May 9, 2018. https://teyit.org/fotografin-muharrem-incenin-camide-halay-cektigini-gosterdigi-iddiasi/.

Foy, Henry. "Valery Gerasimov, the General with a Doctrine for Russia." *Financial Times*, September 15, 2017. https://www.ft.com/content/7e14a438-989b-11e7-a652-cde3f882dd7b.

"German Cyber Defense Blends Military and Commerce." *Deutsche Welle*. 09 2018. https://www.dw.com/en/german-cyber-defense-blends-military-and-commerce/a-45636325.

Germano, Sara. "Facebook, Germany to Collaborate Against Election Interference." *Wall Street Journal*, January 20, 2019, sec. Business. https://www.wsj.com/articles/facebook-germany-to-collaborate-against-election-interference-11548004995.

Golovchenko, Yevgeniy, Mareike Hartmann, and Rebecca Adler-Nissen. "State, Media and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation." *International Affairs* 94, no. 5 (September 1, 2018): 975–94. https://doi.org/10.1093/ia/iiy148.

Grinberg, Nir, Kenneth Joseph, Lisa Friedland, Briony Swire-Thompson, and David Lazer. "Fake News on Twitter during the 2016 U.S. Presidential Election." *Science* 363, no. 6425 (January 25, 2019): 374–78. https://doi.org/10.1126/science.aau2706.

Groeling, Tim. "Media Bias by the Numbers: Challenges and Opportunities in the Empirical Study of Partisan News." *Annual Review of Political Science* 16, no. 1 (2013): 129–51. https://doi.org/10.1146/annurev-polisci-040811-115123.

Hern, Alex. "Macron Hackers Linked to Russian-Affiliated Group behind US Attack." *The Guardian*, May 8, 2017, sec. World news. https://www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack.

Hopkins, Daniel J., and Gary King. "A Method of Automated Nonparametric Content Analysis for Social Science." *American Journal of Political Science* 54, no. 1 (2010): 229–47. https://doi.org/10.1111/j.1540-5907.2009.00428.x.

Howard, Philip N., Aiden Duffy, Deen Freelon, Muzammil M. Hussain, Will Mari, and Marwa Maziad. "Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?" SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 2011. https://papers.ssrn.com/abstract=2595096.

Howard, Philip N., Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois. "The IRA and Political Polarization in the United States, 2012-2018." Computational Propaganda Research Project. Oxford, UK: Oxford Internet Institute, December 2018. https://comprop.oii.ox.ac.uk/research/ira-political-polarization/.

Howard, Philip N., and Bence Kollanyi. "Bots, #Strongerin, and #Brexit: Computational Propaganda During the UK-EU Referendum." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, June 20, 2016. https://papers.ssrn.com/abstract=2798311.

"İlham Aliyev'den FETÖ Darbe Girişimine Kınama." *TRT Haber*, 07 2016. https://www.trthaber.com/haber/dunya/ilham-aliyevden-feto-darbe-girisimine-kinama-261298.html.

Jensen, Michael. "Russian Trolls and Fake News: Information or Identity Logics?" *Journal of International Affairs* 71, no. 1.5 (2018): 115–24.

Jones, Marc Owen. "Hacking, Bots and Information Wars in the Qatar Spat." *Washington Post*. June 7, 2017. https://www.washingtonpost.com/news/monkey-cage/wp/2017/06/07/hacking-bots-and-information-wars-in-the-qatar-spat/.

"Karlov suikastı iddianamesi mahkemede." *NTV*, November 23, 2018. https://www.ntv.com.tr/turkiye/karlov-suikasti-iddianamesi-mahkemede,pG6pIihRcUaQQcbvWqgpEg.

"Karlov suikastı sanığı: Menzil tarikatına bağlıyım." *Sputnik Türkiye*, January 11, 2019. https://tr.sputniknews.com/turkiye/201901111037037495-karlov-suikasti-sanigi-menzil-tarikatini-bagliyim/.

"Karlov suikastını, eski adı El Nusra olan Fetih el Şam üstlendi." *Sputnik Türkiye*, December 21, 2016. https://tr.sputniknews.com/ortadogu/201612211026428039-karlov-fetih-el-sam/.

Kirchgaessner, Stephanie. "Russia Suspected over Hacking Attack on Italian Foreign Ministry." *The Guardian*, February 10, 2017, sec. World news. https://www.theguardian.com/world/2017/feb/10/russia-suspected-over-hacking-attack-on-italian-foreign-ministry.

Lanoszka, Alexander. "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe." *International Affairs* 92, no. 1 (January 1, 2016): 175–95. https://doi.org/10.1111/1468-2346.12509.

Lazer, David M. J., Matthew A. Baum, Yochai Benkler, Adam J. Berinsky, Kelly M. Greenhill, Filippo Menczer, Miriam J. Metzger, et al. "The Science of Fake News." *Science* 359, no. 6380 (March 9, 2018): 1094–96. https://doi.org/10.1126/science.aao2998.

Liu, Peng, Wei Chen, Gaoyan Ou, Tengjiao Wang, Dongqing Yang, and Kai Lei. "Sarcasm Detection in Social Media Based on Imbalanced Classification." In *Web-Age Information Management*, edited by Feifei Li, Guoliang Li, Seung-won Hwang, Bin Yao, and Zhenjie Zhang, 459–71. Lecture Notes in Computer Science. Springer International Publishing, 2014.

Lowen, Mark. "Hunting for Truth in a Land of Conspiracy." *BBC News*. November 15, 2018, sec. Europe. https://www.bbc.com/news/world-europe-46137139.

Matthews, Matt M. "We Were Caught Unprepared: The 2006 Hezbollah-Israeli War." Fort Leavenworth, Kansas: US Army Combined Arms Center, 2007. https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/we-were-caught-unprepared.pdf.

Mayer, Jane. "How Russia Helped Swing the Election for Trump." *The New Yorker*, September 24, 2018. https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump.

McCallum, A., X. Wei, and X. Wang. "Topical N-Grams: Phrase and Topic Discovery, with an Application to Information Retrieval." In *Seventh IEEE International Conference on Data Mining (ICDM 2007)(ICDM)*, 697–702, 2007. https://doi.org/10.1109/ICDM.2007.86.

"Measuring the Information Society Report 2018." International Telecommunications Union, 2018. https://www.itu.int/en/ITU-D/Statistics/Pages/publications/misr2018.aspx.

Mora, Edwin. "Report: Turkey, Syria Helped Keep Islamic State Alive by Buying Their Oil." Breitbart, July 3, 2018. https://www.breitbart.com/national-security/2018/07/03/report-turkey-syria-helped-keep-islamic-state-alive-by-buying-their-oil/.

"Oil Smuggled into Turkey Not Enough to Be Profitable: U.S. Official." *Reuters*, December 4, 2015. https://www.reuters.com/article/us-syria-oil-usa-idUSKBN0TN2P920151204.

Osnos, Evan, David Remnick, and Joshua Yaffa. "Trump, Putin, and the New Cold War," February 24, 2017. https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war.

O'Sullivan, Donie. "Newly Released Facebook Ads Show Russian Trolls Targeted Mexican-Americans after Trump Election." *CNNMoney*, May 10, 2018. https://money.cnn.com/2018/05/10/technology/russian-facebook-ads-targeted-mexican-americans/index.html.

Polyakova, Alina. "Strange Bedfellows: Putin and Europe's Far Right." *World Affairs* 177, no. 3 (2014): 36–40.

Pomerantsev, Peter. "Authoritarianism Goes Global (II): The Kremlin's Information War." *Journal of Democracy* 26, no. 4 (October 19, 2015): 40–50. https://doi.org/10.1353/jod.2015.0074.

Radcliffe, Damian. "How Local Journalism Can Upend the 'fake News' Narrative." The Conversation, November 27, 2018. http://theconversation.com/how-local-journalism-can-upend-the-fake-news-narrative-104630.

Renz, Bettina. "Russia and 'Hybrid Warfare.'" *Contemporary Politics* 22, no. 3 (July 2, 2016): 283–300. https://doi.org/10.1080/13569775.2016.1201316.

"Reuters Institute Digital News Report." Oxford, UK: Reuters Institute, Oxford University, 2018. http://www.digitalnewsreport.org/.

Rid, Thomas. Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Pub. L. No. 033017, § Select Committee on Intelligence (2017).

Rohde, Markus, Konstantin Aal, Kaoru Misaki, Dave Randall, Anne Weibert, and Volker Wulf. "Out of Syria: Mobile Media in Use at the Time of Civil War." *International Journal of Human–Computer Interaction* 32, no. 7 (July 2, 2016): 515–31. https://doi.org/10.1080/10447318.2016.1177300.

"Rus Savaş Uçağının Fetö Tarafıdan Düşürüldüğü İddiası." *Milliyet*, October 7, 2017. http://www.milliyet.com.tr/rus-savas-ucaginin-feto-tarafidan-dusuruldugu-sivas-yerelhaber-2323116/.

"Russia Presents Proof of Turkey's Role in ISIS Oil Trade." *RT International*. December 2, 2015. https://www.rt.com/news/324263-russia-briefing-isis-funding/.

Safarov, Fuad. “Rus uzman, Rus uçağını düşürme emrini kimin verdiğini açıkladı.” *Sputnik Türkiye*, 12 2016. https://tr.sputniknews.com/rusya/201612041026128807-rus-uzman-gulen-ucak/.

Saka, Erkan. “Social Media in Turkey as a Space for Political Battles: AKTrolls and Other Politically Motivated Trolling.” *Middle East Critique* 27, no. 2 (April 3, 2018): 161–77. https://doi.org/10.1080/19436149.2018.1439271.

Sanger, David E., and Charlie Savage. “U.S. Says Russia Directed Hacks to Influence Elections.” *The New York Times*, December 21, 2017, sec. U.S. https://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html.

Saxena, Akrati, Ralucca Gera, and S. R. S. Iyengar. “A Faster Method to Estimate Closeness Centrality Ranking.” *ArXiv:1706.02083 [Physics]*, June 7, 2017. http://arxiv.org/abs/1706.02083.

Schwirtz, Michael. “German Election Mystery: Why No Russian Meddling?” *The New York Times*, January 20, 2018, sec. World. https://www.nytimes.com/2017/09/21/world/europe/german-election-russia.html.

Segerberg, Alexandra, and W. Lance Bennett. “Social Media and the Organization of Collective Action: Using Twitter to Explore the Ecologies of Two Climate Change Protests.” *The Communication Review* 14, no. 3 (July 1, 2011): 197–215. https://doi.org/10.1080/10714421.2011.597250.

“Şeytan taşladı.” *Takvim*, 08 2016. https://www.takvim.com.tr/guncel/2016/08/16/seytan-tasladi.

Shane, Scott. “Five Takeaways From New Reports on Russia’s Social Media Operations.” *The New York Times*, December 18, 2018, sec. U.S. https://www.nytimes.com/2018/12/17/us/politics/takeaways-russia-social-media-operations.html.

Simón, Luis. “The ‘Third’ US Offset Strategy and Europe’s ‘Anti-Access’ Challenge.” *Journal of Strategic Studies* 39, no. 3 (April 15, 2016): 417–45. https://doi.org/10.1080/01402390.2016.1163260.

Snyder, Michael. “Obama Knows That Turkey Is Buying Oil From ISIS And He Isn’t Doing Anything To Stop It.” *InfoWars* (blog), November 28, 2015. https://www.infowars.com/obama-knows-that-turkey-is-buying-oil-from-isis-and-he-isnt-doing-anything-to-stop-it/.

Somaskanda, Sumi. “The Cyber Threat To Germany’s Elections Is Very Real.” *The Atlantic*, September 20, 2017. https://www.theatlantic.com/international/archive/2017/09/germany-merkel-putin-elections-cyber-hacking/540162/.

“Son dakika: YSK, 2018 kesin seçim sonuçlarını açıkladı.” *Hürriyet*, July 4, 2018. http://www.hurriyet.com.tr/gundem/son-dakika-ysk-2018-kesin-secim-sonuclarini-acikladi-40886560.

Spohr, Dominic. “Fake News and Ideological Polarization: Filter Bubbles and Selective Exposure on Social Media.” *Business Information Review* 34, no. 3 (September 1, 2017): 150–60. https://doi.org/10.1177/0266382117722446.

Stelzenmüller, Constanze. “The Impact of Russian Interference on Germany’s 2017 Elections.” *Brookings* (blog), June 28, 2017. https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

Stukal, Denis, Sergey Sanovich, Richard Bonneau, and Joshua A. Tucker. “Detecting Bots on Russian Political Twitter.” *Big Data* 5, no. 4 (December 1, 2017): 310–24. https://doi.org/10.1089/big.2017.0038.

Tandoc Jr, Edson C., Zheng Wei Lim, and Richard Ling. "Defining 'Fake News.'" *Digital Journalism* 6, no. 2 (February 7, 2018): 137–53. https://doi.org/10.1080/21670811.2017.1360143.

Taub, Ben. "The ISIS Oil Trade, from the Ground Up," December 4, 2015. https://www.newyorker.com/news/news-desk/the-isis-oil-trade-from-the-ground-up.

"Text of Newly-Approved Russian Military Doctrine." Carnegie Endowment for International Peace, February 5, 2010. https://carnegieendowment.org/2010/02/05/text-of-newly-approved-russian-military-doctrine-pub-40266.

"The 'Lisa Case': Germany as a Target of Russian Disinformation." NATO, 2016. http://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm.

Thieltges, Andree, Orestis Papakyriakopoulos, Juan Carlos Medina Serrano, and Simon Hegelich. "Effects of Social Bots in the Iran-Debate on Twitter." *ArXiv:1805.10105 [Cs]*, May 25, 2018. http://arxiv.org/abs/1805.10105.

Thomas, Timothy. "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations." Riga: NATO STRATCOM, 2015. https://www.stratcomcoe.org/timothy-thomas-russias-21st-century-information-war-working-undermine-and-destabilize-populations.

Tsvetkova, Maria, and Lidia Kelly. "Russia Says It Has Proof Turkey Involved in Islamic State Oil Trade." *Reuters*, December 2, 2015. https://www.reuters.com/article/us-mideast-crisis-russia-turkey-idUSKBN0TL19S20151202.

"Turkey Confirms Cancellation of $3.4 Billion Missile Defence..." *Reuters*, November 18, 2015. https://www.reuters.com/article/us-turkey-china-missile-idUSKCN0T61OV20151118.

"UK Political Parties Warned of Russian Hacking Threat: Report." *Reuters*, March 12, 2017. https://www.reuters.com/article/us-britain-russia-cybercrime-idUSKBN16J0OE.

Visentin, Marco, Gabriele Pizzi, and Marco Pichierri. "Fake News, Real Problems for Brands: The Impact of Content Truthfulness and Source Credibility on Consumers' Behavioral Intentions toward the Advertised Brands." *Journal of Interactive Marketing* 45 (February 1, 2019): 99–112. https://doi.org/10.1016/j.intmar.2018.09.001.

"Voter Turnout in Turkey Elections Was 87 Percent: State Broadcaster." *Reuters*, June 24, 2018. https://www.reuters.com/article/us-turkey-election-turnout-idUSKBN1JK0SP.

Wagnsson, Charlotte, and Maria Hellman. "Normative Power Europe Caving In? EU under Pressure of Russian Information Warfare." *JCMS: Journal of Common Market Studies* 56, no. 5 (2018): 1161–77. https://doi.org/10.1111/jcms.12726.

Wang, Alex Hai. "Detecting Spam Bots in Online Social Networking Sites: A Machine Learning Approach." In *Data and Applications Security and Privacy XXIV*, edited by Sara Foresti and Sushil Jajodia, 335–42. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2010.

Wasserman, Herman. "Fake News from Africa: Panics, Politics and Paradigms." *Journalism*, December 17, 2017, 1464884917746861. https://doi.org/10.1177/1464884917746861.

Way, Lucan A. "The Limits of Autocracy Promotion: The Case of Russia in the 'near Abroad.'" *European Journal of Political Research* 54, no. 4 (2015): 691–706. https://doi.org/10.1111/1475-6765.12092.

Williams, Oscar. "Russia Is Targeting UK Infrastructure through Supply Chains, NCSC Warns." *New Statesman*, April 6, 2018. https://tech.newstatesman.com/business/russia-uk-critical-infrastructure.

Wintour, Patrick. "Russian Bid to Influence Brexit Vote Detailed in New US Senate Report." *The Guardian*, January 10, 2018, sec. World news. https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report.

Wintour, Patrick, and Andrew Roth. "Russia Summons Dutch Ambassador over Hacking Revelations." *The Guardian*, October 8, 2018, sec. World news. https://www.theguardian.com/world/2018/oct/08/russia-summons-dutch-ambassador-over-hacking-revelations.

Yinanç, Barçın. "Poor Media Literacy 'Making Turks Vulnerable to Fake News' - Turkey News." *Hürriyet Daily News*. December 10, 2018. http://www.hurriyetdailynews.com/poor-media-literacy-making-turks-vulnerable-to-fake-news-139582.

Yılmaz, Mehmet Y. "Davutoğlu bıçağın sırtında." *Hürriyet*, July 19, 2016. http://www.hurriyet.com.tr/yazarlar/mehmet-y-yilmaz/davutoglu-bicagin-sirtinda-40154956.

Yourish, Karen, and Troy Griggs. "8 U.S. Intelligence Groups Blame Russia for Meddling, but Trump Keeps Clouding the Picture." *The New York Times*, July 16, 2018, sec. U.S. https://www.nytimes.com/interactive/2018/07/16/us/elections/russian-interference-statements-comments. html, https://www.nytimes.com/interactive/2018/07/16/us/elections/russian-interference-statements-comments.html.

Zannettou, Savvas, Tristan Caulfield, Emiliano De Cristofaro, Michael Sirivianos, Gianluca Stringhini, and Jeremy Blackburn. "Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web." *ArXiv:1801.09288 [Cs]*, January 28, 2018. http://arxiv.org/abs/1801.09288.

Centre for Economics and Foreign Policy Studies

Cyber Governance and Digital Democracy 2019/1

March 2019

Russian Digital Media and Information Ecosystem in Turkey

H. Akın Ünver | EDAM, Oxford CTGA & Kadir Has University