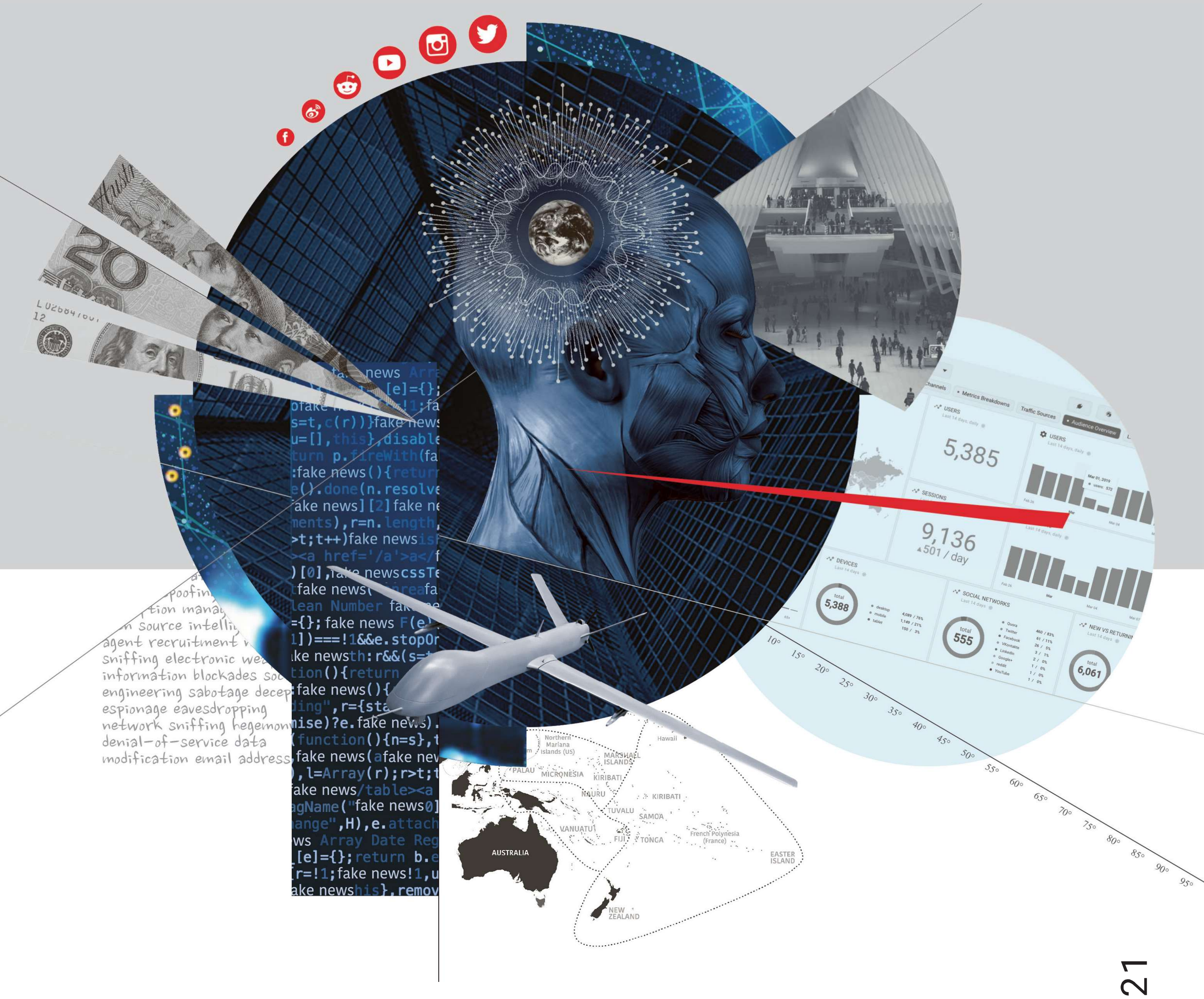
Understanding Mass Influence

A case study of the Internet Research Agency as a contemporary mass influence operation



JULY 2021

Produced for the Department of Defence by: The University of Melbourne in collaboration with
The University of Adelaide, University of New South Wales, Edith Cowan University and Macquarie University

This project report is jointly submitted by the parties set out below as part of a Standard Collaborative Project pursuant to Defence Science Partnering Multi-Party Collaborative Project Agreement (Agreement No. MyIP10379) dated 11 February 2021. The ownership and use of Intellectual Property subsisting in the Report is subject to the terms of that Agreement.

The University of Melbourne
Edith Cowan University
Macquarie University
The University of Adelaide
University of New South Wales

Any comments or queries regarding the project report should be directed to:
Melbourne Defence Enterprise
Melbourne Connect, Level 8, 700 Swanston Street, Carlton, VIC 3053
defence-technologies@unimelb.edu.au
https://eng.unimelb.edu.au/industry/defence

Authors:
Dr Morgan Saletta, The University of Melbourne
Mr Richard Stearne, The University of Melbourne
Ms Emily Ebbott, The University of Melbourne

Text design Raye Antonelli, The Friday Collective
Typesetting by Ms Emily Ebbott, The University of Melbourne
Cover design by Raye Antonelli, The Friday Collective
Cover image by Naomi Cain, The University of Adelaide

AUTHORS AND CONTRIBUTORS

Program Leader and Contributor

The University of Melbourne
Ms Emily Ebbott

Authors and Researchers

The University of Melbourne
Dr Morgan Saletta
Richard Stearne

Contributors

Defence Science and Technology Group
Ms Mirela Stjelja

The University of Melbourne
Professor Christopher Leckie
Associate Professor Atif Ahmad
Associate Professor Andrew Perfors
Associate Professor Richard de Rozario
Professor Len Sciacca
Dr Jey Han Lau
Professor Shanika Karunasekera
Professor Yoshi Kashima
Associate Professor Leah Ruppanner
Associate Professor Tim van Gelder

Edith Cowan University
Dr Andrew Dowse
Dr Violetta Wilk

The University of Adelaide
Associate Professor Tim Legrand
Professor Melissa de Zwart
Professor Dale Stephens
Professor Debi Ashenden
Professor Michael Webb

University of New South Wales
Professor Monica Whitty

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Internet Research Agency (IRA) was a private enterprise that carried out influence operations on behalf of the Russian Government between 2013 and 2018. The University of Melbourne (UoM) was tasked to deliver a case study of the IRA and respond to four primary themes and research questions.

The four themes and questions were:

- **Governance and Ethics:** What was the IRA's business model for operations, including its operating concept, financing arrangements, governance, and legal and ethical framework?
- **Persuasive Technology and Techniques:** How did the IRA use technology and techniques to persuade its target audiences?
- **Systems and Technology:** What were the foundational systems, technology and workforce skills required for IRA's operation?
- **Campaign Awareness and Sensemaking:** How was the IRA able to achieve and maintain awareness of the impact of its influence activities?

To answer these questions the UoM's research team:

- Carried out a systematic literature review.
- Elicited expert knowledge from a multidisciplinary team of senior academics from multiple institutions through an iterative consultation process.
- Synthesised the findings from the literature review and elicitation process into the findings and recommendations of this report.

KEY FINDINGS

- The Russian IRA was a private entity that operated with direct approval and endorsement from Russian President Vladimir Putin.
- There were two key benefits to acting as a private entity: (a) plausible deniability for the Russian Government in relation to its support and involvement, and (b) creative license for the business.
- The IRA was funded by Russian businessman Yevgeny Prigozhin and operated ostensibly as a digital marketing firm, complete with a corporate hierarchy and all the usual business units.
- The IRA had approximately 400-600 staff at any one time and 800-1000 employees over the life of the operation. Staff worked in specialist departments according to their skills.
- The IRA operated 24/7, enabling real-time, time zone-specific content creation and engagement, among other things.
- The IRA's overarching objective was to sow discord and division in nations that were not aligned with Russia's geo-politics, and to undermine confidence in democratic institutions, such as electoral systems. The modus operandi was, predominantly, to amplify existing divisions within societies.
- Bot technology gave the IRA an important force multiplier with the power to direct messaging and content to target audiences easily, quickly and relatively cheaply.
- The IRA operated within Russia's broader disinformation and propaganda ecosystem, leveraging an extensive base of expertise and experience, and the resources of Russia's intelligence community.
- The IRA differed from other Russian influence operations in using social media platforms to reach and engage audiences. Functions native to social media, such as behavioural data tracking, gave the IRA the ability to target a specific audience.

- IRA’s influence operations troops had cultural/linguistic skills and were social media literate. They were familiar with the Internet and online subcultures, which meant they could interact with diverse groups.
- IRA’s influence operations were characterised by their multi-platform, high volume, high-speed messaging and content production and dissemination, or ‘firehose strategy’.
- Transforming online behaviour and beliefs to action in the real world was a key performance metric for IRA operators. Provoking offline violence between online groups was a measure of success.
- IRA influence campaigns were designed to inflame racial and ethnic tensions in the United States (US) and Europe, contravening international treaties to which Russia is signatory.

RECOMMENDATIONS

- Establish an ethical framework for information operations that aligns with Australia’s democratic values, Government policy and international law, with flexibility to adapt in a rapidly evolving threat environment.
- Establish an information operations ecosystem including Defence, intelligence, and non-government expertise.
- Consider off-the-shelf, third party and/or native online tools/capabilities to monitor activity on social media, including tools that identify vulnerable individuals and groups, and regions relevant to Australia’s national interest.
- Survey and develop more advanced methods for sensemaking and campaign awareness, and for assessing the relationship between online and offline behaviour.
- Ensure the cultural/linguistic, cognitive (e.g., critical thinking) and creative (e.g., digital marketing) skills required to avert and conduct influence operations are trained/recruited for.
- Experiment with organisational structures and processes that provide agility (speed, flexibility, innovation) in the information environment.
- Where possible and appropriate, work with Australia’s Five Eyes partners (and other allies) to develop information operations capabilities and principles.
- Engage with our Indo-Pacific partners to increase resilience to malign or hostile information operations and to boost, where possible and appropriate, local capabilities.

BACKGROUND

The IRA was a proxy for the Russian Government. According to US intelligence, it conducted influence operations with the approval of Russian President Putin.[1] Its status as a private business gave the Government plausible deniability in relation to the activities of IRA operatives. It was funded by Yevgeny Prigozhin[2], an oligarch closely associated with Putin and Russian intelligence. And while it appears Prigozhin met regularly with IRA's senior management and gave them direction, they took great pains to disguise the source and purpose of his funding.[3] Known as a "troll farm", the IRA was, in essence, a covert private military company serving the Russian Government's domestic and geopolitical goals. Unlike most private military companies, however, the IRA operated primarily in the information environment. It's focus – in its own words – was "information warfare", and it conducted its business undercover as a corporate entity providing digital marketing services.[4] This business model gave the IRA the ability to evolve and improve its methods in an agile, adaptive manner as it weaponised social media. It did this largely by taking advantage of the opportunities created by social media and its underlying business model. This model, adopted by different platforms, generates revenue from targeted advertising via the collection and sale of vast quantities of users' personal data.

Social media helped the IRA carry out highly sophisticated, large-scale operations. The following statistics reveal the unprecedented scale of these operations. Between 2014 and 2017, it is estimated the IRA engaged at least:[5]

- 126 million Americans on Facebook (using at least 470 pages and accounts). The IRA's most popular Facebook page, Being Patriotic, received 6,431,507 likes and was shared 4,429,880 times.[6]
- 20 million users on Instagram.
- 1.4 million users on Twitter.
- And uploaded more than 1000 videos to YouTube.

The scale of its US operations was remarkable, given it began as a relatively small unit in July 2013, focusing primarily on domestic Russian audiences. This suggests that the IRA was able to experiment, adapt and evolve its tactics and techniques, and access the resources and workforce to transition from a small, domestic operation to an organisation with global reach.

Despite the scale and reach of the IRA's campaigns debate continues about their level of influence.[7] This is due largely to the difficulty in measuring and assessing influence campaigns (discussed in **Campaign Awareness and Sensemaking**.) The IRA had multiple long-term, short-term, strategic and tactical goals relating to its influence operations, and it appears these goals were flexible. This meant the IRA could easily adapt its messaging and

[1] "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections" (Office of the Director of National Intelligence, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[2] Prigozhin also funds and controls various media outlets that form part of Russia's propaganda ecosystem, and he also helps fund and operate the Wagner Group, whose mercenaries operate as proxies for the Russian government in the physical, kinetic environment.

[3] "U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-Cr-32)," February 16, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.

[4] "U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-Cr-32)."

[5] Renee DiResta et al., "The Tactics & Tropes of the Internet Research Agency," 2019, https://digitalcommons.unl.edu/senatedocs/2.

[6] Howard, Philip N, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François. "The IRA, Social Media and Political Polarization in the United States, 2012-2018," 2019.

[7] Christopher A. Bail et al., "Assessing the Russian Internet Research Agency's Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017," *Proceedings of the National Academy of Sciences* 117, no. 1 (January 7, 2020): 243–50, https://doi.org/10.1073/pnas.1906420116.

content to rapidly evolving situations. For example, when it appeared likely presidential candidate Hillary Clinton would win the US election, the IRA put effort into messaging that was designed to undermine her.[8] However, questions such as, 'Did the IRA campaign convince x number of people to vote for Donald Trump?', while important, cloud the bigger picture; the IRA's main goal, it seems, was to sow doubt, amplify existing social divisions and weaken the US (and its allies) as part of a long-term strategy. There is every indication that Putin and the Kremlin, building on Soviet methods of the past, are playing a long game, and the IRA was part of a larger influence and propaganda ecosystem, established to conduct Russia's information and hybrid warfare more broadly.

Historians and social scientists will likely assess the impact of the IRA's influence campaigns against different metrics and indicators into the future. Nevertheless, the campaign targeting the US political system prompted the US Central Intelligence Agency (CIA), National Security Agency (NSA) and Federal Bureau of Investigation (FBI) to say: "Russian intelligence services would have seen their election influence campaign as at least a qualified success because of their perceived ability to impact public discussion".[9] James Clapper, former US director of national security, was even stronger in his testimony to the US Senate, stating:

> *"Russia's influence activities in the run-up to the 2016 election constituted the high-water mark of their long running efforts since the 1960s to disrupt and influence our elections. They must be congratulating themselves for having exceeded their wildest expectations with a minimal expenditure of resource. And I believe they are now emboldened to continue such activities in the future both here and around the world, and to do so even more intensely. If there has ever been a clarion call for vigilance and action against a threat to the very foundation of our democratic political system, this episode is it."*[10]

As stated, the IRA formed part of an influence and propaganda ecosystem comprising bodies and systems controlled directly or indirectly by the Russian Government. These range from official, overt, state-run media to plausibly deniable, proxy outfits and covert influence operations (such as hack and release operations). They are run – directly or indirectly – by Russian intelligence organisations, including the Main Intelligence Directorate (GRU) and the Federal Security Service (FSB).[11] The influence operation targeting the US political system and 2016 Presidential election had three parts – (i) the hacking of US voter registration systems, (ii) the hack and release of documents from the Democratic National Committee (DNC), (iii) the efforts to sow doubt and discord, amplify wedge issues, suppress electoral participation, and promote candidate Trump and denigrate Clinton.[12] IRA messaging was coordinated with these efforts and promoted messaging related to the hacked DNC emails. The same thing occurred during the 2017 French elections with Emmanuel Macron's hacked and released emails, also attributed to Russian intelligence services[13]. However, it is unclear whether there were any direct connections between the IRA and Russian intelligence, though this is possible. Generally, however, at the

[8] "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections" (Office of the Director of National Intelligence, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[9] "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections" (Office of the Director of National Intelligence, 2017), p. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[10] "Full Transcript: Sally Yates and James Clapper Testify on Russian Election Interference," *Washington Post*, accessed June 3, 2021, https://www.washingtonpost.com/news/post-politics/wp/2017/05/08/full-transcript-sally-yates-and-james-clapper-testify-on-russian-election-interference/.

[11] "Pillars of Russia's Disinformation and Propaganda Ecosystem" (U.S. Department of State Global Engagement Center, 2020).

[12] Snegovaya and Watanabe.

[13] Emilio Ferrara, "Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election," *First Monday*, July 31, 2017, https://doi.org/10.5210/fm.v22i8.8005.

operational and tactical level, Russian influence campaigns are decentralised in terms of their governance, with messaging guided by a "… sense of the Kremlin's desires rather than any master plan".[14]

While the IRA was essentially a private military company dedicated to influence operations, it presented as a digital marketing firm. It used digital marketing methods to maximise the opportunities provided by the advertising and revenue-raising business models of social media. Harvesting user data to build profiles to sell to businesses for targeted advertising is one example. The IRA used this to wage influence operations on a target audience as opposed to selling an audience a business or product.

While innovative, and revolutionary in their way, the scale and sophistication of the IRA's malign online campaigns owed a lot to an influence system that has been through multiple evolutions. Firstly, they were an evolution and adaptation of the Soviet era, 'active measures' playbook.[15] Secondly, the IRA grew out of the Russian Government's existing online influence activities. Russia began experimenting with – and developing – the capability to influence domestic political audiences via social media in the mid-2000s.[16]

The IRA started as a relatively small operation as part of these efforts in 2013. Based in a small mansion in the Olgino district of St Petersburg, it tended to target Russian audiences with pro-Putin messaging and messaging "slandering (Russian anti-corruption activist Alexei) Navalny".[17] These operations were exposed by individuals, journalists who infiltrated the operations and job advertisements posted online. The organisation grew from this to a company listed on the Russian Government's registry of businesses.[19]

In 2014 the IRA deployed its influence operations in the Ukraine to target international opinion around Russia's annexation of Crimea, and the downing of MH17. Regionally focused operations such as this were a turning point for the IRA. Russia's Government appears to have given the IRA the go ahead to deploy influence campaigns against Western governments, its institutions and citizens. The precise date is unknown but the IRA moved to larger premises at 55 Savushkina St, St Petersburg the same year.

The 2014 Columbian Chemicals plant explosion hoax was one of the first IRA operations in the US. IRA tweets, text messages and YouTube videos falsely claimed there had been a dangerous explosion at a chemical plant in Centerville, Louisiana. Later that year, many of the same Twitter accounts were linked to a minor Ebola outbreak panic in Atlanta, Georgia.[18]

By 2016, the IRA was deploying between 400 and 1000 hired civilian 'trolls' as proxy influence operations 'foot soldiers' to post online comments, tweets, blog posts and other content. They created websites and cultivated

[14] Maria Snegovaya and Kohei Watanabe, "The Kremlin's Social Media Influence Inside the United States: A Moving Target | Free Russia Foundation" (Free Russia Foundation, 2021), https://www.4freerussia.org/the-kremlin-s-social-media-influence-inside-the-united-states-a-moving-target/.

[15] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare.*, 2020; "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections."

[16] Ethan Guge, "Targeted Disinformation Warfare: How and Why Foreign Efforts Are Effective, and Recommendations for Impactful Government Action" (2020); Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections." Office of the Director of National Intelligence, 2017.

[17] "'How Our Politics Is Done' - (VKontakte Wall Post about Interview at Early Version of Internet Research Agency)," VK, accessed February 11, 2021, https://vk.com/wall-56388599_313.

[18] Adrian Chen, "The Agency," *The New York Times*, June 2, 2015, sec. Magazine, https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

followers, audiences and potential 'assets' using false, online sock puppet personas (online identity used for the purposes of propagating false information).[19]

IRA tactics listed here, and explored in later sections, point to its modus operandi:

- Create fake social media accounts - Reddit, Facebook, Instagram, and other social media platforms.
- Gain credibility and grow audience with targeted messaging, including 'feelgood' content to draw audiences in.
- Use advertising tools created by Facebook, Google, among others, to target audiences with paid advertisements.
- Promote selected 'like-minded' accounts on fake accounts.
- Promote/amplify selected messaging/content and accounts with bots.

TIMELINE

Between 2014 and 2018, the IRA used this modus operandi in influence operations against a range of Western audiences, and in the context of different political and geopolitical events, including:

2014-2018 US audiences and political system including the 2016 Presidential elections. Goals included creating social discord, inflaming racial issues, promoting candidate Trump, and denigrating candidate Clinton.

2015 Greek audiences targeted with anti-European Union (EU) messaging. IRA-linked accounts push messaging suggesting Greece should leave the EU.[20]

2015-2017 US and Western audiences targeted with messaging that is pro-Bashar al-Assad, anti-US and pro-Russian intervention in Syria.[21]

2016 United Kingdom (UK) EU membership referendum ("Brexit"). IRA-linked accounts worked to inflame anti-Islamic sentiment as part of a pro-Brexit campaign. IRA Twitter accounts widely cited by the UK media (>80 times).[22]

2016 Dutch referendum on EU trade deal with the Ukraine, 2016. IRA created and spread a video purporting to be an official statement by Ukraine's infamous right-wing Azov Battalion and threatening terror attacks in the Netherlands if the deal was rejected.[23]

2017 German federal elections. IRA-linked accounts targeted both ends of the political spectrum and sought to inflame political divisions. This appears to have been coordinated with activities targeting the right wing by RT

[19] Tim Lister, Jim Sciutto and Mary Ilyushina, "Putin's 'chef,' the Man behind the Troll Factory," CNN, accessed June 10, 2021, https://www.cnn.com/2017/10/17/politics/russian-oligarch-putin-chef-troll-factory/index.html; "U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-Cr-32)," February 16, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.

[20] "The Internet Research Agency In Europe 2014-2016.Pdf" (Cardiff University Crime and Security Research Institute, 2019), https://static1.squarespace.com/static/57875c16197aea2902e3820e/t/5cd14804104c7bb3cafeaa06/1557219339758/The+Internet+Research+Agency+In+Europe+2014-2016.pdf.

[21] DiResta et al., "The Tactics & Tropes of the Internet Research Agency."

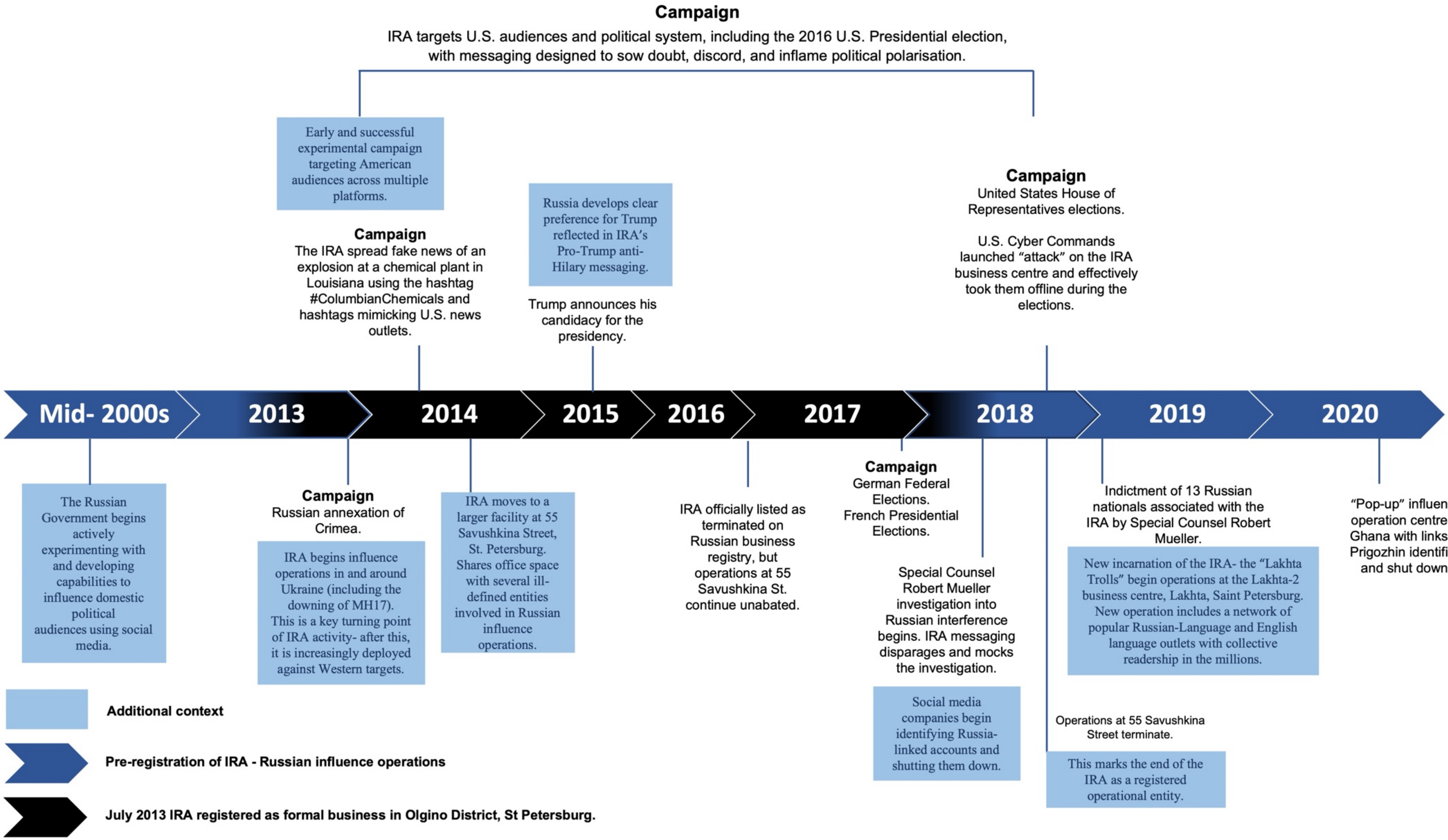
[22] "The St. Petersburg Troll Factory Targets Elections from Germany to the United States - EU vs Disinformation," EU vs Disinformation, 2019, https://euvsdisinfo.eu/the-st-petersburg-troll-factory-targets-elections-from-germany-to-the-united-states/.

[23] bellingcat. "Behind the Dutch Terror Threat Video: The St. Petersburg 'Troll Factory' Connection," April 3, 2016. https://www.bellingcat.com/news/uk-and-europe/2016/04/03/azov-video/.

and Sputnik, including the promotion of the "Lisa Case" (later debunked) of a young Russian/German girl raped by immigrants. This story was also mentioned at least twice by Russian foreign minister Sergey Lavrov.[24]
2017 French Presidential elections. IRA repurposed Twitter bots previously used to target US audiences. These were involved in messaging relating to the hacked and released emails of President Macron (an operation attributed to the GRU).[25]

[24] Jeffrey Mankoff, "Russian Influence Operations in Germany and Their Effect," 2020, https://www.csis.org/analysis/russian-influence-operations-germany-and-their-effect.

[25] Emilio Ferrara, "Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election," *First Monday*, July 31, 2017, https://doi.org/10.5210/fm.v22i8.8005; Amaelle Guiton, "«MacronLeaks» : de nouveaux éléments accréditent la piste russe," Libération, accessed May 16, 2021, https://www.liberation.fr/france/2019/12/08/macronleaks-de-nouveaux-elements-accreditent-la-piste-russe_1767982/.



Campaign
IRA targets U.S. audiences and political system, including the 2016 U.S. Presidential election, with messaging designed to sow doubt, discord, and inflame political polarisation.

The Russian Government begins actively experimenting with and developing capabilities to influence domestic political audiences using social media.

Campaign
Russian annexation of Crimea.

IRA begins influence operations in and around Ukraine (including the downing of MH17). This is a key turning point of IRA activity- after this, it is increasingly deployed against Western targets.

Early and successful experimental campaign targeting American audiences across multiple platforms.

Campaign
The IRA spread fake news of an explosion at a chemical plant in Louisiana using the hashtag #ColumbianChemicals and hashtags mimicking U.S. news outlets.

IRA moves to a larger facility at 55 Savushkina Street, St. Petersburg. Shares office space with several ill-defined entities involved in Russian influence operations.

Russia develops clear preference for Trump reflected in IRA's Pro-Trump anti-Hilary messaging.

Trump announces his candidacy for the presidency.

IRA officially listed as terminated on Russian business registry, but operations at 55 Savushkina St. continue unabated.

Campaign
German Federal Elections.
French Presidential Elections.

Special Counsel Robert Mueller investigation into Russian interference begins. IRA messaging disparages and mocks the investigation.

Social media companies begin identifying Russia-linked accounts and shutting them down.

Campaign
United States House of Representatives elections.

U.S. Cyber Commands launched "attack" on the IRA business centre and effectively took them offline during the elections.

Operations at 55 Savushkina Street terminate.

This marks the end of the IRA as a registered operational entity.

Indictment of 13 Russian nationals associated with the IRA by Special Counsel Robert Mueller.

New incarnation of the IRA- the "Lakhta Trolls" begin operations at the Lakhta-2 business centre, Lakhta, Saint Petersburg. New operation includes a network of popular Russian-Language and English language outlets with collective readership in the millions.

"Pop-up" influence operation centre in Ghana with links to Prigozhin identified and shut down.

🟦 **Additional context**

Pre-registration of IRA - Russian influence operations

July 2013 IRA registered as formal business in Olgino District, St Petersburg.

Figure 1: Internet Research Agency Timeline (Prepared by Jemma Smith, Emily Ebbott, Richard Stearne and Dr Morgan Saletta)

The scale and scope of these operations (especially in the US) drew a great deal of attention from investigative journalists, intelligence organisations, law enforcement agencies, militaries, politicians and social media platforms. The IRA's plausible deniability was called into question and it became clear it was a proxy for the Russian Government.

However, while the impact(s) of IRA influence campaigns are subject to continuing debate, its influence operations, particularly against the US political system and 2016 Presidential elections, were considered a success by Putin.[26] It is, therefore, unsurprising that Prigozhin – and others formerly associated with the IRA – have been associated with multiple clones and pop-up shop iterations, in St Petersburg and as far afield as Ghana. The Russian Government's continuing deployment of influence operations via digital and social media platforms is based on its perception that they are effective, cheap, difficult to defend against, plausibly deniable and a kind of 'equaliser' against the West.[27]

APPROACH AND METHOD

The UoM team applied the project's four thematic research questions to the IRA. It gave each question a section (e.g. Systems and Technology/Techniques) in the following order:

- **Governance and Ethics:** What was the IRA's business model for operations, including its operating concept, financing arrangements, governance, and legal and ethical framework?
- **Persuasive Technology and Techniques:** How did the IRA use technology and techniques to persuade their target audiences?
- **Systems and Technology:** What were the foundational systems, technology and workforce skills required for IRA's operation?
- **Campaign Awareness and Sensemaking:** How was the IRA able to achieve and maintain awareness of the impact of their influence activities?

At the start of research, the team modified Question 2 (**Persuasive Technology and Techniques**) to include the word 'techniques'. As research progressed, it decided to include an exploration of the psychological principles that may have informed or, perhaps, been integral to IRA tactics. The Joint Influence Activities (JIA) expressed an interest in this sub-question during the consultation phase. It also expressed an interest in the role, if any (and if known), Russia's intelligence agencies played in IRA operations. The team explored this in two sections, Persuasive Technology and Techniques, and Campaign Awareness and Sensemaking, but found no clear evidence intelligence agencies were involved.

During the research it became evident that the term 'Internet Research Agency' can be a catch-all for Russian influence campaigns. In consultation with JIA, the UoM team decided to apply the term specifically to the entity founded and registered as a business (the IRA) in the Olgino district of St Petersburg in 2013, before operations moved to 55 Savushkina St in 2014. While Russia's business registry indicates the IRA terminated as a business in 2016, operations at 55 Savushkina St continued unabated until late 2018. The later operations were likely undertaken through one of several other shadowy entities, such as the Federal News Agency. These entities,

[26] "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections" (Office of the Director of National Intelligence, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf; "Report of the Senate Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference. Volume 2: Russia's Use of Social Media with Additional Views" (116th Congress, 2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

[27] "Report of the Senate Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference. Volume 2: Russia's Use of Social Media with Additional Views." 116th Congress, 2019. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

housed at the same address, appear to have been funded by Prigozhin. Thus, for the purposes of this report, the term IRA refers to an organisation that was in operation from 2013-2018 and was based for most of that time at 55 Savushkina St, St Petersburg.

Literature Review

The UoM team began its research with a systematic literature review of scholarly databases (Jstor, Scopus, Ebscohost, Web of Science). It found more than 800 items of interest, including journalistic and first person accounts, 'grey literature' government and think tank reports, and scholarly research articles. Mindful of the project's time frame, the team elected to modify the systematic review process and bypass a comprehensive coding process. Instead, it embarked on an exclusion/inclusion process that excluded works with little or no substantive relation to the research (based on the abstract and a scan of the text) and included, for further study, the most relevant. It finally chose to review approximately 100 works.

The IRA's existence and objectives were an open secret in Russia. Following its establishment in July 2013 job ads appeared for IRA "internet operators". In August, a Russian woman spoke about her interview on social media. Articles and exposes about the IRA's role as a "troll farm", or "troll factory", began appearing in independent Russian media, providing an insight into the organisation and its structure. Western journalists and independent investigators were aware of the IRA as early as 2014 via articles by people like Aric Toler, now at Bellingcat,[28] and Adrien Chen, who wrote "The Agency" for The New York Times.[29] Another independent journalist, Lawrence Alexander, now also at Bellingcat, linked the IRA to a network of some 20,000 pro-Kremlin Twitter accounts, most of them bots. Alexander concluded, based on his research, that they were "created by a common agency".[30]

However, most of the information regarding IRA influence operations relates to the IRA's campaign to upset the US political system and 2016 Presidential elections. Important insights into its US operations flowed from the indictment of 13 Russian nationals by Special Counsel Robert Mueller in February 2018, and the criminal complaint of the United States of America v. Elena Alekseena Khusaynova in September the same year. In addition, there were two major reports to the US Senate Select Committee on Intelligence, assessments by the US Intelligence Community, grey literature reports from think tanks, and original scholarly research articles cited in this report.[31]

A potential issue with our reliance on open-source documents was the possibility that deception would feature in some of the material, e.g., in first person accounts by former 'trolls' or Russian journalistic investigations. This deception may be intentional, or it might be unintentional. However, as the report draws on a variety of sources, including unclassified US Government investigations and intelligence assessments (where unclassified evidence and sources are not listed), we believe our assessment of the IRA and its operations is as accurate as possible.

[28] Aric Toler, "Inside the Kremlin Troll Army Machine: Templates, Guidelines, and Paid Posts," *Global Voices* (blog), March 14, 2015, https://globalvoices.org/2015/03/14/russia-kremlin-troll-army-examples/.

[29] Adrian Chen, "The Agency," *The New York Times*, June 2, 2015, sec. Magazine, https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

[30] Lawrence Alexander, "Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign," *Global Voices* (blog), 2015, https://globalvoices.org/2015/04/02/analyzing-kremlin-twitter-bots/.

[31] "U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-Cr-32)," February 16, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere; "US District Court Criminal Complaint against Elena Khusyaynova" (U.S. District Court: Eastern District of Virginia, September 28, 2018); Renee DiResta et al., "The Tactics & Tropes of the Internet Research Agency," 2019, https://digitalcommons.unl.edu/senatedocs/2; Philip N Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012-2018," 2019.

Expert Consultation and Knowledge Elicitation Process

Consultation with senior academic project members at the UoM and partner institutions was key to this project, and primary researchers met fortnightly with other UoM team members to discuss progress. After the initial draft outline, there was a week-long consultation process. The Loomio online platform gave members access to the draft document, and the ability to post questions and provide feedback. Academics from partner institutions were also consulted and their feedback informed the next phase of the research, including ongoing literature searches and, where gaps were identified, consultation with senior academics. Consultation with senior academics and the JIA was ongoing and informed the final report.

GOVERNANCE AND ETHICS

SUMMARY OF FINDINGS

- The IRA operated with approval/direction from Russian President Putin and funding from Yevgeny Prigozhin.
- It functioned as an influence operations force devoted to promoting the Kremlin's domestic and geopolitical/strategic goals – a kind of private military company operating in the information environment.
- The IRA used operatives to gather intelligence and carry out missions (purchase of server space, etc.) on the ground.
- It cultivated unwitting and/or witting assets in target populations.
- Trolls acted as influence operations 'foot soldiers', or operatives, who each posted hundreds of comments, and additional content, daily.
- The IRA adopted the business model and, to a degree, the cover of a digital marketing firm.
- It used off-the-shelf social media analytic software and tools to segment (map) populations into discrete audiences (and for sensemaking).
- The IRA (and Russian influence operations generally) operated with ethical and "ideological fluidity".
- Its primary goal was advancing Russian domestic and geopolitical interests, where the end justified the means.
- International public opinion did not seem to matter, insofar as those in authority tried to maintain plausible deniability (for some operations) to remain credible actors in the international community.

The IRA's efforts to inflame racial and ethnic tensions contravened international treaties to which Russia is signatory. These are:

- The International Convention on the Elimination of all Forms of Racial Discrimination (CERD).
- The International Covenant on Civil and Political Rights (ICCPR).

STRENGTHS AND WEAKNESSES

Strengths

The IRA operated with Putin and the Russian Government's domestic and strategic geopolitical goals in mind. As long as its influence operations embraced these broad goals, it could operate with ideological fluidity and, thus, target diverse audiences across the political spectrum. For example:

- The IRA's legal incorporation as a private company and hidden/disguised funding via Prigozhin's businesses gave President Putin and the Russian Government plausible deniability in relation to the IRA's influence operations.
- The IRA's business model, based on a digital marketing firm, was tailor-made to take advantage of the new information environment created by social media platforms and lax regulation.
- The IRA's business model maximised the data harvested by social media companies to segment populations and micro target audiences based on demographics, behaviour, attitudes and other factors.
- The IRA's business model was easy to clone, and pop-up influence shops appeared in Russia and elsewhere.

- Large numbers (estimates range from 400-1000) of 'trolls' with basic linguistic, cultural and technical skills were able to create and rapidly disseminate large amounts of content/messaging across multiple platforms.

Weaknesses

The IRA's business model left a 'paper trail' – a physical and digital footprint that eventually reduced its plausible deniability.

Criminal activity (in the US) resulted in indictments against Prigozhin and other IRA managers, as well as sanctions by the US Department of the Treasury against individuals including Prigozhin, and associated business entities.

GOVERNANCE STRUCTURE

The IRA was a legally registered business in Russia which operated under the business model of a digital marketing firm, as discussed in greater detail below. It was often referred to as a 'troll farm'. The term 'troll' is used in this report to describe the IRA's 'influence operation troops'. However, it does not fully encompass the sophisticated capabilities of IRA employees or the tactics they used.

The IRA served as a kind of covert private military company carrying out influence operations in the information environment, using the methods, business model and cover of a digital marketing firm. Its employees, including the so-called 'trolls', were paid as influence operations troops, or operatives, engaged in what internal documents called 'information warfare' against targets including the US and its allies.

This research project defines the IRA as a private military company engaged in information warfare and operating as a proxy for President Putin and the Kremlin. It breaks down the IRA's governance and business model into three components – strategic, operational and tactical.

Strategic

At a strategic level, in the assessment of the US Intelligence Community, the IRA operated with the approval of Russian President Putin and he ordered specific influence campaigns (of which the IRA was a part but which also included Russian intelligence services) targeting the US political system and 2016 elections. At the operational and tactical levels, Russian influence campaigns, including those of the IRA, tended to be decentralised in terms of governance, with the various organisations and individuals involved "guided by their sense of the Kremlin's desires rather than any master plan". [32]

The IRA was funded by Prigozhin, through his Concord Management and Consulting LLC and Concord Catering company. Great pains were taken to obscure this funding source; Concord recorded payments for software and IT services, which were then more deeply concealed by being routed through at least 14 separate bank accounts held in its name and the names of its business affiliates.

Prigozhin is an oligarch close to Putin who made his money in food and catering. He is sometimes referred to derogatively as Putin's chef. Crucially, he has established online news operations to push Russian Government and nationalist agendas, and he controls the Wagner Group, which operates pro-Russian covert operations and

[32] Snegovaya, Maria, and Kohei Watanabe. "The Kremlin's Social Media Influence inside the United States: A Moving Target," February 10, 2021.

mercenary services.[33] The Wagner Group is closely associated with the GRU[34] Prigozhin had regular meetings with senior IRA management, and they were aware of his role. According to the US Justice Department, Prigozhin was involved in approving IRA activity. Mikhael Bystrov, the director general of the IRA, as well as of some of its entities, had regular, in person meetings with Prigozhin, while his second in command, Mikhael Burchik, also met personally with Prigozhin. It is reasonable to assume that Prigozhin provided oversight and operated as a kind of go-between for the IRA and President Putin.

At the strategic level, the IRA was, as stated previously, part of a much larger ecosystem of propaganda and influence controlled by the Russian Government. The IRA was directed to help President Putin achieve his geopolitical goals, including weakening the West – and its democratic alliances – and re-establishing Russia's influence, both in the immediate region and as a global power. More specifically, these goals included:

- Ensuring the current regime-maintained power.
- Returning Russia – economically, politically, and militarily – to the status of a Great Power and restoring the prestige of the former Soviet Union.
- This included amplifying divisions between ethnic Russians and other populations, and the governments of these nations, while projecting solidarity with ethnic Russians.
- Undermining NATO and other democratic alliances, and faith in Western dominated, global institutions and systems.
- Undermining faith in democratic governments, institutions, and leaders.
- Undermining the legitimacy of US global leadership and weakening the US generally.
- Sowing doubt, discord and distrust, and corrupting, polluting, or infecting the information environment of target populations, to prevent or reduce rational democratic discourse and decision making, and potentially achieving/coercing policy decisions beneficial to Russian interests.

Operational

Specific campaigns and targets of the IRA, such as the US political system and 2016 Presidential elections, were authorised by President Putin. However, campaign decisions and preparations at the operational level appear to have been made in-house. Where activity indicates the coordination of IRA messaging with covert activity by Russian intelligence services and proxies (such as the hack and release of US Democratic Committee emails), the coordination was likely from the top down, from Putin and/or Prigozhin. However, it is possible that there was also horizontal cooperation, and even integration of Russian intelligence agents and the IRA. However, there is no direct evidence of this.

The IRA did not operate like a traditional military or intelligence organisation. Rather, as discussed, it adopted the business model and structure of a "digital marketing firm".[35] It was led by Bystrov (an ex-Police colonel) and run by a management team (with backgrounds in, among other things, IT entrepreneurship, and advertising and public relations). It was organised into departments and teams, including:[36]

- Content Development, or "bloggers", departments

[33] Centre for Strategic International Studies,"Band of Brothers: The Wagner Group and the Russian State." September 21, 2020. https://www.csis.org/blogs/post-soviet-post/band-brothers-wagner-group-and-russian-state.

[34] Nathaniel Reynolds, "Putin's Not-So-Secret Mercenaries: Patronage, Geopolitics, and the Wagner Group," Carnegie Endowment for International Peace, July 8, 2019.https://carnegieendowment.org/2019/07/08/putin-s-not-so-secret-mercenaries-patronage-geopolitics-and-wagner-group-pub-79442.; U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-cr-32), February 16, 2018. https://www.justice.gov/file/1035477/download

[35] DiResta et al., "The Tactics & Tropes of the Internet Research Agency."

[36] "US District Court Criminal Complaint against Elena Khusyaynova" (U.S. District Court: Eastern District of Virginia, September 28, 2018).

- Content developers worked individually and in teams (e.g. when driving comments and discussions on websites)
- Teams/departments focused on geographic regions – e.g. 'American Department' (also known as the Translator Project)
- Data Analysis Department
- Search Engine Optimisation Department
- Design and Graphics Department
- IT Department
- Finance Department

This model, from the commercial world, was ready-made to take advantage of the opportunities provided by the new information environment and social media, to segment and target audiences with content based on behaviour, attitudes, and so on. It also meant the IRA could remain agile and experimental.

The IRA employed around 400-600 people (some estimates suggest it may have had as many as 1000 employees), and ran on a budget of about US $1.25 million a month.[37] (As a comparison, the annual military budget of the Russian Federation was some US $61.7 billion in 2020).[38] The bulk of the employees appear to have been 'trolls', and their jobs equivalent to entry level social media content developers. However, some positions required advanced language and cultural skills to operate the more sophisticated sock puppet accounts. These employees were paid between 25,000 and 45,000 rubles ($AU450-700) a month.[39] It is unclear whether the employees knew of Prigozhin and his role in the operation. However, insider reports suggest staff did know they were employed to create content and messaging aligned with the Russian Government's agenda. Moreover, that the IRA was run at the behest of the Russian Government was an open secret, and independent journalists covered the organisation in Russia from the first months of its inception.

Management conducted social media analysis and gave daily tasking briefings to 'trolls' and other content developers. However, while these briefings outlined targets and issued broad instruction on how to target different audiences, it appears the trolls were allowed creative license in implementing the instructions, as long as they met specified targets regarding the number of words used, and the use of graphics and other content.[40]

The IRA also appears to have been just one organisation within a larger operation, known as Project Lakhta, which targeted foreign and domestic populations with influence operations and propaganda. Project Lakhta and the IRA were both funded by Prigozhin, primarily through the Concord Management and Consulting LLC and Concord Catering businesses. However, there is very little open-source material about Project Lakhta. We know virtually nothing about it, other than the fact its operations were hidden behind a multitude of business entities, including the IRA.

Tactical

At the tactical level, content and messaging were created and propagated daily by teams of influence operation troops ('trolls'), following tasking briefs from managers, who conducted online sensemaking and intelligence

[37] U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-cr-32), 16 February 2018; DiResta et al., "The Tactics & Tropes of the Internet Research Agency."

[38] "Ranking: Military Spending by Country 2020," Statista, accessed June 20, 2021, https://www.statista.com/statistics/262742/countries-with-the-highest-military-spending/.

[39] For reference, the average Russian salary in 2019 was approximately 48,000 rubles a month (statistica.com).

[40] US District Court Criminal Complaint against Elena Khusyaynova" (U.S. District Court: Eastern District of Virginia, September 28, 2018); Toler, "Inside the Kremlin Troll Army Machine."2015

gathering – something digital marketers call social listening. This will be discussed in more detail in Campaign Awareness and Sensemaking.

As mentioned, the IRA employed roughly 400-600 people, with some estimates suggesting it may have had up to 1000 employees. Most of these employees were paid "trolls" who:

- Worked rotating schedules of 12-hour shifts, five days a week (the IRA was a 24/7 operation).
- Earned a monthly wage of 40,000-50,000 rubles (AU$700-800).
- Were required to create at a minimum 135 posts/comments during a 12-hour shift, as well as blog posts and other content.
- Maintained six Facebook accounts/10 Twitter accounts, with connections taking place via proxy servers and Virtual Private Networks (VPN).
- Cultivated social media followings across multiple platforms.
- Were required to have a minimum 500 followers by the end of their first month on the job.
- Received fines for not reaching the required number of posts each day.
- Worked in rooms with about 20 people, often operating in groups of three (one troll would post a controversial statement, another would challenge it and a third would post a link to a website, generally a Russian 'news' propaganda site).[41]
- Received instructions in the form of a brief (technical tasks) outlining the political or social themes and topics to address.
- Were responsible for creating non-political posts/content and online personas.[42]

And, as we discuss later, the IRA used bots/botnets as force multipliers for messaging/content propagation.

ETHICAL FRAMEWORK

Ethical Fluidity

Ethically, the actions of the IRA, unlike the Soviet era active measures, were not serving a larger ideological purpose. Rather, the goals appeared to be purely aligned with furthering Russia (and Putin's) domestic and geopolitical goals, including weakening the West. Thus, the IRA, and Russian influence operations generally, operated with an ethical and ideological fluidity that allowed them to simultaneously target diverse audiences across the political spectrum, to sow doubt, discord and distrust. And because the primary goal was advancing Russian domestic and geopolitical interests/goals, which included weakening the West and its allies, the messaging did not have to align with facts, or even be consistent with other messaging (in targeting different groups, for instance). In the US, for example, it targeted audiences across the political spectrum, with content tailored to groups from conservative Texas secessionists to Greens, financial elites and LGBTQ activists.[43] And, to maximise the division and strife these influence campaigns produced, IRA operatives often posted opposing

[41] Natasha Bertrand, "Russian Internet Trolls Are Trained to Spread Propaganda in Three-Person Teams," Business Insider Australia, April 1, 2015, https://www.businessinsider.com.au/russian-internet-trolls-are-trained-to-spread-propaganda-in-three-person-teams-2015-3; Shaun Walker, "The Russian Troll Factory at the Heart of the Meddling Allegations | Russia | The Guardian," 2015, https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house.

[42] Shaun Walker, "The Russian Troll Factory at the Heart of the Meddling Allegations | Russia | The Guardian." April 2 2015. https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house.

[43] "Report of the Senate Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference. Volume 2: Russia's Use of Social Media with Additional Views", 2019; DiResta et al., "The Tactics & Tropes of the Internet Research Agency.", 2019

views – promoting racial and social justice to minority groups, while attacking Black Lives Matter and similar groups in posts to 'white' audiences.

Domestic Laws in Targeted Countries

It is unclear whether the IRA, a legally registered private business, broke Russian laws in its influence operations, or its funding arrangements. However, it contravened laws in other countries. In the US it contravened Federal laws preventing foreign interference in elections and laws to do with the fact it was a criminal enterprise. Thirteen IRA employees were indicted by the US Department of Justice, including Prigozhin. Prigozhin and other of his associates and businesses were targeted with US Department of the Treasury sanctions relating to their influence operations.[44]

Contravening International Law

According to the US Department of Justice, the IRA sought, in the words of one operative, to "effectively aggravate the conflict between minorities and the rest of the population". The IRA wanted to inflame ethnic tensions. It pursued this aim in the US, as per the example above, and its near abroad (e.g., targeting ethnic Russian populations in Eastern Europe). The IRA contravened at least two international treaties to which Russia is a signatory, as well as the spirit of the UN Charter. Article 1 outlines the UN's commitment to a "respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion".

Legal scholars agree the IRA contravened the following international treaties prohibiting racial discrimination and hate speech:

- The International Convention on the Elimination of all Forms of Racial Discrimination (CERD).
- In Article 4 CERD calls on member states to condemn "all propaganda and all organizations which are based on ideas or theories of superiority of one race or group of persons of one colour or ethnic origin, or which attempt to justify or promote racial hatred and discrimination...".
- The International Covenant on Civil and Political Rights (ICCPR).
- In Article 20(2) the ICCPR states that "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law".[45]
- The Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, ECHR).

Russia does seem to care what the international community thinks insofar as it makes some attempt to remain a credible actor. For example, IRA messaging in Syria maintained US intervention was causing the country's problems, while Russian intervention was supporting a legitimate government.

Moreover, many countries have proposed or adopted legislation to address online influence campaigns. Social media companies are also implementing procedures to identify and shut down accounts engaged in influence activities (often referred to as coordinated inauthentic activity).[46]

The IRA was quick to adapt to these developments. When Facebook started investigating and shutting down its accounts it moved to Instagram.[47] In Russia today, interest has waned in sock puppet accounts because they can

[44] U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-cr-32), 16 February 2018

[45] "OHCHR | International Covenant on Civil and Political Rights," accessed June 9, 2021, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

[46] Nathaniel Gleicher and David Agranovich.

[47] DiResta et al., "The Tactics & Tropes of the Internet Research Agency."

be removed. There is evidence of a shift in Russian influence operations, towards engaging native freelance journalists and news media outlets to drive pro-Kremlin narratives in targeted countries.[48]

[48] Snegovaya and Watanabe.

PERSUASIVE TECHNOLOGY

SUMMARY OF FINDINGS

Characteristics of IRA online influence operations (and Russian online influence operations generally) include:

- Multi-platform, high volume, high-speed messaging, and content production/dissemination.
- Blending/coordinating overt and covert operations.
- Extensive use of influence operations troops/operatives ('trolls').
- Amplifying selected content and narratives using automated accounts/bots.
- IRA influence operations appear to use known psychological principles of influence.
- The IRA took advantage of social media platforms' advertising revenue and data harvesting business models, and off-the-shelf (native and third party) tools, to segment and micro target diverse audiences.
- The IRA purchased server space (with stolen US identities) in the US to disguise activity with VPN.
- It used digital marketing techniques to create 'doppelganger' (evil twin) ecosystems of brands and sock puppet personas to grow audiences, target audiences and cultivate assets.
- The IRA also organised offline protests, using witting or unwitting agents.

The IRA adopted the business model of a digital marketing firm to carry out its online influence campaigns. It took advantage of the new possibilities to micro target audiences provided by the social media platforms' advertising and data harvesting business models. To hide its operations, it used stolen US identities, created false sock puppet identities, and purchased server space (with stolen US identities) in the US to disguise activity with VPN.

It used off-the-shelf (native and third party) tools to segment and micro target diverse audiences, and conduct other social media analytics, to identify key narratives and content it could use to tailor messaging in evolving multi-platform campaigns that used best practice, digital marketing techniques for malign influence. This enabled the IRA to reach and engage with tens of millions of US citizens between 2014 and 2018.

STRENGTHS AND WEAKNESSES

Strengths

- Ability to target audiences across multiple platforms at high-speed and volume.
- Ability to micro target audiences across the political spectrum - from Black Lives Matter followers to 'gun rights' activists and LGBTQ groups.
- Ability to grow (and target) large followings using false, sock puppet accounts, websites, etc.
- Ability to cultivate and recruit assets for online and offline activities.
- Ability to analyse social media data using off-the-shelf, third-party software and tools native to platforms, to segment and target audiences.
- Ability to amplify selected messages and narratives (e.g. wedge issues, conspiracy theories) using bots and botnets.
- IRA messaging and content effectively targeted the emotions and social identities of audiences. This included extensive nationalistic messaging.

Weaknesses

- Reliance on sock puppet and other false/counterfeit sites to grow and target large audiences. When these accounts or sites were taken down (social media platforms are getting better at this), the audiences were effectively lost.
- Reliance on botnets to amplify messaging/narratives. Tools and methods for identifying and taking down botnets are improving (this is also likely an 'arms race'), and it has become easier for platforms to remove inauthentic coordinated activity en masse.

The following sections explore some of the IRA's principal persuasive technologies and techniques in more detail (amplification, which could be included, features in the **Systems and Technology** section).

PERSUASIVE TACTICS

IRA tactics designed to persuade audiences included but were not limited to:[49]

- Multi-platform messaging at high-speed and volume. The IRA was active on several social media platforms. This increased credibility because the messages audiences received came from multiple, apparently independent sources. Using hundreds of human operators meant messaging could be produced at high-speed and volume and, during an event like MH17, embed thoughts and impressions while the official investigations were underway. These could be amplified by bots and botnets (see below).
- Amplification. The IRA used bots extensively to amplify its own messaging and material from websites, influencers, etc., where the content aligned with its goals. Amplification also aided multi-platform messaging at high-speed and volume.
- Micro targeting. The availability of vast amounts of user data harvested from social media platforms, analysed by native and third-party social media analytic software, data brokers and other means, meant the IRA could segment populations and micro target audiences with tailored messaging.
- Paid advertising. The IRA used paid ads on multiple platforms to grow and target audiences. These were based on behavioural and psychometric data harvested and available from social media platforms and other sources.
- "Doppelganger" websites and brands. The IRA created an extensive ecosystem of doppelganger (evil twin) websites that mimicked the websites of genuine 'brands' and social movements, such as Black Lives Matter, to grow, target and influence audiences (and cultivate assets).
- Sock puppet personas/accounts. The IRA used fake personas (some quite sophisticated) to infiltrate social media groups and engage with online audiences, and to groom and recruit assets to write posts, organise rallies and demonstrations, and engage in other ways. An example is "Tennessee GOP" which, under the Twitter handle @TENN_GOP, accrued some 100,000 followers who presumably believed that the account represented, or was associated with, the Tennessee Republican Party.[50]
- Memes and audio visual/symbolic messaging. The IRA generated a lot of original content (memes, YouTube videos, tweets etc.), and extensively recycled/repurposed existing memes and other material

[49] Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, et al., "The Tactics & Tropes of the Internet Research Agency," 2019; Philip N Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012-2018," 2019.

[50] *U.S. v. Internet Research Agency LLC, et al* (U.S. District Court for the District of Columbia; 1:18-cr-32), 16 February 2018

to amplify its messaging. The IRA created memes but also extensively appropriated, adapted and amplified existing memes.

- Recruiting journalists to write pro-Russian news articles.
- The IRA distributed content/messaging using Twitter handles mimicking US (and other) news sources to spread disinformation and grow target audiences. It appears to have pioneered the tactic during the Columbian Chemicals plant hoax of 2014.[51]
- The IRA used false online personas to recruit assets to hire unwitting Western journalists to write articles for news outlets in Russia's ecosystem of influence. Common themes/topics included human rights abuses committed in the US and UK.
- IRA content directed traffic (with links and comments, and other content) to multiple pro-Russian 'news' websites, such as PeaceData.net, using human trolls and bots.
- Organising offline protests. Using false persona accounts, and posing as grassroots US activists, IRA operatives "organised and coordinated"[52] offline political activity in the US. They did this by creating politically charged social media pages and groups to lure genuine activists, who became unwitting participants, organising rallies and protests, and sometimes receiving financial compensation for their work. The IRA promoted the events with paid advertising on Facebook and Instagram, and via individualised messaging that encouraged people to attend. They supported the IRA's strategy of promoting political and social discord. On more than one occasion the organisation orchestrated duelling rallies. A "Show your support for President-elect Donald Trump" rally and a "Trump is NOT my President" rally were held at the same time and place.[53]
- Purchasing followers. Forensic analyses of accounts suggest the IRA also used the "black market", social media manipulation[54] technique of purchasing followers. Some IRA Twitter accounts acquired up to "10,000 followers in a very short period of time".[55] There are companies that offer services to buy followers/likes. You can purchase up to 2,500 followers on Twitter for as little as $50. Other "growth" agencies offer packages designed to grow larger followings. It is unclear whether IRA trolls purchased followers to meet their performance metrics, or whether followers were purchased as part of the organisation's strategy.[56]
- Follower fishing. Another tactic the IRA used to build audience and influence was 'follower fishing'. Follower fishing is used (particularly on Twitter) to gain new followers. An IRA account, often a bot account, would click follow on thousands of new accounts in the hope they would "follow back". Once

[51] Adrian Chen, "The Agency," *The New York Times*, June 2, 2015, sec. Magazine, https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

[52] "U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-Cr-32)," February 16, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.

[53] "U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-Cr-32)," February 16, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.

[54] "The Black Market for Social Media Manipulation | StratCom," accessed February 2, 2021, https://www.stratcomcoe.org/black-market-social-media-manipulation.

[55] Andrew Dawson and Martin Innes, "How Russia's Internet Research Agency Built Its Disinformation Campaign," *The Political Quarterly* 90, no. 2 (June 2019): 245–56

[56] Dawson and Innes.

the new followers were on board, the IRA would unfollow the accounts. This increased the IRA accounts' 'followers per followed' ratio, boosting its position on the platform's algorithm.[57]

It is worth exploring some of these tactics in more detail, especially sock puppet accounts and 'doppelganger' websites. These appear to have been quite successful in growing audiences, but also in their ability to influence both online and offline behaviour, and in the recruitment of witting and unwitting assets.[58] The IRA's possible use of the psychological principles of persuasion[59] will also be discussed in more detail.

Multi-Platform Campaigns

The IRA engaged audiences across multiple platforms and channels, leveraging the content creation and curation provided by hundreds of human employees, and numerous false, online identities - commonly referred to as sock puppet accounts - to deeply embed itself in a target population's social media network. In the US, between 2013 and 2018, it concentrated first on Twitter but rapidly evolved a multi-platform strategy, eventually reaching tens to hundreds of millions of Americans, including an estimated 126 million Facebook users. At least 30 million users shared IRA content or pages with friends and family on Facebook and Instagram, generating likes and comments and other reactions. [60] Twitter identified 3,841 IRA-linked "troll" accounts and up to 50,000 bot accounts. [61] Twitter's own analysis identified that at least 1.4 million US users engaged (by liking, quoting, retweeting, or replying/commenting) with IRA-controlled accounts at the time of the 2016 US Presidential election.[62]

The IRA also utilised certain platforms to trial content and determine what forms of messaging would elicit the greatest engagement, before moving content to other platforms. For example, the IRA used Reddit to "trial balloon" or "kite-fly" messaging on a smaller audience. It took the most successful messaging from Reddit, tailored it, and disseminated it on social media platforms that were proving more popular, such as Facebook.[63]

An evolution in its activities shows how the IRA adapted and adjusted its online behaviour over time. For instance, the timeline on page 6 of this report shows the IRA first targeted US audiences on Twitter. Then, towards the end of 2014, it began to ramp up its activities on other platforms, first on YouTube, then Instagram and, lastly, on Facebook.[64]

[57] Dawson and Innes.

[58] Renee DiResta et al., "The Tactics & Tropes of the Internet Research Agency," 2019, https://digitalcommons.unl.edu/senatedocs/2.

[59] A question that JIA expressed particular interest in during consultation.

[60] Howard, Philip N, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François. "The IRA, Social Media and Political Polarization in the United States, 2012-2018," 2019.p.3

[61] "Update on Twitter's Review of the 2016 US Election." January 31, 2018 https://blog.twitter.com/en_us/topics/company/2018/2016-election-update.html.

[62] Golovchenko, Yevgeniy, Cody Buntain, Gregory Eady, Megan A. Brown, and Joshua A. Tucker. "Cross-Platform State Propaganda: Russian Trolls on Twitter and YouTube during the 2016 U.S. Presidential Election." *International Journal of Press/Politics* 25, no. 3 (July 2020): 357–89. https://doi.org/10.1177/1940161220912682.p262

[63] Josephine Lukito, "Coordinating a Multi-Platform Disinformation Campaign: Internet Research Agency Activity on Three U.S. Social Media Platforms, 2015 to 2017," *Political Communication* 37, no. 2 (March 3, 2020): 238–55, https://doi.org/10.1080/10584609.2019.1661889.

[64] Howard, Philip N, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François. "The IRA, Social Media and Political Polarization in the United States, 2012-2018," 2019.

Sock Puppet Personas

The IRA used false identities to create sock puppet personas (false online identities) in large numbers for the purposes of deception, and to create and disseminate messaging and content that looked authentic. In the US, it purchased the stolen identities of US citizens to establish these accounts and target America's political system. Some were highly sophisticated. The Twitter account @PoliteMelanie, which targeted urbane, left leaning US audiences, amassed more than 20,000 followers. Trolls operating accounts such as @PoliteMelanie and @TyraJackson posted a range of content, including feelgood material, to build audiences. But they also engaged in activity that bordered on incitement to violence, including posting videos of purportedly racist behaviour, with the phone numbers or names of perpetrators, and encouragement to people to act.[65]

Many of these accounts had tweets discussed in the mainstream media. The Chicago Tribune gave @PoliteMelanie a tweet of the week award. It seems success in the tactic, known as 'breaking out' (i.e., mainstream media or influencers picking up IRA messaging), was highly sought after by operators and there are hundreds of examples.[66] Breaking out built on Soviet era active measures. Soviet defector Lawrence Martin-Bittman said success in a disinformation campaign was measured by the extent to which the information featured in a country's media or political dialogue.[67] Thus, it appears the IRA considered messaging (e.g., tweets) successful when the content was picked up by mainstream media, or absorbed into societal/political discourse.[68] Certainly, a number of IRA Twitter accounts were successful both in attracting large followings and breaking out.[69]

Doppelganger Websites and Brands

The IRA created interlinked ecosystems of doppelganger ('evil twin') websites, Facebook pages and brands that mimicked authentic social movements and affinity group sites when their real purpose was malign influence. It used digital marketing practices to create doppelganger brands such as BlackMattersUS, a fake Black Lives Matter group, developing logos and hiring US citizens to make Facebook stickers and other material.[70]

[65] Darren Linvill and Patrick Warren, "That Uplifting Tweet You Just Shared? A Russian Troll Sent It," *Rolling Stone*, November 1, 2019, https://tigerprints.clemson.edu/communication_pubs/18. Linvill and Warren.

[66] "Twitter Exploit: How Russian Propaganda Infiltrated U.S. News," accessed January 18, 2021, https://uwmadison.app.box.com/v/TwitterExploit. Ben Nimmo, "The Breakout Scale: Measuring the Impact of Influence Operations," 2020, 15.

[67] Mirela Silva et al., "Facebook Ad Engagement in the Russian Active Measures Campaign of 2016," 2020, https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edsarx&AN=edsarx.2012.11690&site=eds-live&scope=site&custid=s2775460. Silva et al.

[68] Silva et al., "Facebook Ad Engagement in the Russian Active Measures Campaign of 2016"; "Perspective | Russian Trolls Can Be Surprisingly Subtle, and Often Fun to Read," *Washington Post*, accessed May 24, 2021, https://www.washingtonpost.com/outlook/russian-trolls-can-be-surprisingly-subtle-and-often-fun-to-read/2019/03/08/677f8ec2-413c-11e9-9361-301ffb5bd5e6_story.html; "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections"; Ben Nimmo, "The Breakout Scale: Measuring the Impact of Influence Operations," n.d., 15. Silva et al., "Facebook Ad Engagement in the Russian Active Measures Campaign of 2016"; "Perspective | Russian Trolls Can Be Surprisingly Subtle, and Often Fun to Read"; "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections"; Nimmo, "The Breakout Scale: Measuring the Impact of Influence Operations."

[69] "Twitter Exploit: How Russian Propaganda Infiltrated U.S. News." "Twitter Exploit: How Russian Propaganda Infiltrated U.S. News."

[70] DiResta et al., "The Tactics & Tropes of the Internet Research Agency"; Andrew J. Webber, *The Doppelgänger: Double Visions in German Literature* (Clarendon Press, 1996); Craig J. Thompson, Aric Rindfleisch, and Zeynep Arsel, "Emotional Branding and the Strategic Value of the Doppelgänger Brand Image," *Journal of Marketing* 70, no. 1 (January 1, 2006): 50–

The IRA used social media marketing tools and techniques, including native and third-party social media analytic software, to identify groups and websites to mimic. The tools helped in identifying/segmenting target populations and placing them into affinity groups/ 'tribes', with their own themes/issues. Basic demographic segmentation was possibly used in combination with psychographic information. These affinity groups, or 'tribes', included but were not limited to[71]:

- Black culture/community issues
- Police brutality/Black Lives Matter
- Pro-Trump/anti-Clinton groups
- Pro-Police/Blue Lives Matter groups
- Anti-refugee/immigration groups
- Texas culture
- Southern culture
- Separatist movements
- Muslim groups
- LGBT groups
- Gun rights/2nd Amendment activist groups
- Tea Party and affiliated groups
- Religious rights
- Native American groups
- Veteran groups

The IRA's doppelganger brands were active across social media. BlackMattersUS, for example, was active on Facebook, Twitter, YouTube, Instagram and Tumblr. It had a podcast on Soundcloud and placed 31 advertisements through Google Ads. Generally, IRA messaging was most prominent on Twitter, Facebook and Instagram, with significant - but somewhat less - activity on the other platforms. The IRA linked much of the content across these platforms and, at times, presented as the same individual imposter or group. The tactic fitted with the IRA's overall strategy to build a doppelganger ecosystem and "surround" its target audiences with messaging.

Developing Assets

According to US Government documents, the IRA worked to recruit witting and/or unwitting agents, using established tactics including infiltrating protest movements and gathering compromising material that could be used later to blackmail or manipulate individuals. IRA agents posed as US citizens and some trolls acted as 'honeypot' trolls. However, their activities went far beyond that.

IRA websites and personas posing as US citizens posted job ads and requests for people to undertake certain tasks. The targets were individuals and groups across the political spectrum but the African American community received special attention. There were ads and requests for people to [72]:

64, https://doi.org/10.1509/jmkg.70.1.050.qxd. DiResta et al., "The Tactics & Tropes of the Internet Research Agency"; Webber, *The Doppelgänger*; Thompson, Rindfleisch, and Arsel, "Emotional Branding and the Strategic Value of the Doppelgänger Brand Image."

[71] Renee DiResta et al., "The Tactics & Tropes of the Internet Research Agency," 2019, https://digitalcommons.unl.edu/senatedocs/2.

[72] Jack Stubbs, "Duped by Russia, Freelancers Ensnared in Disinformation Campaign by Promise of Easy Money," *Reuters*, September 3, 2020, https://www.reuters.com/article/us-usa-election-facebook-russia-idUSKBN25T35E; DiResta et al., "The

- Organise protests.
- Write articles for IRA doppelganger websites.
- Speak at protests.
- Provide free self-defence courses.
- Take photos at protests.
- Upload photos to IRA doppelganger websites.
- There were job ads for designers to help with website design, Facebook stickers and other material.
- The IRA also posted ads that offered counselling to people struggling with sexual behaviour/addiction, or sexual identity.

PSYCHOLOGICAL INFLUENCE

IRA activity suggests the organisation may have leveraged psychological principles in developing and disseminating its persuasive messaging. However, it is possible this was an indirect result of applying techniques common to digital marketing. Nevertheless, IRA messaging tapped into an individual's social identity to produce an emotional response. Research suggests this makes messaging and content more believable, increasing the likelihood it will be shared.[73]

Creating First Impressions

The IRA understood the importance of controlling the narrative through resilient first impressions. [74] Psychological literature on the subject suggests that initial messaging is resistant to correction, and continues to shape people's thinking long after a retraction or contradictory message emerges.[75] The IRA was often the first to release an account/version of news or events because fact-checking, consistency and objective reality were not a concern. 'Briefs' or 'taskings' directed trolls to put a pro-Russian spin on the latest news, events and any associated conspiracy theories. The IRA seemed to have leveraged this idea in its messaging implicating the Ukraine in the MH17 disaster, which coincided with its highest ever number of tweets.[76] The approximately 45,000 IRA tweets that appeared in the immediate aftermath blamed the Ukraine.[77] Many people who received

Tactics & Tropes of the Internet Research Agency"; Julia Carrie Wong, "Russian Agency Created Fake Leftwing News Outlet with Fictional Editors, Facebook Says," The Guardian (Online) (London (UK), United Kingdom: Guardian News & Media Limited, September 2, 2020), https://www.proquest.com/docview/2439507422/citation/638552B13B484CE2PQ/1. Stubbs, "Duped by Russia, Freelancers Ensnared in Disinformation Campaign by Promise of Easy Money"; DiResta et al., "The Tactics & Tropes of the Internet Research Agency"; Wong, "Russian Agency Created Fake Leftwing News Outlet with Fictional Editors, Facebook Says," September 2, 2020.

[73] Stephan Lewandowsky et al., "Misinformation and Its Correction: Continued Influence and Successful Debiasing," *Psychological Science in the Public Interest*, September 17, 2012, https://doi.org/10.1177/1529100612451018.

[74] Petty, Richard E., John T. Cacioppo, Alan J. Strathman, and Joseph R. Priester. "To Think or Not to Think: Exploring Two Routes to Persuasion." In *Persuasion: Psychological Insights and Perspectives, 2nd Ed*, 81–116. Thousand Oaks, CA, US: Sage Publications, Inc, 2005.

[75] A. L. Wilkes and D. J. Reynolds, "On Certain Limitations Accompanying Readers' Interpretations of Corrections in Episodic Text," *The Quarterly Journal of Experimental Psychology A: Human Experimental Psychology* 52A, no. 1 (1999): 165–83, https://doi.org/10.1080/027249899391278; Lewandowsky et al., "Misinformation and Its Correction."

[76] C.Kriel, A.Pavliuc. "Reverse Engineering Russian Internet Research Agency Tactics through Network Analysis. | StratCom." Accessed February 3, 2021. https://www.stratcomcoe.org/ckriel-apavliuc-reverse-engineering-russian-internet-research-agency-tactics-through-network.p.223

[77] VoxUkraine. "How Russian 'Troll Factory' Tried to Effect on Ukraine's Agenda. Analysis of 755 000 Tweets." Accessed March 25, 2021. https://voxukraine.org/longreads/twitter-database/index-en.html.p.

them continue to believe them,[78] despite clear evidence MH17 was shot down by a surface-to-air-missile, supplied and operated by Russian armed forces.

Repetition And Quantity

The IRA leveraged repetition and volume in its persuasive messaging. Repetition allowed the IRA to amplify key narratives and create the impression that some opinions were more widespread than they were.[79] Social and cognitive psychology research suggests the volume of messaging matters, as message repetition can generate a feeling of familiarity, linked in some research to a greater tendency to believe the message.[80] Cognitive psychology suggests that “repeated exposure to a statement increases the subjective ease with which that statement is processed [which] in turn, increases the probability that the statement is judged to be true”.[81] The truth illusory effect is an established theory that suggests repeated exposure to a statement increases its acceptance as true.[82] Social psychology suggests that familiarity brought about by repetition will cause a failure to “discriminate weak arguments from strong arguments”.[83] The IRA persisted with its false claims that Ukraine was responsible for the downing of MH17 well after the stories were debunked. This suggests it was leveraging repeating a statement to increase its acceptance as true. The tactic also gave the IRA freedom to mount weak arguments because, in high rotation, they were processed non-analytically (heuristically). The IRA also used high volume, repetitive messaging to slander Clinton during the 2016 US elections using bots. During the campaign, analyses of the social bot traffic showed that significantly more tweets were pro-Trump than pro-Clinton.[84]

Building Credibility and Information Reinforcement

The IRA leveraged strategies (e.g., doppelganger websites, sock puppet personas) to enhance its credibility and make its messaging more effective and persuasive. Repetition of messaging that comes from, or appears to come from, peers can create the illusion of proof,[85] increasing the likelihood people will adopt an idea, attitude, or

[78] Petty, Richard E., John T. Cacioppo, Alan J. Strathman, and Joseph R. Priester. “To Think or Not to Think: Exploring Two Routes to Persuasion.” In *Persuasion: Psychological Insights and Perspectives, 2nd Ed*, 81–116. Thousand Oaks, CA, US: Sage Publications, Inc, 2005.

[79] Renee DiResta et al., “The Tactics & Tropes of the Internet Research Agency,” 2019, https://digitalcommons.unl.edu/senatedocs/2.

[80] Robert H. Gass and John S. Seiter, *Persuasion: Social Influence and Compliance Gaining* (Routledge, 2015); Daniel Kahneman, *Thinking, Fast and Slow* (Penguin, 2012), https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=cat00006a&AN=melb.b4827859&site=eds-live&scope=site&custid=s2775460; Robert F. Bornstein and Paul R. D’Agostino, “Stimulus Recognition and the Mere Exposure Effect,” *Journal of Personality and Social Psychology* 63, no. 4 (1992): 545–52, https://doi.org/10.1037/0022-3514.63.4.545; Robert B. Zajonc, “Attitudinal Effects of Mere Exposure,” *Journal of Personality and Social Psychology* 9, no. 2, Pt.2 (1968): 1–27, https://doi.org/10.1037/h0025848; “Mere Exposure: A Gateway to the Subliminal - R.B. Zajonc, 2001,” accessed April 30, 2021, https://journals.sagepub.com/doi/abs/10.1111/1467-8721.00154.

[81] Rolf Reber and Christian Unkelbach, “The Epistemic Status of Processing Fluency as Source for Judgments of Truth,” *Review of Philosophy and Psychology* 1, no. 4 (2010): 563–81, https://doi.org/10.1007/s13164-010-0039-7.

[82] Lynn Hasher, David Goldstein, and Thomas Toppino, “Frequency and the Conference of Referential Validity,” *Journal of Verbal Learning & Verbal Behavior* 16, no. 1 (1977): 107–12, https://doi.org/10.1016/S0022-5371(77)80012-1.

[83] Teresa Garcia-Marques and Diane M. Mackie, “The Feeling of Familiarity as a Regulator of Persuasive Processing,” *Social Cognition* 19, no. 1 (February 1, 2001): 9–34, https://doi.org/10.1521/soco.19.1.9.18959.

[84] “DemTech | Bots and Automation over Twitter during the U.S. Election,” accessed April 28, 2021, https://demtech.oii.ox.ac.uk/research/posts/bots-and-automation-over-twitter-during-the-u-s-election/; Mazarr et al., “Hostile Social Manipulation.” “DemTech | Bots and Automation over Twitter during the U.S. Election”; Mazarr et al., “Hostile Social Manipulation.”

[85]Robert B Cialdini, “Harnessing the Science of Persuasion,” 2001.

behaviour. [86] The IRA produced messaging in large volumes across multiple platforms.[87] Research suggests that messaging from different sources has more credibility because consumers assume it includes a range of perspectives.[88] Some research suggests people who find a message credible struggle to change their mind when it is later proved false or inaccurate.[89]

In-Group And Out-Group Identification

Studies on disinformation, misinformation and fake news suggest that messaging that taps into group identity, particularly when it produces an emotional response (including threats to that identity), is more persuasive and likely to be believed.[90] Research indicates that individuals are more likely to identify with, and be influenced by, people from their reference group, or people whose narratives align with their own. [91] Some research suggests individuals who hold extreme ideological beliefs and are hostile to out-groups are less cognitively flexible and, therefore, less able to evaluate information in an unbiased, evidence-based manner.[92] Other research suggests that ideologically framed and interpreted messages are key to generating political polarisation.[93]

Social psychology also suggests that individuals and groups use emotion and emotion-laden messaging to create their own constructed interpretations and realities.[94] The IRA leveraged these processes, for example, to exploit social divisions in the US along racial, religious, political and class lines, among others. Doppelganger Facebook pages and websites helped in this. The IRA's "Being Patriotic" page targeted Americans opposed to expanding refugee settlements; a "Secured Borders" page propagated anti-immigration and anti-Muslim messaging; "Texas Rebels" promoted Texas's independence from The Union; and different sites mimicked Black Lives Matter. In a related tactic the IRA would frame a group, or politician, such as Clinton, as a threat. Some research suggests that emotions and emotional arousal (discussed below) can help create or enforce group boundaries and identifications.[95]

[86] Harkins, Stephen G., and Richard E. Petty. "The Multiple Source Effect in Persuasion: The Effects of Distraction." *Personality and Social Psychology Bulletin* 7, no. 4 (December 1, 1981): 627–35. https://doi.org/10.1177/014616728174019.p.627

[87] Chivvis, Christopher. *Understanding Russian "Hybrid Warfare": And What Can Be Done About It*. RAND Corporation, 2017. https://doi.org/10.7249/CT468.p.3

[88] "The Multiple Source Effect in Persuasion: The Effects of Distraction - Stephen G. Harkins, Richard E. Petty, 1981." Accessed April 14, 2021. https://journals.sagepub.com/doi/10.1177/014616728174019.

[89] Petty, Richard E., John T. Cacioppo, Alan J. Strathman, and Joseph R. Priester. "To Think or Not to Think: Exploring Two Routes to Persuasion." In *Persuasion: Psychological Insights and Perspectives, 2nd Ed*, 81–116. Thousand Oaks, CA, US: Sage Publications, Inc, 2005.

[90] Lewandowsky, Stephan, Ullrich K. H. Ecker, Colleen M. Seifert, Norbert Schwarz, and John Cook. "Misinformation and Its Correction: Continued Influence and Successful Debiasing." *Psychological Science in the Public Interest*, September 17, 2012. https://doi.org/10.1177/1529100612451018.p.108

[91] Paul, Christopher, and Miriam Matthews. *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*. RAND Corporation, 2016. https://doi.org/10.7249/PE198.

[92] Leor Zmigrod, "A Psychology of Ideology: Unpacking the Psychological Structure of Ideological Thinking" (PsyArXiv, September 4, 2020), https://doi.org/10.31234/osf.io/ewy9t; Leor Zmigrod et al., "The Psychological Roots of Intellectual Humility: The Role of Intelligence and Cognitive Flexibility," *Personality and Individual Differences* 141 (April 15, 2019): 200–208, https://doi.org/10.1016/j.paid.2019.01.016; "Cognitive Underpinnings of Nationalistic Ideology in the Context of Brexit | PNAS," accessed June 1, 2021, https://www.pnas.org/content/115/19/E4532.short.

[93] Yoshihisa Kashima et al., "Ideology, Communication and Polarization," *Philosophical Transactions of the Royal Society B: Biological Sciences* 376, no. 1822 (April 12, 2021): 20200133, https://doi.org/10.1098/rstb.2020.0133.

[94] Bernard Rimé, "Emotions at the Service of Cultural Construction," *Emotion Review* 12, no. 2 (April 1, 2020): 65–78, https://doi.org/10.1177/1754073919876036.

[95] Yoshihisa Kashima, Paul G. Bain, and Amy Perfors, "The Psychology of Cultural Dynamics: What Is It, What Do We Know, and What Is Yet to Be Known?," *Annual Review of Psychology* 70, no. 1 (2019): 499–529, https://doi.org/10.1146/annurev-psych-010418-103112.

Emotional Arousal

IRA messaging often sought to stir emotions such as fear and anger but trolls also used feelgood messaging to attract audiences.[96] Marketers often design campaigns to elicit certain emotions, e.g., fear, love, regret. Emotional narratives are incredibly powerful and strongly engage audiences.[97] The IRA used this to its advantage; when campaigns invoked anger and fear audiences were more engaged.[98] Some research links emotional content to virality.[99]

Information Overload

The IRA appeared to deliberately employ repetitive messaging (amplified by bots) to produce an overwhelming amount of information. Depending on the audience, the content aimed to confuse, distract, or exhaust, and to disable the ability (and will) of an individual to distinguish between factual and misleading or false information. This is often referred to as information overload or cognitive overload. When an individual is exposed to information beyond the limits of their processing ability, their decision-making is impaired, and they can be rendered confused and vulnerable to influence.[100]

[96] DiResta et al., "The Tactics & Tropes of the Internet Research Agency"; Linvill and Warren, "That Uplifting Tweet You Just Shared?" DiResta et al., "The Tactics & Tropes of the Internet Research Agency"; Linvill and Warren, "That Uplifting Tweet You Just Shared?"

[97] Chethana Achar et al., "What We Feel and Why We Buy: The Influence of Emotions on Consumer Decision-Making," *Current Opinion in Psychology*, Consumer behavior, 10 (August 1, 2016): 166–70, https://doi.org/10.1016/j.copsyc.2016.01.009.

[98] Chris J. Vargo and Toby Hopp, "Fear, Anger, and Political Advertisement Engagement: A Computational Case Study of Russian-Linked Facebook and Instagram Content," *Journalism & Mass Communication Quarterly* 97, no. 3 (September 2020): 743–61, https://doi.org/10.1177/1077699020911884.

[99] Jonah Berger and Katherine L. Milkman, "What Makes Online Content Viral?," *Journal of Marketing Research* 49, no. 2 (April 1, 2012): 192–205, https://doi.org/10.1509/jmr.10.0353; Bernard Rimé, "Emotions at the Service of Cultural Construction," *Emotion Review* 12, no. 2 (April 1, 2020): 65–78, https://doi.org/10.1177/1754073919876036.

[100] "Metzger, Miriam J., and Andrew J. Flanagin. "Credibility and Trust of Information in Online Environments: The Use of Cognitive Heuristics." *Journal of Pragmatics*, Biases and constraints in communication: Argumentation, persuasion and manipulation, 59 (December 1, 2013): 210–20. https://doi.org/10.1016/j.pragma.2013.07.012.

SYSTEMS AND TECHNOLOGY

SUMMARY OF FINDINGS

“Off-the-shelf” online technologies, including third party software and native tools (e.g., Google and Facebook analytics) for social media analytics, audience segmentation, targeting, and content development and dissemination. These included:

- Social media advertising systems (e.g., Facebook Ads Manager, Google AdSense).
- Bots and botnets to amplify accounts, messaging and content, and to help with other tasks (e.g., growing audiences).
- VPN hosted on US servers to hide traffic origin.

IRA workforce requirements included[101]:

- Management and financial skills (top level managers).
- Intelligence gathering/analysis skills (managers and operators undertaking physical or online intelligence gathering missions).
- Cultural knowledge of target audiences (managers conducting social listening and creating tasking briefs, as well as trolls).
- Basic to advanced computer/internet skills, depending on an operative’s role.
- Linguistic skills (intermediate to advanced knowledge of a target audience’s language).
- Medium level technical skills to create/operate bots/botnets.
- Web programming skills.
- Digital marketing skills - knowledge of social media KPIs (Key Performance Indicators), social media analytic and social listening skills, content development, desktop publishing and audio visual skills, search engine optimisation skills, social media analytics, etc.
- Basic understanding of principles of psychological persuasion.
- Ability to think critically and creatively to produce meaningful, manipulative messaging.

STRENGTHS AND WEAKNESSES

Strengths

- Ability of human trolls to creatively generate engaging content and messaging.
- Influence operations required complex cultural, linguistic, cognitive (e.g. critical thinking) and creative (e.g. digital and social media marketing) skills. The IRA’s ability to hire a large cohort of relatively low-paid workers with these skills was a key strength of its operation.
- Ability to leverage the new opportunities provided by social media platforms in terms of data harvesting and micro targeting.

[101] Jane Lytvynenko, “Here Are Some Job Ads For The Russian Troll Factory,” BuzzFeed News, 2018, https://www.buzzfeednews.com/article/janelytvynenko/job-ads-for-russian-troll-factory; “U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-Cr-32),” February 16, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere; “US District Court Criminal Complaint against Elena Khusyaynova” (U.S. District Court: Eastern District of Virginia, September 28, 2018).

- Ability to deploy a large number of bots (estimates range from 25,000-50,000) to amplify messages and narratives.
- Ability to use off-the-shelf software and tools to analyse data, segment populations, and manage social media messaging and content.
- Understanding of best practice digital marketing tools and techniques for creating content, websites, and messaging.
- Understanding of basic psychological principles related to persuasion and messaging.

Weaknesses

- May not have made maximum use of advertising tools available on social media platforms such as Facebook.
- Reliance on false identities and bots made influence campaigns subject to takedowns as social media companies became aware of these activities.
- Linguistic weakness (grammar mistakes made by Russian speaking ESL trolls were a key factor in identifying some accounts).

HUMAN INTELLIGENCE

Workforce Skills

In planning and carrying out its influence operations the IRA relied on a reasonably skilled workforce using off-the-shelf technology to conduct influence operations, as well as analysis and sensemaking, and to maintain situational awareness in the information environment.

For example, IRA operatives had to use (and technical operatives had to implement) VPN networks to hide their identity and location. Other operatives obtained fraudulent documents and stolen identities purchased with cryptocurrency; these allowed the IRA to establish and operate hundreds of US based email accounts, establish PayPal accounts, purchase political advertising, and operate false persona social media accounts for long periods without detection.[102]

The IRA also needed operatives with skills in graphic and audio visual tools and software to produce content for these platforms, ranging from visual memes to videos for YouTube.[103] At management level, social media analytic and monitoring platforms, as well as tools provided by platforms such as Facebook for Business, were used for situational awareness, sensemaking, audience segmentation and to assist in producing the daily tasking briefs trolls received to guide their online commentaries, blog posts and other content. Many of these tools can schedule content across multiple platforms and it is likely the IRA made use of these features as well. Additionally, the IRA made extensive use of automated accounts, or ‘bots’, to develop audiences and amplify content.

The IRA had a corporate, hierarchical structure, and a management team and departments. Job listings posted on Russian social media show it recruited for skills such as web programming (html CSS, JavaScript and PHP) and fluent English (including a "strong command of the written language, and creativity”).[104] A slightly higher paying

[102] U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-cr-32), 16 February 2018

[103] DiResta et al., “The Tactics & Tropes of the Internet Research Agency.”

[104] “RBC Investigation: How the ‘Troll Factory’ Worked in the US Elections (Расследование РБК: Как «фабрика Троллей» Поработала На Выборах в США),” Журнал РБК, 2017, https://www.rbc.ru/magazine/2017/11/59e0c17d9a79470e05a9e6c1.

position was “Social Media Specialist”. Here a candidate would need to grow social media audiences/followings and monitor the growth of online groups.[105]

Tasking Briefs

Top level managers developed strategic guidelines for trolls. These guidelines, referred to internally as “Briefs”, “Technical Tasks” or “Taskings”, outlined themes, topics, political events and social issues for particular focus. These taskings included “detailed analysis of timely news articles and guidance for how to describe the articles in social media”.[106] They included links to news articles trolls were to include in their posts. Taskings showed that management had a sound knowledge of the US media landscape, including conspiracy and partisan websites, to which trolls directed traffic. Management issued specific directions, e.g, “If you write posts in a conservative group, do not use Washington Post or BuzzFeed's titles”.[107] According to the US Justice Department, “Members of the Conspiracy were directed to create political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements”. The Conspiracy also sought, in the words of one IRA member, to “effectively aggravate the conflict between minorities and the rest of the population”.[108]

The taskings provided guidance to trolls on how to effectively aggravate tensions between different social and political groups and listed “hot-button” social issues that would best inflame existing tensions. The taskings even provided details of which infographics, phraseology and timing would make a post work most effectively within a particular ethnic/social or political group. One set of instructions suggested liberals were more active at night.[109] Managers were required to analyse news articles, summarise the key points, categorise its themes and provided trolls with a strategic response. A strategic response to a news article about the distinguished US senator and presidential candidate John McCain reads - “Brand McCain as an old geezer who has lost it and who long ago belonged in a home for the elderly”.[110]

Trolls

Trolls formed the backbone of the IRA’s workforce. Most were in their twenties, working 12-hour shifts (the IRA operated 24/7), generally five days a week.

In terms of their digital marketing skills, they were essentially social media content developers. As such, they had to have basic internet and social media skills, competent English and some basic marketing skills, which were likely acquired on the job. While they received daily tasking briefs identifying key targets and narratives, self-motivation and creativity were essential to meeting the daily requirements. Trolls were required to create multiple blogs and longer posts each day (political and non-political), and post hundreds of comments on posts by other trolls.

Social Media Fluency

Trolls were required to create, develop and manage multiple social media accounts on numerous platforms. They were required to create false personas and original content. They had to develop a social media presence, drive engagement and establish a following. These responsibilities required more than technical computer skills. Trolls

[105] Jane Lytvynenko.
[106] “US District Court Criminal Complaint against Elena Khusyaynova.”
[107] “US District Court Criminal Complaint against Elena Khusyaynova.”
[108] “US District Cournt Criminal Complaint against Elena Khusyaynova.”
[109] “US District Court Criminal Complaint against Elena Khusyaynova.”
[110] “US District Court Criminal Complaint against Elena Khusyaynova.”

needed, at a minimum, social media literacy – and fluency – across multiple platforms. They needed an understanding of platform dynamics, i.e., which content worked on which platforms. They also needed basic research skills, to develop a cultural understanding of their target audience, and the ability to use their online "voice" to communicate authentically. They also needed the ability to change their tone of voice to suit different audiences and operate different accounts/personas. A former employee described how she "kept up several blogs…juggling the virtual identities of a housewife, a student and an athlete".[111]

Cultural Knowledge

Trolls were also required to create believable personas and engage with a native audience daily. As said, this required cultural and linguistic knowledge of their target audience. Tasking briefs outlined key events/issues and talking points trolls had to adhere to. However, it was a troll's responsibility to develop an online persona that interacted with genuine individuals, infiltrated groups and, in some cases, recruited unwitting assets. Trolls had to develop not only a sound knowledge of the political landscape of their target country but, also, a sound knowledge of its social dynamics and cultural values. It is important to note that only a fraction of the content (tweets, posts, etc.) was politically charged. The scope of messaging contained in the IRA's tweets can be viewed in this archive - https://russiatweets.com/. The tweets included football scores, jokes, rap lyrics, and comments on pop culture and celebrity.

DIGITAL TECHNOLOGIES

Bots And Botnets

Automated accounts, or bots, were a key technology used by the IRA to amplify its messaging and push its content across multiple channels/platforms. Bot technology gave the IRA a powerful force multiplier to amplify selected messaging and content to its target audience easily, quickly and relatively cheaply, e.g., by [112]leveraging online social media platforms "sharing functions and algorithms". This increased the visibility of IRA content and made it appear more popular, relevant and credible.[113]

A general distinction can be made between bots and social bots. Social bots mimic the social behaviour of a human social media user, while ordinary bots do not. Social bots have a number of capabilities, including the ability to perform social interactions, respond to questions and "generate debate by posting messages about trending topics".[114] The IRA utilised these capabilities to "simulate human behaviour on social media, which allowed them to believably and strategically interact with users and promote relevant content".[115] Social bots can harvest private users' personal data, such as email addresses and phone numbers.[116] Social bots were one of at least three tactics the IRA used to influence social media discourse.

- **Smoke Screening** – distracted and diverted the reader's attention from the core issues of a particular topic by using a hashtag such as #BLM to discuss trivial issues.

[111] Marina Koreneva, "Here's What It's like Being a Paid Internet Troll for the Russian Government," Business Insider, accessed June 3, 2021, https://www.businessinsider.com/afp-trolling-for-putin-russias-information-war-explained, 2015.

[112] Ethan Guge, "Targeted Disinformation Warfare: How and Why Foreign Efforts Are Effective, and Recommendations for Impactful Government Action," 2020.

[113] Ethan Guge.

[114] "How Is Fake News Spread? Bots, People like You, Trolls, and Microtargeting | Center for Information Technology and Society - UC Santa Barbara," accessed February 18, 2021, https://www.cits.ucsb.edu/fake-news/spread.

[115] Ethan Guge.

[116] Yazan Boshmaf et al., *The Socialbot Network: When Bots Socialize for Fame and Money*, *ACM International Conference Proceeding Series*, 2011, https://doi.org/10.1145/2076732.2076746.

- **Misdirecting –** was an extension of the previous tactic. Misdirecting used a hashtag such as #BLM but then discussed something completely unrelated.
- **Astroturfing –** used false personas and front organisations to create the illusion of a grassroots movement and the sense that a large number and/or most people supported its viewpoint.[117]
- **Social bots-** were generally partially controlled by a 'bot master' as part of a network, and their creation and control required medium level technical expertise. [118]

Estimates of the number of bots used to amplify IRA messaging during the 2016 US election influence campaign range from 36,000-50,000.[119] Whether the IRA designed and developed, or purchased and repurposed, most of the bots is unknown. However, Burchik, one of the 13 IRA employees indicted by the US Department of Justice, was a tech entrepreneur who had previously developed his own amplification software. Burchik would likely have had the skills to create bots and botnets.

Bots used by the IRA performed technically simple amplification tasks, such as liking or sharing content, and could be created with simple, freely available, off-the-shelf software.[120] And, while some social bots did have limited AI capabilities, it appears the IRA chose not use them. However, social bots with more advanced AI, which can potentially remain undetected on social media platforms, will likely be an emerging threat in future influence operations. [121]

Social Media Environment

The technological innovations and developments of the online information environment gave the IRA new opportunities to design and implement fast, cheap, easy influence campaigns across multiple platforms. Native features of online social media platforms, including behavioural data tracking, allowed the IRA to target specific audiences.

Furthermore, systems and technology that enabled the IRA to persuade target audiences were also largely built into the platforms. They included algorithmic design, social media management services and behavioural data tracking, and were key to helping the IRA achieve its objectives. These systems and technology helped the IRA to design messaging, identify target audiences and disseminate information to the right people at the right time. Thus, the IRA exploited the systems and technologies of social media platforms, a readily available "ecosystem of digital advertising and marketing technologies".[122]

Platforms like Facebook offer a range of services (e.g., Audience Insights) that give advertisers an insight into audience demographics, behaviour and interests. These can be used to plan campaigns, develop targeted content, and monitor audience engagement. The IRA most likely made use of these in-built data collection features and targeting capabilities. Facebook for Business, for example, is essentially a how-to-guide to running a successful online advertising campaign (legitimate commercial influence), with numerous analytic and social listening tools. These same tools can be used to carry out malign influence operations. Such features, and "data-

[117] "AGUK_CommunicationSnapshot_SocialBots_June2018.Pdf," accessed April 7, 2021, https://www.akademischegesellschaft.com/fileadmin/webcontent/Publikationen/Communication_Snapshots/AGUK_CommunicationSnapshot_SocialBots_June2018.pdf.

[118] Dennis Assenmacher et al., "Demystifying Social Bots: On the Intelligence of Automated Social Media Actors," *Social Media + Society* 6, no. 3 (July 2020): 205630512093926, https://doi.org/10.1177/2056305120939264.

[119] "U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-Cr-32)"; "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections."

[120] Assenmacher et al.

[121] Assenmacher et al.

[122] Dipayan Ghosh and Ben Scott, "Digital Deceit."

driven" advertising, allowed the IRA to first identify, then home in on vulnerable target audiences.[123] This is evident in its geographically targeted advertising in swing states, and its politically targeted advertising designed to dissuade people from certain ethnic communities from voting. These features also gave the IRA an opportunity to experiment with multiple variations of ads and trial different targeting frameworks, to assess which messaging received "optimal engagement".[124] While it is clear the IRA utilised advertising and analytic services, and other features offered by Google and Facebook, it is likely - but not known for sure - it also employed the services of information technology companies, including data brokers, to gain further insights.

Data Analytics Software and Tools

The IRA used off-the-shelf social media management and analytic tools and took advantage of tools native to social media platforms. The US Department of Justice, for example, outlines an IRA IT expenses budget that includes the purchase of social media analytic and optimisation software, such as Twidium and Novapress.[125]

The IRA also exploited existing technological features built into social media platforms to amplify their influence campaign.[126] Social media platforms design algorithmic recommendation systems that reward and promote sensational content.[127] The IRA leveraged such technological features to disseminate messaging and exacerbate political polarisation. IRA messaging was often sensational. The aim was to elicit a strong emotional response, to garner a "share" or "like", thereby signalling to recommendation algorithms that the message was worth disseminating more widely.[128] The IRA took advantage of this feature on YouTube by linking to YouTube videos in its tweets.[129]

Additionally, online platforms' data collection and targeting capacities allowed the IRA to "experiment with different targeting parameters".[130] Every social media platform has a system to record online behaviour. The information is then used to build consumer profiles. The IRA exploited these features to disseminate relevant messaging to its target audiences.[131]

It is also likely, given it had a search engine optimisation (SEO) department, the IRA engaged in behaviour designed to boost the rank of a page, or content known collectively as "black hat SEO". Black hat SEO can trick search engine algorithms into promoting content for a few hours within a news cycle before Google (or other search engines) 'catch on' and correct the skewed results. This behaviour violates search engine terms and conditions but was widely used by disinformation operators.[132]

[123] Osservatorio Balcani e Caucaso, "Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech," Media Freedom Resource Centre OBCT, 2018,

[124] Caucaso.

[125] "US District Court Criminal Complaint against Elena Khusyaynova."p.9

[126] F. Saurwein and C. Spencer-Smith, "Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe," *Digital Journalism* 8, no. 6 (2020): 820–41, https://doi.org/10.1080/21670811.2020.1765401.p.823 Saurwein and Spencer-Smith.p.823

[127] Nicholas Thompson, "Inside Facebook's Two Years of Hell," *Wired*, 2018, https://www.wired.com/story/inside-facebook-mark-zuckerberg-2-years-of-hell/.

[128] Saurwein and Spencer-Smith, "Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe.", 2020

[129] Yevgeniy Golovchenko et al., "Cross-Platform State Propaganda: Russian Trolls on Twitter and YouTube during the 2016 U.S. Presidential Election," *International Journal of Press/Politics* 25, no. 3 (July 2020): 357–89, https://doi.org/10.1177/1940161220912682.

[130] Ethan Guge, "Targeted Disinformation Warfare: How and Why Foreign Efforts Are Effective, and Recommendations for Impactful Government Action.", 2020

[131] Dipayan Ghosh and Ben Scott, "Digital Deceit: The Technologies Behind Precision Propaganda on the Internet," New America, 2018, http://newamerica.org/pit/policy-papers/digitaldeceit/.

[132] Dipayan Ghosh and Ben Scott, "Digital Deceit."

Thus, by leveraging sophisticated analytic technology readily available on the open market (and often provided by social media platforms), the IRA was able to engage with target audiences to maximise its messaging. The consumer segmentation and social listening software/technologies allowed the IRA to carefully curate messages for either side of an issue. Furthermore, these consumer data analytics identified exactly which divisive political and social issues were most vulnerable to the strategies and techniques of "wedge politics".[133]

[133] Matt Peterson and Abdallah Fayyad, "The Irresistible Effectiveness of Wedge Politics - The Atlantic," 2017, https://www.theatlantic.com/membership/archive/2017/12/the-irresistible-effectiveness-of-wedge-politics/547946/.

CAMPAIGN AWARENESS AND SENSEMAKING

SUMMARY OF FINDINGS

- The availability of online data and tools for targeting and situational awareness was an enormous resource, providing the IRA with most of the intelligence it needed to conduct influence operations.
- The IRA conducted "social listening" to identify key narratives, events, audiences, influencers and content using social media analytic tools including:
- Off-the-shelf social media analytic and management software, such as Twidium and Novapress.
- Advertising, content development and analytic tools provided by social media platforms, including Facebook Advertising and Google Adwords.
- The IRA used digital marketing metrics, such as awareness and reach, to monitor its campaigns. However, research on these metrics and monitoring techniques is limited, and the subject of debate.
- The IRA also conducted physical intelligence gathering operations/espionage (at least in some instances).

STRENGTHS AND WEAKNESSES

Strengths

- The IRA took advantage of existing digital marketing sensemaking and situational awareness techniques (and technology) to identify and target audiences, and to target and amplify cultural and political divisions, etc.
- The IRA tracked public and audience interests and opinions using off-the-shelf software and tools, and established digital marketing techniques. These methods and tools combined qualitative and quantitative analysis.
- The IRA monitored its own activities using these same tools and techniques, and digital marketing metrics to monitor and adapt their own influence campaigns.

Weaknesses

Digital marketing metrics and existing social media qualitative/quantitative analytic methods are generally used in ad hoc ways when applied to influence campaign sensemaking, and may not reliably predict or reflect the relationship between online and offline behaviour, changes in attitudes, changes in beliefs, etc.

ONLINE

As discussed, the availability of online data and tools for targeting, sensemaking and situational awareness was an enormous resource for the IRA. It used off-the-shelf, third-party social media analytic software and tools, including Twidium and Novapress, as well as tools provided by the social media platforms themselves, such as Facebook Advertising and Google Adwords.[134] These tools allowed the IRA to segment the population into discrete audiences, and micro target these audiences' using demographic, behavioural and attitudinal data.

[134] "U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-Cr-32)," February 16, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-

These tools also meant the IRA could monitor and track its own activities, using standard digital marketing metrics such as awareness (also called reach), the number of individuals who had seen content, and their engagement, e.g., the number of likes, shares, comments and similar interactions that content or messaging receives.[135] Combining and analysing metrics such as engagement and awareness would have helped build a picture of the performance and impact of IRA influence operations. (Impact is here defined as a measurable change in an audiences' knowledge, attitudes, or behaviour, offline or online.)

Measuring the impact (as stated above, any measurable change in an audience's attitudes, behaviour, or knowledge, as the result of engagement or exposure to a campaign) of an influence operation is complex and, at least for now, imperfect. It is often an ad hoc process, as much an art as a science. Performance also depends on a campaign's goals;[136] as this report points out, the IRA had goals that cannot be simply reduced to changes in voting behaviour or, indeed, other offline behavioural changes. Many of its goals seem to have been oriented towards attitudes and sentiment (sowing discord, amplifying negative attitudes, polarisation and so on), and this is not unusual for influence operations. Moreover, tactically speaking, these goals changed over time – e.g, undermining Clinton when it appeared she might win the presidency.[137] Additionally, as previously stated, the IRA was just one part of a much larger influence and propaganda ecosystem serving Russia's long-term strategic goals.

Social media metrics such as reach and engagement provide important insights but are at best proxies for impact, and prone to manipulation. Other indicators of impact include adapted digital marketing metrics, like "share of voice". These attempt to measure the amount of conversation within a specific audience dominated by messaging from an influence operation. Tracking specific artefacts (memes, videos and so on) used by an influence operation can also provide insights into an operation's impact. For example, the IRA watermarked images and memes in its campaigns (until it became a way for the platforms to track and remove IRA accounts). It seems likely that this was also used by the IRA to track the spread of, and engagement with, this content.

Moreover, digital marketing tools were not designed to assess the impact of influence campaigns on geopolitical dynamics. Additionally, there does not appear to be consensus among social scientists on the best way to measure, or establish the impact of, influence operations given the complex social systems in which they occur (and the various time scales in which they operate). Nevertheless, there are efforts to establish better methods of sensemaking and assessing influence campaigns.[138] And, while disentangling causality between offline and online behaviour is difficult, there is generally a correlation between online and offline activism; this suggests that if an influence campaign can increase activism online, there may be more activism offline (in the case of influence activities, this may include calls for violence and insurrection).[139]

interfere; Renee DiResta et al., "The Tactics & Tropes of the Internet Research Agency," 2019, https://digitalcommons.unl.edu/senatedocs/2.

[135] Louis Reynolds and Henry Tuck, "The Counter-Narrative Monitoring & Evaluation Handbook" (Institute for Strategic Dialogue), accessed February 8, 2021, https://www.isdglobal.org/isd-publications/the-counter-narrative-monitoring-evaluation-handbook/.

[136] Louis Reynolds and Henry Tuck, "The Counter-Narrative Monitoring & Evaluation Handbook" (Institute for Strategic Dialogue), accessed February 8, 2021, https://www.isdglobal.org/isd-publications/the-counter-narrative-monitoring-evaluation-handbook/.

[137] "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections" (Office of the Director of National Intelligence, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[138] Ben Nimmo, "The Breakout Scale: Measuring the Impact of Influence Operations," 2020, 15; "Influence Campaign Awareness and Sensemaking," accessed June 18, 2021, https://www.darpa.mil/program/influence-campaign-awareness-and-sensemaking.

[139] Hedy Greijdanus et al., "The Psychology of Online Activism and Social Movements: Relations between Online and Offline Collective Action," *Current Opinion in Psychology*, Social Change (Rallies, Riots and Revolutions), 35 (October 1, 2020): 49–54, https://doi.org/10.1016/j.copsyc.2020.03.003.

Imperfect as they are, the IRA used digital marketing metrics, as well as qualitative and quantitative methods, to gain situational awareness, and to measure the performance of an operation,[140] probably because they were the best tools available. Other indicators, such as whether IRA messaging 'broke out' (i.e., was picked up by mainstream media or key 'influencers'), or online influence activities succeeded in producing real world outcomes (such as rallies), were likely also used to assess the performance and impact of campaigns.[141] This is in step with Soviet active measures, where performance indicators included the degree to which campaign narratives were picked up by the 'mainstream' media, or became part of the political discourse (e.g, as with the KGB's AIDS Disinformation campaign).[142]

IRA managers also conducted what digital marketers call 'social listening' to identity key narratives, events, audiences, influencers and content, and used this information to develop tasking briefs to guide trolls in posting comments, creating blogs and spreading content online through sock puppet personas. As early as 2014, high ranking operatives in the IRA's American Department tracked and observed the metrics of various social movements and affinity groups, or 'tribes', in the US, presumably to identify effective messaging and to inform the IRA's operations generally.[143] Digital ethnographic (or netnographic) methods are another way qualitative and quantitative methods can be used to gain an understanding of audiences and their interactions with certain content, and it is possible the IRA used some of these techniques (which overlap with but are generally more rigorous than social listening).[144]

These activities amounted to online intelligence gathering, via sensemaking and the establishment of situational awareness. Intelligence gathering operations also included the study of US political groups on social media, as well as groups dedicated to social causes. It should be noted, however, as stressed previously, the use of digital marketing and other techniques for campaign sensemaking is more art than science, and it is likely senior IRA managers used them in an ad hoc manner.

OFFLINE

As mentioned above, in addition to online intelligence gathering, the IRA engaged in physical intelligence gathering, in the US and Europe. Less is known about its European activities but there is evidence to suggest that an IRA employee undertook intelligence gathering around the Greek EU Parliamentary elections in 2014, in what appears to have been an attempt to identify security weaknesses.[145]

According to the US Department of Justice, an intelligence gathering mission to inform the IRA's influence campaign against the US took place in June 2014. Senior employees of the IRA, Aleksandra Krylova and Anna

[140] "U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-Cr-32)," February 16, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.

[141] Ben Nimmo, "The Breakout Scale: Measuring the Impact of Influence Operations," n.d., 15; Louis Reynolds and Henry Tuck, "The Counter-Narrative Monitoring & Evaluation Handbook" (Institute for Strategic Dialogue), accessed February 8, 2021, https://www.isdglobal.org/isd-publications/the-counter-narrative-monitoring-evaluation-handbook/.

[142] Douglas Selvage, "Operation 'Denver': The East German Ministry of State Security and the KGB's AIDS Disinformation Campaign, 1985–1986 (Part 1)," *Journal of Cold War Studies* 21, no. 4 (October 1, 2019): 71–123, https://doi.org/10.1162/jcws_a_00907; Mirela Silva et al., "Facebook Ad Engagement in the Russian Active Measures Campaign of 2016," 2020, https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edsarx&AN=edsarx.2012.11690&site=eds-live&scope=site&custid=s2775460.

[143] "U.S. v. Internet Research Agency LLC, et al (U.S. District Court for the District of Columbia; 1:18-Cr-32)."

[144] Robert V. Kozinets, "Netnography," in *The International Encyclopedia of Digital Communication and Society* (American Cancer Society, 2015), 1–8, https://doi.org/10.1002/9781118767771.wbiedcs067.

[145] "The Internet Research Agency In Europe 2014-2016.Pdf."

Bogacheva, went on a three-week intelligence gathering mission in the US, focusing on key electoral states. The operatives used burner phones and sims, and had an evacuation plan in the event their operation was compromised. They compiled a report on American politics and submitted it to their superiors in St Petersburg.[146] Bogacheva was in charge of data analysis in the IRA's American Department, while Krylova was the IRA's third-highest ranking employee, with advertising and public relations experience.[147] It is unknown whether they were working for the GRU, SRV or another intelligence agency in Russia prior to, or during, their time at the IRA, or had received training/advice on how to carry out their mission from Russian intelligence. We can surmise they received advice on operational security and procedures (such as evacuation plans), and it is also possible they met with, and received assistance from, US-based Russian intelligence agents.

Although the IRA did conduct traditional intelligence gathering operations on the ground, most of the intelligence they needed was available online. The systems and technologies the IRA accessed and utilised gave them insight into US citizens' behaviours, preferences and beliefs, allowing them to design and execute sophisticated campaigns to great effect. The readily available insights gained through social media platforms' systems and technologies helped the IRA develop their operations. This meant that, for the most part, the IRA didn't need highly trained employees to design and operate state of the art systems, or run expensive and risky intelligence operations on the ground. Most of the data they needed had already been gathered, sorted and packaged ready for use.

OBSERVATIONS AND TRENDS

While the term IRA is, as previously stated, sometimes loosely used to describe Russian online influence campaigns generally, this study focused on a specific period, between 2013 and 2018, when the entity known as the IRA, and based for most of this time at 55 Savushkina St, St Petersburg, was in operation. However, Russian influence operations did not begin during this period and did not end with it.

Russia's deployment of online influence operations is considered successful, cheap, plausibly deniable and an equaliser against the West. Russia will continue to adapt, evolve and deploy them (as will others). The IRA (and its reincarnations/clones) were revolutionary in the way they conducted influence operations, particularly in the way the mobilised a human workforce, existing technological resources and the Soviet era disinformation 'playbook', to take advantage of new possibilities in the emerging social media ecosystem and information environment.

- Russia is using the IRA's business model to create "pop-up influence shops" (e.g., in Ghana).
- Key ingredients - access to internet, workers with adequate knowledge of target audience language/culture.
- Other state and non-state actors are learning from/adapting IRA techniques for their own influence operations.[148]
- The legal, ethical, social and political environment surrounding influence operations is changing rapidly and Russia's (and other state and non-state actors') tactics continue to evolve.

[146] "U.S. v. Internet Research Agency LLC, et al

[147] "U.S. v. Internet Research Agency LLC, et al; Ivan Nechepurenko and Michael Schwirtz, "What We Know About Russians Sanctioned by the United States," *The New York Times*, February 17, 2018, sec. World, https://www.nytimes.com/2018/02/17/world/europe/russians-indicted-mueller.html.

[148] Jacob Wallis Cave Tom Uren, Elise Thomas, Albert Zhang, Samantha Hoffman, Lin Li, Alexandra Pascoe, Danielle, "Retweeting through the Great Firewall," accessed June 12, 2020, https://www.aspi.org.au/report/retweeting-through-great-firewall.

- For example, as social media platforms get better at detection, there has been a shift away from amassing large followings, towards the use of (witting or unwitting) freelancers and proxy media outlets, many of which have ties to Russian intelligence services.[149]
- As social media platforms improve their ability to track and take down accounts involved in influence campaigns (coordinated inauthentic behaviour), they are unlikely to differentiate between campaigns undertaken by Western countries and their adversaries, when/if the campaigns rely on false identities and sock puppet accounts.
- For example, a French influence operation targeting audiences in Francophone Africa, and in some cases 'duelling' with Russian influence operations, was taken down by Facebook and linked (by Facebook) to individuals associated with the French military.[150]
- The availability of big data through social media platforms and third-party data brokers is a problem but also an opportunity.
- Accessing it will require clear ethical and legal standards and guidelines.
- The use of organised influence operations forces/proxies (such as the IRA) for online influence is a widespread, rapidly evolving, global phenomenon.
- Influence operations forces are a threat but also an opportunity.
- Western allies operate "influence operations forces" (e.g., UK anti-radicalisation).[151]

RECOMMENDATIONS

JIA asked for recommendations regarding future capabilities in relation to the four, agreed-upon thematic questions addressed in this report. The report includes recommendations for the Department of Defence, under the themes developed in consultation with the JIA:

Governance, Code of Practice, Ethics, And Legitimacy

- Establish principles, codes of conduct and rules of engagement for information operations that:
- Align with and protect Australia's democratic principles and values.
- Accord with Australian Government policies and international treaties to which Australia is a signatory.
- Consider differences between defensive and offensive capabilities and operations.
- Have the flexibility to conduct effective operations and to develop new capabilities that respond to rapidly evolving threats in the information environment.

Workforce Composition

- Train, recruit and develop a multidisciplinary, creative and innovative workforce that retains these qualities through a program of continuing education.
- Train and/or recruit the complex cultural, linguistic, cognitive and creative skill sets required for information operations.

[149] Snegovaya and Watanabe, "The Kremlin's Social Media Influence Inside the United States."

[150] Nathaniel Gleicher and David Agranovich, "Removing Coordinated Inauthentic Behavior from France and Russia.", 2020

[151] Scanzillo, Thomas M, and Edward M Lopacienski. "Influence Operations and the Human Domain," United States Naval War College, 2015. https://www.hsdl.org/?view&did=814708

- Establish multidisciplinary teams to survey international, Western democratic allied countries to determine best practice, and develop the methods, tools and equipment to detect, deter and defend against malign influence operations, and shape the information environment.
- Information operations require complex cognitive and creative capabilities as well as technical skills. Human operators will be an essential component for the foreseeable future. Defence should:
- Ensure the cultural/linguistic, cognitive (e.g., critical thinking) and creative (e.g., digital marketing) skills required for defending against and conducting influence operations are adequately trained/recruited for.
- Develop a flexible workforce planning system to ensure Australia has a sustainable workforce with the right skills for information operations.
- Establish multidisciplinary teams to survey emerging international, best practices/techniques, and the equipment, tools, resources, people and skills for defending against, and conducting, information operations.
- Coordinate an information operations ecosystem with Defence, intelligence and non-government expertise.
- Experiment with organisational structures and processes to ensure agility (speed, flexibility, innovation) in influence operations.

Measuring Campaign Impact And Effectiveness

- Develop and implement campaign situational awareness techniques that combine quantitative and qualitative methods for population mapping and monitoring social media activities, including influence operations.
- Consider using multidisciplinary academic teams to identify, develop and conduct training in these methods.
- Digital ethnographic research is a promising technique for gaining situational awareness in the information environment, for monitoring social media for malign influence operations, and for gaining critical insights into populations and audiences. Consider using multidisciplinary teams to adapt and expand this research and related methodologies (e.g., social listening) to gain situational awareness in the information environment.
- Establish metrics and indicators.
- Metrics and indicators to assess information operations is a rapidly evolving field involving cutting edge research in academia, government and industry.
- Consider forming multidisciplinary academic teams to survey existing metrics and indicators, and identify their strengths and weaknesses in measuring the impact and effectiveness of information operations.
- Consider using multidisciplinary teams to develop new metrics and indicators, and methods for monitoring and measuring the complex causal relationship between offline and online behaviour.

Technology

- Use off-the-shelf third party and native tools/capabilities to monitor the social media environment, including key groups and individuals. If required, develop customised responses.
- Consider bringing academia and industry together to:
  - Translate academic capabilities including technological and human resources, skills and expertise into commercially viable products, and
  - Cultivate academic and industry capabilities to create relevant technologies and human resources.

- Conduct horizon scanning relating to advancing technologies to maintain awareness of evolving platforms and countering techniques.

Interoperability

- Engage with Australia's Five-Eyes partners (and other allies) on information operations and joint forces interoperability. Where possible and appropriate, coordinate with these partners to develop capabilities and doctrines for information operations.
- Engage with regional partners in the Indo-Pacific to increase resilience to malign or hostile information operations and to boost, where possible and appropriate, local capabilities in the information environment.

CONCLUSION

This report provides an overview of the IRA in the context of the Russian influence operations ecosystem. It focuses on the strengths and weaknesses of the IRA as a state sponsored entity that perpetrated information operations. It is framed around four key themes, Governance and Ethics, Persuasive Technology and Techniques, Systems and Technology, and Campaign Awareness and Sensemaking, and addresses the associated research questions. It shows that the IRA derived strength from its establishment as a digital marketing firm, contracted as a private military company to the Russian Government.

The IRA wasn't hamstrung by ethical considerations. It was free to act with ethical fluidity and this helped it drive its messaging to a large audience. The report shows the IRA's roughly 1000-strong workforce included people with varying competencies in social media, systems and technology, and persuasive techniques informed by psychology. The IRA relied heavily on established social media tools to conduct its large volume, high-speed messaging campaigns.

The report tracks the IRA's evolution in influence operations, developing tactics locally in the first instance, then applying what it had learnt to operations of a more strategic, geopolitical nature, including the 2016 US elections.

Based on the key findings, the report recommends that, as part of its emerging influence operations capabilities, the Department of Defence:

(i) Develop training regimes to establish an agile, innovative workforce, including people trained to scan the horizon for advancing technologies, to ensure ongoing awareness of evolving platforms and countering techniques.

(ii) Augment native tool sets with off-the-shelf, third-party tools to monitor social media, and identify vulnerable groups and individuals relevant to Australia's national interest.

(iii) Survey and develop methods for identifying, monitoring, and measuring the predictability, and complex relationship, between online and offline behaviour.

(iv) Develop an ecosystem combining Defence, intelligence, and non-government personnel to provide expertise across the full spectrum of operations.

(v) Engage with regional partners in the Indo-Pacific to increase resilience to malign or hostile information operations, and to increase, where possible and appropriate, local capabilities to combat this influence.

THE UNIVERSITY of ADELAIDE

THE UNIVERSITY OF MELBOURNE

UNSW

AUSTRALIA ECU EDITH COWAN UNIVERSITY

MACQUARIE University SYDNEY · AUSTRALIA