Spreading Lies Through the Cyber Domain

Thomas Dempsey
American Military University, Charles Town, USA

thomas.dempsey@mycampus.apus.edu

Abstract: The expansion of Information Operations (IO) over the past ten years has allowed individuals and groups to increase their sphere of influence on a global scale. Nation-state cyber threat actors have increased their presence on social media, building out false personas to influence large populations. This type of activity is difficult to stop due to the availability of social networks on the internet and the ease of creating false personas that can't be directly attributed to the actor. IO activity has been observed with the Russian cyber activity during the 2016 U.S. Presidential elections and from Russian social media campaigns provoking extremist groups and attempting to cause physical harm, such as the 2017 campaign on Facebook to start a rally and a simultaneous counter rally in front of the Islamic Da'wah Centre of Houston. Although Russia has been observed leveraging this capability, they are not the only global actor in the cyber domain taking advantage of IO. Global threat actors have leveraged social media platforms and blogs to influence the global population and spread propaganda. This type of activity has been seen within traditional warfare using propaganda techniques. With the introduction of the cyber domain into warfare, there is an increased ability to communicate not only to one population but to the global community with the intent to manipulate the masses using IO. This paper examines the Cybersecurity Operations (CO) that have been observed utilizing IO and the psychological impacts they have had in successful campaigns against the United States. This paper argues that with increased influence capabilities in the cyber domain, individuals and groups will continue using IO to support tactical and strategic objectives. Through the available literature, this paper examines the impacts that IO has had on the United States through attempts to manipulate elections and create divides in the nation over the last ten years. This paper leverages the psychology of group processes to analyze the literature involving social media campaigns and the influencing of groups through the lens of social identity theory to provide new insight into mitigating and countering IO.

Keywords: Information Operations, Disinformation, Cybersecurity Operations, Social Identity, Cyber, psychology

1. Introduction:

This research examines the question of what are the psychological impacts of disinformation and Information Operation campaigns on the population of the United States between 2012 and 2022? Unlike other time periods in U.S. history, there has been a significant increase in disinformation and Information Operations (IO) over the past ten years affecting the U.S. population. These IO campaigns against the United States have attempted to impact the U.S. elections and have been attributed to countries such as Russia, China, and Iran (Martin et al. 2022). The campaigns have spread disinformation regarding political parties and attempted to influence public opinion either for or against specific candidates in support of the nation-state's national objectives. This has been seen with the Russian campaigns supporting Trump in the 2016 elections and the 2018 midterm elections (Martin et al. 2022), along with attacking Hillary Clinton during the 2016 elections (Martin et al. 2022). With the increase of disinformation and IO campaigns, it is becoming important to understand the impact and effectiveness of these campaigns. This research examines the hypothesis that successful disinformation or IO campaigns will have a psychological impact on the target audience by manipulating the social identity by reinforcing an existing social-political standpoint or changing the social-political standpoint of the target audience.

The United States National Institute of Standards and Technology (NIST) defines Information Operations as "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO" (NIST 2022). In other words, Information operations are the use of information to influence an audience and can be used to shape perceptions and understanding of a targeted population to achieve the tactical or strategic goals of the executing party. Information operations have been around for a long time. During World War II, President Roosevelt established the U.S. Office of War Information (OWI), specifically tasked with information activity and propaganda in the U.S. and overseas (Roholl 2012). Altheide and Grimes (2005) argue that the Iraq war was a successful propaganda campaign in that the American public was not aware of the full context and that the storyline from the media was that Hussein was involved in the 9/11 attacks, he supported terrorism and planned to use Weapons of Mass Destruction (WMD) against the U.S. creating a sense of urgency to intervene.

Modern disinformation operations are achieved through social media platforms like Twitter and Facebook, along with other online forums like Reddit. With social media, there is a larger audience that can be accessed

throughout the internet, and information operations are easier to conduct. Social media has been growing exponentially, making it easier than ever to spread false information and have an impact on the population. During the 2022 U.S. midterm elections, social media platforms such as Telegram were used by Russian-associated hacktivist groups to claim Distributed Denial of Service (DDoS) attacks against political party websites and promote the narrative that Russia can influence the U.S. elections (Wahlstrom et al. 2022). The increased accessibility to information on the internet has made disinformation a significant problem in the information age. Information operations are not just about hacking or cyber warfare anymore. These operations use data to influence a target audience's emotions, beliefs, attitudes, and behaviours.

The United States is a target and instigator of disinformation campaigns that foreign actors carry out to support their national objectives. In a declassified 2021 Intelligence Community Assessment (ICA) on the foreign threats to the 2020 U.S. elections, it was identified that there were multiple information operations in the form of influence campaigns from foreign actors, including Russia, Iran, Lebanese Hizballah, Cuba, and Venezuela (National Intelligence Council 2021). These campaigns can have a profound psychological impact on the U.S. population. Due to the anonymity that can be achieved through social media, it can be difficult to track down those responsible for spreading disinformation. A greater understanding of the psychology behind the disinformation and its psychological impacts on the population is required to better prepare for the next attack. This paper will explore how the use of disinformation in information operations has become commonplace and what psychological impacts it has on people within the United States.

2. Literature Review:

The relevant literature regarding disinformation and information operations (IO) focuses on what is described as "fake news". Pathak et al. identify, "Disinformation intentionally attempts to mislead people into believing a manipulated narrative to cause chaos or, in extreme cases, violence." (Pathak et al. 2021). Pathak et al. argue that using manual processes, organizations cannot handle the speed required to verify or fact-check the volume of information being released and disseminated through the internet (Pathak et al. 2021). In the research, Pathak et al. show that through the use of natural language inference (NLI), there is promise in moving away from manual processes currently used for verifying fake news by implementing automated or semi-automated processes that can identify fake news and apply fact-checking capabilities (Pathak et al. 2021). Using automated processes to verify and fact-check fake news may be effective; however, there is no mechanism to identify the root source that distributed the content that would allow for attribution or identification of IOs. Rubin identifies that the ability to attribute news content to a source is critical when judging the content's credibility; with the news becoming increasingly available in decontextualized forms such as social media, it becomes even more difficult to identify the sources (Rubin 2019).

Tandoc et al. used a different method when evaluating fake news. They evaluated the characteristics of the fake news and what elements of the fake news were shared with legitimate news. The analysis from Tandoc et al. found, "The analysis showed that 98.6% of the articles analyzed included the news value of timeliness; 89.2% included the news value of negativity; 79.7% included the news value of prominence; but only 32% included the news value of impact." (Tandoc et al. 2021). In their study, it was also identified that topics about government and politics were among the highest percent of topics that consisted of fake news, with 51.6% of the analyzed news being related to these topics; terrorism or crime were the second highest topics, with 19.5% of content analyzed being related to these topics and science, health, and technology were in the lower percentages at around 10.3% of the content being related to these topics (Tandoc et al. 2021). Through the research of Paterson and Hanley, it is identified that within the United States, state security failed to detect the 2016 Russian interference with the Presidential election (Paterson and Hanley 2020). Paterson and Hanley state, "The use of social media as part of larger information warfare operations, combined with malicious programming and the promotion of political distrust, is a major challenge and one that democracies have not done enough to address." (Paterson and Hanley 2020).

In a disinformation study that was conducted by Raman et al. (2020), it was found that when individuals are presented with disinformation, the responses are still high enough to where a targeted attack utilizing disinformation could provoke a response that could result in negative effects on physical infrastructure (Raman et al. 2020). Raman et al. argue that based on the findings in their research, there need to be communication channels and mitigation strategies established by policymakers that address the identified vulnerability and would allow for warnings to be distributed to the public in an effort to reduce the responses to disinformation campaigns (Raman et al. 2020). Pathak et al. identified, "Since it is relatively easy and inexpensive to rapidly disseminate content through social media platforms, there is an urgent need for automated solutions to combat

disinformation." (Pathak et al. 2021). Along with the identified need for automated solutions to combat disinformation, Raman et al. displayed through their study that the response to disinformation is high enough that disinformation can be weaponized and may have the capability to cause physical damage (Raman et al. 2020).

For international campaigns, Lanoszka (2019) argues that disinformation campaigns with an international scope are ineffective at disrupting the balance of power and changing the decisions of the target state. Three primary barriers prevent disinformation from being effective internationally, uncertainty over international signals, pre-existing ideologies, and countermeasures that are in place to prevent disinformation (Lanoszka 2019). The reviewed literature did not address the potential impacts that disinformation campaigns have on the psychology of a population. Raman et al. show how disinformation and IO campaigns can be weaponized and used to conduct targeted attacks that invoke the target population to take the desired response action. Rubin identified that people only have a "slightly better than chance" of identifying deception and are generally highly susceptible to disinformation (Rubin 2019).

To expand on the existing research regarding disinformation and IO, psychology can be leveraged through the lens of social identity theory and potentially provide additional insight into the targeting of campaigns. There are three basic principles of social identity theory defined by Brown and Pehrson "First, people seek a positive self-concept (they want to see themselves in a positive light). Second, because the evaluation of groups that they belong to carries implications for this positive self-concept, individuals will try to achieve a positive social identity. Third, since evaluating the value of a social identity is essentially comparative, people prefer to see their groups as superior to other groups, at least on the criteria that matter most to them." (Brown and Pehrson 2019). From the definition of the social identity principles described by Brown and Pehrson (2019), in social identity theory, groups prefer to have an image of superiority; they will attempt to promote a positive social identity of themselves and within the group. Applying social identity theory to disinformation and IO campaigns may contend that social groups may have a greater likelihood of neglecting to verify disinformation that is in line with their beliefs, supports their group's social image, and provides a positive persona for the group. The neglect to verify information may cause the groups to inadvertently spread false information in efforts to establish supremacy for the group, which would increase the impact of a disinformation campaign.

The definition of disinformation provided by Pathak et al. is that it is false and misleading information that is shared intentionally to cause harm (Pathak et al. 2021). One of the primary objectives of disinformation is to impact and disrupt the balance of power (Lanoszka 2019). It is important to recognize that there is also a difference between disinformation and misinformation. Unlike disinformation, misinformation tends to have inaccuracies or errors and is typically unintentional (Rubin 2019). Verifying the source of information to verify its integrity has become increasingly difficult with the speed at which information is spread through social media platforms (Rubin 2019). Falls argues that disinformation is misleading information with the primary function of misleading (Fallis 2015). Disinformation is similar to lying, which creates different indicators to detect disinformation versus misinformation, where someone doesn't know what they are talking about and is unintentionally spreading information (Fallis 2015). Expanding on the existing research will provide insight into the psychological impacts and group processes that may cause disinformation to spread intentionally, increasing the reach of IO and disinformation campaigns.

3. Methods:

This research seeks to expand on the existing literature and identify the number of disinformation or IO campaigns that have taken place against the United States, and to identify any psychological impacts through the lens of social identity theory. According to the reviewed literature from Paterson and Hanley (2020), nation-state cyber actors are utilizing disinformation and IO to cause disruptions in the political processes of the United States, such as interference in the 2016 Presidential election. Are these targeted attacks successful at manipulating the political views of the nation? Raman et al. (2020) showed through their research that there was a high enough follow-through based on disinformation to cause blackouts of the power grid. The hypothesis for this research is that successful disinformation or IO campaigns will have a psychological impact on the target audience by manipulating the social identity by reinforcing an existing social-political standpoint or changing the social-political standpoint of the target audience. Examining identified campaigns, the research attempts to identify the psychological impacts on the social-political standpoints of the target audience of the campaign.

Utilizing the ten-year timeframe identified in the research question, correlations have been made using the election data. The analysis will focus on IO and disinformation that has targeted political campaigns. In an effort

to identify campaigns targeting political parties, multiple datasets have been examined. The datasets have been obtained using a combination of open-source data repositories that have collected known fake news from social media and online news sources. This known fake news and data regarding the mentions of information operations and disinformation will be correlated with data scrapes conducted from multiple social media platforms from 2016 through 2019 to identify how popular the known fake news relating to the political parties was through that timeframe. The political party polling data has been used to look at changes to the support for the political party aligned to the associated timeframe of the campaigns. From the three principles of social identity theory, this research examines how disinformation propagates through social groups and expands into successful disinformation campaigns.

Using a semi-quantitative approach and utilizing the data from the MIT Election Data and Science Lab, the election results were examined for the House, Senate, and Presidential elections from 2012 through 2021. During this timeframe, there were three different U.S. Presidents in office. From 2012 through 2017, President Obama finished his second term as President. From 2017 through 2021, President Trump served as President, and from 2021 to the time of this research, President Biden has served as the President. Based on the U.S. Presidents in office over the identified timeframe, two different political parties held office, President Obama 2012 through 2017 and President Biden 2021 to the present as the Democratic candidate, and President Trump 2017 through 2021 as the Republican candidate. This information was also used when collecting data from open-source datasets.

Nine keywords were used to search through the data to identify where there are mentions of political affiliations. The nine keywords used were House, Senate, Democrat, Republican, Obama, Trump, Hillary, Sanders, and Biden. These nine keywords were selected based on three being the names of former or current U.S. Presidents as identified earlier. Hillary and Sanders were used based on those being the popular names for the democratic candidates in the 2016 election. Democrat and Republican were chosen due to those being the names of the primary parties in the U.S. elections. Senate and House were used to represent the other areas of the U.S. government that the identified presidential candidates did not capture. The data available from the MIT Election Data and Science Lab for the Senate elections spans from 2012 through 2021. For the House elections, the MIT Election Data and Science Lab dataset only contained data from 2012 through 2020. To maintain consistency in examining the data, only the data from 2012 through 2020 was utilized from all three of the datasets. The identified IO and disinformation campaigns were aligned to the election results to highlight0 if there are any significant correlations between the campaigns and the election results data. A mixed-method research approach was taken to quantify the areas where disinformation has been observed. Based on the results from the semi-quantitative approach, a qualitative analysis will be conducted to examine the potential psychological impacts of the political standings observed in the United States over the examined timeframe.

4. Findings and Analysis:

Examining the dataset sourced from FakeNewsNet (Shu et al. 2017 – 2018), the data captures the number of tweets that mentioned the keywords within the dataset. Using the nine keywords House, Senate, Democrat, Republican, Obama, Trump, Hillary, Sanders, and Biden, the dataset was examined to identify how many tweets were associated with the identified fake news and the respective keyword. The results of the number of tweets associated with fake news by the keywords can be seen in Figure 1.

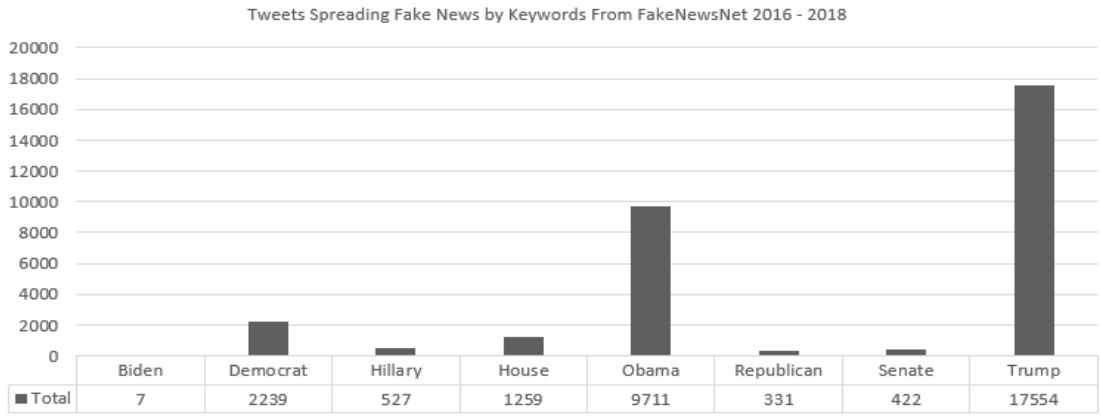


Figure 1: Number of Fake News Tweets About the Keywords (Shu et al. 2017 - 2018)

It is important to note that there were no relevant results in the dataset for the keyword Sanders and limited data regarding the keyword Biden. From the data relating to fake news, the number of results that related to the keyword Trump in 2016 through 2018 timeframe was a great deal higher than those relating to any of the other keywords. The second highest was Obama, with 9711 identified tweets associated with the keyword dealing with fake news. The timeframe of this dataset overlaps with the 2016 election when President Obama left office, and President Trump was coming into office. Martin et al. identified 20 information operations that took place against the United States, starting from 2014 through 2019. The country and timeframes are displayed in figure 2. During the 2014 attacks, the primary threat actor was Russia, and the three attacks aimed to spread misinformation, undermined the image of Obama, and polarize politics in America (Martin et al. 2022). The operations starting in 2015 also came primarily from Russia. They focused on attacking Hillary Clinton in the 2016 elections, attacking the democratic party during the 2016 and 2018 elections, discrediting institutions in America, and supporting Trump in the 2016 and 2020 elections (Martin et al. 2022). In the campaigns observed starting in 2016, there were additional threat actors, including Iran and unknown actors conducting information operations. These campaigns intended to attack Hillary Clinton (UNK), attack critics of Trump after the 2016 elections (RUS), support Trump in the 2016 election and 2018 midterm elections (UNK), support independence movement in California and Texas (RUS), attack Trump in the 2016 and 2020 elections (IRN), and support Alt-right movements in the 2016 and 2020 elections (RUS) (Martin 2022). In 2017 there were campaigns observed from China, Russia, and Iran with the intent to support Republican senator Roy Moore (RUS), attack the Republican party (IRN), and Polarize politics in America (CHN, IRN) (Martin 2022). In 2018 only Russia and Iran were observed with the intent to support Trump's Nominees in Courts (RUS) and promote Iranian foreign policy initiatives (IRN) (Martin 2022). The campaign starting in 2019 was from Russia and focused on attacking Biden in the 2020 election (Martin 2022).

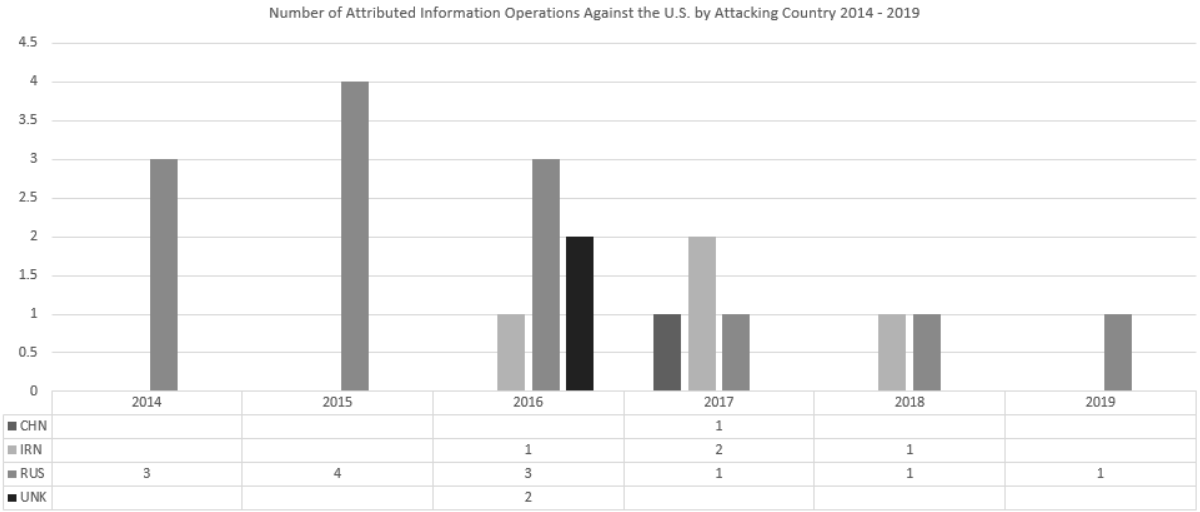
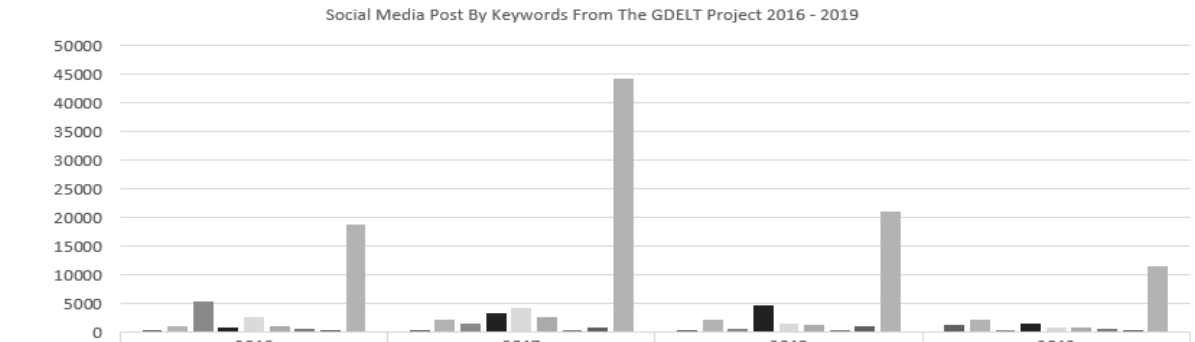


Figure 2: Information Operations Against the U.S. (Martin et al. 2022)

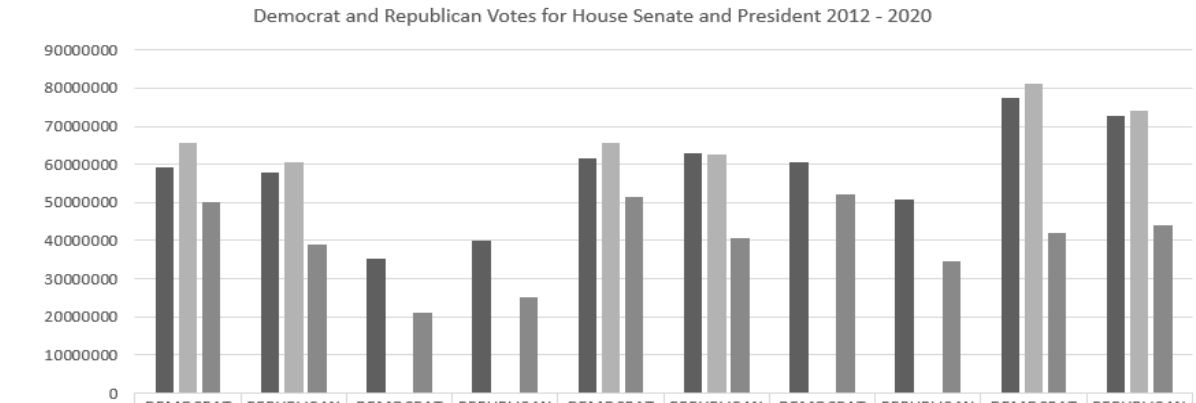
Due to the timeframe captured with the fake news dataset, there is no data to compare for the 2014 and 2015 Russian campaigns. There is data for 2016 – 2018; based on the keywords, there was fake news identified with the keywords Trump and Obama along with Hillary, House, and Democrat, which aligns with the majority of the identified campaign's intent from the 20 campaigns. To gain an idea of the social media landscape during that timeframe, additional social media posts were examined to understand how many mentions the keywords received from a general dataset. This was done by using the Global Database of Events, Language, and Tone (GDELT) Project dataset that captured social media posts from Facebook, Instagram, QQ, Twitter, Vimeo, VK, and YouTube from April 2016 through the end of September 2019 (The GDELT Project 2019). Figure 3 shows the breakdown of social media posts relating to the keywords during the timeframe captured in the dataset. When examining the dataset from GDELT, only posts that discussed the keywords were examined. Any post originating from an account associated with the keyword was not counted toward the keyword.



	2016	2017	2018	2019
Biden	203	342	239	1215
Democrat	1045	2123	2275	2126
Hillary	5395	1486	599	252
House	787	3245	4730	1407
Obama	2724	4306	1399	787
Republican	971	2605	1253	883
Sanders	588	370	408	607
Senate	316	910	942	290
Trump	18676	44236	21012	11511

Figure 3: Social Media Post by Keywords (The GDELT Project 2019)

From GDELT dataset, there is a consistently high number of social media posts involving the keyword Trump. Similar to what was observed in the fake news data, in 2017, Obama is second in the number of social media posts. Because this is looking at the social media post and not considering the number of shares or associated tweets such as the fake data, the number for Obama is lower than what is observed in the fake news dataset. The GDELT dataset showed the greatest numbers in 2017, and overall, the numbers appear to be declining for the keywords Trump, Republican, Obama, Hillary, and Biden moving into 2018. The GDELT dataset contained data through September 2019, meaning there is not a full year's worth of data for 2019. Though there is not a full year of data, there is still an increase in the mentions relating to the keyword Biden and Democrat. Figure 4 contains the voting results for elections that took place for the House, Senate, and Presidential elections from 2012 through 2020. What would be expected is that if the IO conducted during these timeframes were successful, there would be a clear deviation in the voting results showing the social-political impact of the campaigns.



	DEMOCRAT	REPUBLICAN	DEMOCRAT	REPUBLICAN	DEMOCRAT	REPUBLICAN	DEMOCRAT	REPUBLICAN	DEMOCRAT	REPUBLICAN
	2012		2014		2016		2018		2020	
US HOUSE	59194640	57977915	35273163	39926535	61417454	62772633	60454544	50752541	77336102	72671813
US PRESIDENT	65752017	60670117			65677288	62692670			81268908	74216146
US SENATE	49988282	39128301	21246466	25010851	51315969	40842211	52208408	34721533	42138692	43948213

Figure 4: U.S. Votes by Party (MIT Election Data and Science Lab 2017)

During 2016 when the highest number of IO campaigns were observed targeting the democratic candidate Hilary Clinton and supporting Donald Trump, these results are similar to the results observed in the 2012 elections. In the voting numbers from the 2016 elections, the democratic party won in both the Senate and the President, and the Republican candidate won the Presidential election through the electoral college, not from the overall

votes received. Based on the examined data, it does not appear that the observed IO campaigns met their intent or that the disinformation spread through fake news had a large enough impact on the targeted population to noticeably change the social-political views of the population.

5. Conclusion:

This research examines the question of what are the psychological impacts of disinformation and Information Operation campaigns on the United States between 2012 and 2022? The intent is to test the hypothesis that a successful disinformation or IO campaign will have a psychological impact on the target audience by manipulating the social identity by reinforcing an existing social-political standpoint or changing the social-political standpoint of the target audience. Based on the available data that was used in this research, it does not suggest that the observed IO and disinformation campaigns were successful at changing the social-political standpoint of the target audience. Further research is required to understand the scope of the impact that IO and disinformation may have on the psychology of a targeted population. Although Raman et al. (2020) displayed that disinformation can be weaponized to potentially cause physical damage if there are high enough responses to the campaign. The findings of this research further support Lanoszka's analysis of international disinformation campaigns being ineffective at changing the decisions of the target state and disrupting the balance of power (Lanoszka 2019). From the three primary barriers discussed by Lanoszka, the pre-existing ideologies (Lanoszka 2019) may be a contributing factor as to why the voting data showed similar trends from 2012 and 2016, even though there were more disinformation and IO campaigns taking place during the 2016 timeframe. Although the impact of the IO and disinformation campaigns didn't appear to be significant from the observed data, further research is required to focus on where the IO and disinformation campaigns have been effective. Using IO and disinformation has continued to be a relevant tactic deployed by nation-states, as observed from China, Russia, and Iran through this paper. It is important to gain a better understanding of what creates a successful campaign to enable safeguards to be deployed that can mitigate the impact of a successful campaign.

References:

Altheide, D. L., and Jennifer N. Grimes. (2005). War Programming: The Propaganda Project and the Iraq War. [online], The Sociological Quarterly, 46(4), 617–643. http://www.jstor.org/stable/4121509

Brown, R. and Pehrson, S. (2019) Group Processes (3rd Edition), [online], Wiley Global Research (STMS), https://online.vitalsource.com/books/9781118719312

Fallis, D. (2015) 'What Is Disinformation?', [online], Library Trends, 63(3), pp. 401–426. https://doi.org/10.1353/lib.2015.0014.

Lanoszka, A. (2019) 'Disinformation in international politics', [online], *European Journal of International Security*, 4(2), pp. 227–248. https://doi.org/10.1017/eis.2019.6.

Martin, D. A., Shapiro, J. N., & Ilhardt, J. G. (2022). Introducing the Online Political Influence Efforts dataset. [online], Journal of Peace Research, 0(0). https://doi-org.ezproxy1.apus.edu/10.1177/00223433221092815

Martin, D. A., Shapiro, J. N., & Ilhardt, J. G. (2022) "Replication data and Online Appendix for: "Introducing the Online Political Influence Efforts dataset" Journal of Peace Research", [online], Harvard Dataverse V1, https://doi.org/10.7910/DVN/8IF59Q,

MIT Election Data and Science Lab (2017) "U.S. House 1976–2020", [online], Harvard Dataverse, V11, UNF:6:ry6R0P1KRBhWkIfZzKiM8A== [fileUNF], https://doi.org/10.7910/DVN/IG0UN2

MIT Election Data and Science Lab (2017) "U.S. President 1976–2020", [online], Harvard Dataverse, V6; 1976-2020-president.tab [fileName], UNF:6:4KoNz9KgTkXy0ZBxJ9ZkOw== [fileUNF], https://doi.org/10.7910/DVN/42MVDX

MIT Election Data and Science Lab (2017) "U.S. Senate 1976–2020", [online], Harvard Dataverse, V6, UNF:6:dogvks8KPD0c/hzNi9kaag== [fileUNF], https://doi.org/10.7910/DVN/PEJ5QU

National Institute of Standards and Technology (NIST) (2022) "information operations (IO)", [online], Information Technology Laboratory, Computer Security Resource Center, https://csrc.nist.gov/glossary/term/information_operations

National Intelligence Council (2021) "Foreign Threats to the 2020 US Federal Elections", [online], Intelligence Community Assessment, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

Paterson, T. and Hanley, L. (2020) "Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'Deep Fakes.'", [online], Australian Journal of International Affairs 74, no. 4: 439–54. https://doi.org/10.1080/10357718.2020.1734772.

Pathak, A., Rohini, S., and Nihit, N. (2021) "Disinformation: Analysis and Identification.", [online], Computational and Mathematical Organization Theory 27, no. 3: 357–75. https://doi.org/10.1007/s10588-021-09336-x.

Raman, G., AlShebli, B., Waniek, M., Rahwan, T., and Peng, J. (2020) "How Weaponizing Disinformation Can Bring down a City's Power Grid.", [online], Edited by Qi Jiang. PLOS ONE 15, no. 8: e0236517. https://doi.org/10.1371/journal.pone.0236517.

Roholl, M. (2012) "Preparing for Victory. The U.S. Office of War Information Overseas Branch's illustrated magazines in the Netherlands and the foundations for the American Century, 1944-1945", [online], European Journal of American Studies, vol. 7, no. 2.

Rubin, V. (2019) "Disinformation and Misinformation Triangle: A Conceptual Model for 'Fake News' Epidemic, Causal Factors and Interventions.", [online], Journal of Documentation 75, no. 5: 1013–34. https://doi.org/10.1108/JD-12-2018-0209.

Shu, K., Mahudeswaran, D., Wang, S., Lee, D., and Liu, H. (2018) "FakeNewsNet: A Data Repository with News Content, Social Context and Dynamic Information for Studying Fake News on Social Media" arXiv preprint arXiv:1809.01286

Shu, K., Sliva, A., Wang, S., Tang, J., and Liu, H. (2017) "Fake News Detection on Social Media: A Data Mining Perspective" ACM SIGKDD Explorations Newsletter, volume 19 no. 1 pg. 22-36.

Shu, K., Wang, S., and Liu, H. (2017) "Exploiting Tri-Relationship for Fake News Detection" arXiv preprint arXiv:1712.07709

Tandoc, E., Thomas, R., and Bishop L. (2021) "What Is (Fake) News? Analyzing News Values (and More) in Fake Stories", [online], Media and Communication 9, no. 1: 110–19. https://doi.org/10.17645/mac.v9i1.3331.

The GDELT Project (2019) "Compiling A Master List Of Social Media In The News 2016-2019", [online], https://blog.gdeltproject.org/compiling-a-master-list-of-social-media-in-the-news-2016-2019/

Wahlstrom, A., Xia, J., Revelli, A., and Serabian, R. (2022) "Information Operations Targeting 2022 U.S. Midterm Elections Include Trolling, Narratives Surrounding Specific Races, Politicians", [online], Mandiant, https://www.mandiant.com/resources/blog/information-operations-2022-midterm-elections