Social Media as Information Warfare

AUGUST 2021

STRATEGIC MULTILAYER ASSESSMENT

Student paper series in collaboration with the TRADOC e-intern program

Author: Hannah Matthews

The College of William & Mary

Hannah Matthews, E-intern, The College of William & Mary

Hannah Matthews is a student at the College of William & Mary where she is pursuing a major in Government, and a minor in English. She served as part of the TRADOC Virtual Intern Program in 2021.

Social Media as Information Warfare

Hannah Matthews, College of William & Mary[1]

The flow of disinformation through social media, combined with the illusory truth effect, establish social media as an emerging threat in *information warfare* (IW). The illusory truth effect is the idea that repeatedly seeing information makes it more likely to be seen as true. *Artificial intelligence* (AI) can create articles containing false information that will then be distributed to the public. These articles are entirely computer generated and require little to no human input. Quantum computing can get into most computer encryptions, with the ability to place false information into trusted online formats. With social media being the main way that people receive their news, this intrusion of false information will cause the degradation of trust in news sources, leading to a similar decrease of trust in democracy. Social media combined with AI and quantum computing may allow for disinformation to be easily distributed and immediately read. Depending on the frequency of this dissemination based on the illusory truth effect it may also be believed to be true. Artificial intelligence is currently developing further as is quantum computing. Within the next ten years, the growth of technological capabilities will further bring social media into information warfare, in new and dangerous ways. In order to be successful, it is necessary for the United States to examine social media and its role in information warfare and adopt it into US tactics. This paper will demonstrate that disinformation combined with the illusory truth effect will establish social media as a powerful tool in IW.

2

[1] *Contact Information*: hmmatthews@email.wm.edu

[2] Information warfare is defined as gathering, providing, and denying information in order to improve one's own decision-making and position while damaging the enemy's (Crane).

History of News and Social Media

Trust in all forms of media is important for the health of a democracy. Society relies on media heavily for political news, meaning that any negative change in confidence in the media can interfere with the ability to discern important issues from trivial ones (Johnson & Kaye, 2015, p. 128). Furthermore, mass media, depending on its messages, can influence society in either a positive or negative way. An example of negative media influence is Bosnia during the mid-1990s, when nationalist leaders in Serbia seized control of broadcasts and fired journalists who refused to support the nationalist party line. The rhetoric these leaders used persuaded many people to support severe mistreatment of their fellow Bosnians (Armoudian, 2020). One of the underlying reasons media has this influence on forming opinions, is in the psychological phenomenon described as the illusory truth effect, which says that the repetition of a statement increases its likelihood of being judged as true (Li, 2019). Social media creates individual but direct links between the public, the government, and media. Through social media platforms, confidence in media and government is influenced in different ways (Johnson & Kaye, 2015, p. 128, p. 130). Declining citizen's confidence in institutions undermines the credibility of official information in news and opens the public to alternative information sources (Bennett & Livingston, 2018, p. 122).

Disinformation and Propaganda

Social networking technologies change the scale, scope, and precision of how information is transmitted in the digital age, as well as social media being instantaneous (Bradshaw & Howard, 2019, p. 11). Disinformation is defined as "intentional falsehoods spread as news stories or simulated formats to advance political goals" (Bennett & Livingston, 2018, p. 124). Many democratic nations are experiencing increased levels of disinformation circulating through social media and political websites that are mimicking journalism formats. Governments around the world are increasing their use of disinformation, even though Facebook and other social media platforms are working to combat it. Facebook stands as the number one social network for disinformation. Also, the use of bots, fake social media accounts, and hired trolls is increasing (Alba & Satariano, 2019). Cyber troops often work in conjunction with private industries, civil society organizations, internet subcultures, youth groups, hacker collectives, fringe movements, social media influencers, and volunteers who support their cause (Bradshaw & Howard, 2019, p. 9). Disinformation through social media can involve any combination of a broad range of techniques, including classic propaganda, highly plausible fabricated video and audio material, and discrediting key institutions that can distinguish between true and false information (Mazarr et al., 2019, p. 156). This flow of disinformation, combined with the illusory truth effect, establish social media as a leading threat in information warfare. As demonstrated in the prior section, social media platforms provide a different way for information to be presented. These platforms can increase the volume at which information is presented, playing into the illusory truth effect because the more information is seen, the more likely it is to be perceived as true.

Hostile social manipulation is defined as "the purposeful, systematic generation and dissemination of information to produce harmful social, political, and economic outcomes in a target country by affecting beliefs, attitudes, and behaviors" (Mazarr et al., 2019, p. xi). This manipulation targets beliefs and attitudes, not physical assets or military forces. More specifically, the target is the adversary's will (Mazarr et al., 2019, p. 6, p. 9). In August of 2020, Netflix released a documentary titled "*The Social Dilemma*." This particular documentary investigates the new role social media plays in individuals' lives. Furthermore, it serves as a warning against the increasing role social media plays in society (The Social Dilemma, 2020). When propaganda is disseminated by a particular organization or individual, it contains nothing necessarily new in regard to disinformation. Bots, humans, and cyborgs are three types of fake accounts being used. Bots are highly automated accounts designed to mimic human behavior online and are used to amplify narratives or drown out political dissent. Human-run accounts engage in conversations by posting comments or tweets, or by private messaging individuals via social media platforms. A cyborg blends automation with human creation. Another type of fake account being used is hacked or stolen accounts. These high-profile accounts are used by cyber troops to spread pro-government propaganda or censor freedom of speech by revoking access to the original owner (Bradshaw & Howard, 2019, p. 11). Familiarity is the key component of uptake of viral messages, meaning that the more a claim is heard, the less likely the claim is going to be assessed critically. Social media algorithms work by drawing attention to content and trends on their networks, especially when people are outraged by it (Silverman, 2019, p. 385). With social media becoming an integral part of IW, it is necessary to examine its growing role in society.

Social Media's Role in Government

Disinformation is used by authoritarian regimes to control their people through suppressing fundamental human rights, discrediting political opponents, and drowning out dissenting opinions. Some governments use computational propaganda[3] for foreign influence operation (Alba & Satariano, 2019). As a way to prevent any growing opposing beliefs, manipulation of social media through the use of disinformation is a way to oppose democracy and lead to further degradation of trust in democratic institutions. This practice will likely become more common as more countries continue to grow in opposition to democracies. When it comes to social media and political movements, there is evidence of organized social media disinformation campaigns, which have taken place in 70 countries. Also, in each of the seventy countries, at least one political party or government agency is using social media to shape public attitudes domestically. Recently, certain governments have been using social media to influence public opinion through bots to amplify, trolls to harass dissidents and journalists, and fake social media accounts to misrepresent the number involved in the issue (Alba & Satariano, 2019). Most

[3] Computational propaganda is the "use of algorithms, automation, and big data to shape public life."

government-linked disinformation is focused domestically but at least seven countries have been found to use Facebook and Twitter to influence audiences globally (Bradshaw & Howard, 2019). Fifty-two out of the 70 countries examined in a particular study, actively created content of memes, videos, fake news websites, or manipulated media to mislead users, targeting specific communities with disinformation or manipulated media. These countries also censor speech and expression through mass-reporting of content and accounts (Bradshaw & Howard, 2019, p. 15).

As two leading countries in social media warfare, it is important to examine how China and Russia have used this tactic. An authoritarian regime striving to control its citizens, China largely uses disinformation against their own country. This control was demonstrated with the protests in Hong Kong. The protests' purpose was transformed by the Chinese government to represent something entirely different to its population outside of Hong Kong. China also controls its population with its firewall of information. The firewall essentially is a machine of online controls that prevents the population from accessing information other than what the Chinese government allows them to see (Myers & Mozur, 2019). This firewall is established further with China specific social media apps, such as Weibo. By only allowing for this specific app, China is limiting the information their population is receiving as well as distributing to others (Lu et al., 2016, p. 420).

Russia operates largely in the information warfare domain with their military branch that consists of information warfare warriors. This branch is responsible for spreading information on Wikileaks, a "non-state hostile intelligence service abetted by state actors like Russia" (Prier, 2017, p. 67). However, the information posted by Russia would fail if not for the existing network of Americans in support of that message to spread that information. In 2015, Russian trolls spread disinformation and accused journalists of failing to cover important issues with the Black Lives Matter movement. Their goal was to spread fear, while discrediting institutions like American media (Prier, 2017, p. 68). Russia orchestrated the best-known example of government propaganda and disinformation on social media with the 2016 US presidential election, using Facebook, Instagram, Twitter, and YouTube (Ingram, 2019). With this election, Russian propaganda had a narrative to build upon based on the strong polarizations between candidates. They were able to create trends, as well as using bot tweets and hashtag hijacking (Prier, 2017, p. 71).

These examples demonstrate how the power of social media is being manipulated for political goals. Social media is likely going to continue to be used in this way because it is global and instantaneous, and is embedded in the economic, social, and political fabric of societies but only half of the world is online with access and exposure to this form of disinformation (Silverman, 2019, p. 384). Also, the design of social media makes information warfare significantly easier to conduct. Social media platforms allow for authoritarian communication campaigns to widen and deepen gaps between citizens and countries (Oates, 2020, p. 5). The internet has become a battlefield. Not only for individuals, but it has

become indispensable to militaries, governments, and armed groups who are able to use it to further their interests against their adversaries.

Future of Social Media Warfare

Looking to the future of social media and IW, national security will increasingly rely on a resilient infosphere that works to present factual information to readers. Furthermore, conflicts will be increasingly waged between and among these internet networks (Mazarr et al., 2019, p. xv). Computational propaganda is the "use of algorithms, automation, and big data to shape public life – it is becoming a pervasive and ubiquitous part of everyday life," and it has become a pervasive part of the digital information ecosystem. It is used to suppress fundamental human rights, discredit political opposition, and drown out political dissent (Bradshaw & Howard, 2019, p. 2). New technologies, like AI and *virtual reality* (VR), are going to reshape society and politics (Bradshaw & Howard, 2019, p. 21). When these technologies are applied to social media, the information being presented to humans will grow even stronger in terms of disinformation.

Artificial Intelligence has the potential to easily and quickly generate massive amounts of fake news. Because of how sophisticated the technology of AI is, it can produce information to targeted populations. If AI algorithms are used to overflow social media with disinformation and convince the public that articles are truthful, this would further play into the illusory truth effect because of the amount of articles declaring something as real. Disinformation groups using AI would be able to publish massive amounts of fake articles and headlines, blurring the line of truth to the public (Li, 2019). Social media is a dangerous outlet for AI disinformation because the amount of people that would be exposed to fabricated content would go beyond what could have ever been done prior. AI has capabilities that enables anyone with access to push out content, undetectably, quickly, and cheaply. In the past, propaganda needed humans to write it but now it can be done without the need of humans. While currently AI has certain tells, advances in technology will eliminate those, with operators far less sophisticated than the Russian government being able to robo-generate tweets. Even though detection technology will grow in sophistication, the tools generating images, videos, and texts will also be growing. Eventually internet users will give up on trying to judge authenticity for each tweet and article as AI capabilities continue to increase (DiResta, 2020). The capabilities of AI are predicted to grow significantly within the next five years, making it even more desperate to increase AI capabilities as much as possible (Li, 2019).

Another future facing social media is quantum computing: computing that uses the laws of quantum physics to process information faster than typically possible. Modern encryption protocols use asymmetric encryption but with Shor's quantum prime factorization algorithm, it would render asymmetric encryption effectively useless, allowing access to essentially any encrypted system. This could also be used to plant disinformation within trustworthy news sources by changing content in

articles after being published. On an institutional level, quantum computing could be used to ruin the public opinion of conventionally trusted sources by consisting of publishing false content from those sources, diminishing accurate information (Li, 2019). With quantum computing, any post on social media holds the potential to be altered, allowing for the spread of disinformation and propaganda. While quantum computing is still being largely researched, it is likely to be implemented in a similar timeframe to AI, as more research is done. A current problem of a similar nature is the use of deep fakes, which is a product of AI. Deep fakes allow anyone with a computer and internet to create realistic photos and videos of people saying and doing things that they did not actually say or do (Toews, 2020).

To successfully defend against other countries in information warfare, the United States has to keep up with the ever-growing trend of social media as IW and adopt it as a focus. This focus includes AI and quantum computing and adopting them into aggressive tactics if necessary. If social media platforms have the knowledge on accounts as discussed in "Social Dilemma," aggressors could easily target certain groups of people into unknowingly serving a foreign government's purpose. (Li, 2019). It is also necessary to combat the tactics that are growing in this rate, requiring a coalition of governments, private companies, and academic and non-profit organizations (CB Insights, 2020). Perhaps the most important tool, however, is investing in research and understanding to begin building forms of inoculation and resilience against the worst forms of information-based social manipulation (Mazarr et al., 2019, p. xvii). An item for consideration is how Generation Z overuses social media, to the point that their daily lives are centered around different platforms. Since the majority of their lives are spent on these apps, the algorithms and disinformation on social media platforms directly plays into their hands, potentially having the ability to control their opinions. With bots and fake accounts, it is possible to influence the current generation's opinions on social media in a specific direction. By establishing credibility or influencing their opinions, when AI and quantum computing becomes more prevalent, there will already be an established credibility. The dangers presented by AI and quantum computing present countless possibilities for social media and its manipulation in terms relating to IW.

Conclusion

As discussed in this paper, social media is a large and emerging threat in IW. The flow of disinformation through social media, along with the illusory truth effect and growing technological capabilities establish social media as a powerful tool in IW. Artificial intelligence and quantum computing will continue to change the way disinformation is presented to the public through social media, which threatens the public's trust of news sources and decreases the trust in democracy. The ease and speed that information is transmitted with social media only increases the potential of disinformation being spread. In the next ten years, social media will be an active part of IW, making it necessary for the United States to incorporate social media into its information warfare defense tactics.

Works cited

Alba, D. & Satariano, M. (2019). At Least 70 Countries have had Disinformation Campaigns, Study Finds. *The New York Times,* https://www.nytimes.com/2019/09/26/technology/government-disinformation-cyber-troops.html

Armoudian, M. (2020, December 12). Perspective – Toxic Media Destroys Democracy. Here's what to do about it. *Washington Post,* https://www.washingtonpost.com/outlook/2020/12/21/toxic-media-destroys-democracy-heres-what-do-about-it/

Bennett, W. L., and Livingston, S. (2018). "The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions." *European Journal of Communication, 33*(2), pp. 122-139, https://doi-org.proxy.wm.edu/10.1177/0267323118760317, doi:10.1177/0267323118760317

Bradshaw, S., & Howard, P. N. (2019). "The Global Disinformation Order." *Oxford Internet Institute*, https://comprop. oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

CB Insights. (2020 October 21). Weaponization of the Future: Digital Warfare & Disinformation. *CB Insights.* https://www.cbinsights.com/research/future-of-information-warfare/

Crane, C. (2019). The United States Needs an Information Warfare Command: A Historical Examination. *War on the Rocks.* https://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/

DiResta, R. (2020). The Supply of Disinformation Will Soon be Infinite. *The Atlantic*, https://www.theatlantic.com/ideas/archive/2020/09/future-propaganda-will-be-computer-generated/616400/

Harris, T. (2019). Our Brains are no Match for our Technology. *New York Times*, https://www.nytimes.com/2019/12/05/opinion/digital-technology-brain.html?auth=link-dismiss-google1tap.

Ingram, D. (2019). More Governments Choosing Propaganda Over Censorship on Social Media, Report Says. https://www.nbcnews.com/tech/tech-news/more-governments-ever-are-using-social-media-push-propaganda-report-n1076301

Johnson, T. J., & Kaye, B. K. (2015). Site Effects: How Reliance on Social Media Influences Confidence in the Government and News Media. *Social Science Computer Review, 33*(2), pp. 127-144, https://doi-org.proxy.wm.edu/10.1177/0894439314537029, doi:10.1177/0894439314537029

Li, E. (2019). "The Future of Disinformation." *Harvard International Review*, https://hir.harvard.edu/futureofdisinformation/

Lu, B., Zhang, S., & and Fan, W. (2016). Social Representations of Social Media use in Government: An Analysis of Chinese Government Microblogging from Citizens' Perspective. *Social Science*

Computer Review, 34(4), pp. 416-436, https://doi-org.proxy.wm.edu/10.1177/0894439315595222, doi:10.1177/0894439315595222

Mazarr, M. J., et al. (2019). The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment. https://www.rand.org/pubs/research_reports/RR2714.html

Myers, S. L., & Mozur, P. (2019, August 13). China is Waging a Disinformation War Against Hong Kong Protesters. *The New York Times*. https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html

Oates, S. (2020). The Easy Weaponization of Social Media: Why Profit has Trumped Security for U.S. Companies. *Digital War*, *CrossRef*, https://doi.org/10.1057/s42984-020-00012-z, doi:10.1057/s42984-020-00012-z

Prier, J. (2017). Commanding the Trend; Social Media as Information Warfare. *Strategic Studies Quarterly, 11*(4), pp. 50-85. http://www.jstor.org/stable/26271634

Silverman, M. (2019). LikeWar: The Weaponization of Social Media P. W. Singer, and Emerson T. Brooking. *International Review of the Red Cross, 101*(910), pp. 383-387. https://proxy.wm.edu/login?url=https://www-proquest-com.proxy.wm.edu/scholarly-journals/i-international-review-red-cross-likewar/docview/2338699964/se-2?accountid=15053, doi:http://dx.doi.org.proxy.wm.edu/10.1017/S1816383119000511

Toews, R. (2020). Deepfakes Are Going To Wreak Havoc On Society. We Are Not Prepared. *Forbes.* https://www.forbes.com/sites/robtoews/2020/05/25/deepfakes-are-going-to-wreak-havoc-on-society-we-are-not-prepared/

The Social Dilemma. (2020). The Social Dilemma - More about the film. https://www.thesocialdilemma.com/the-film/