2021

The Role of the Internet in Intelligence Gathering and Spreading Propaganda

Leila Halawi
Embry-Riddle Aeronautical University, halawil@erau.edu

Scholarly Commons Citation
Halawi, L. (2021). The Role of the Internet in Intelligence Gathering and Spreading Propaganda. *Issues in Information Systems, 22*(2). DOI: https://doi.org/10.48009/2_iis_2021_243-251

Issues in Information Systems
Volume 22, Issue 2, pp. 231-238, 2021

DOI: https://doi.org/10.48009/2_iis_2021_243-251

The role of the Internet in intelligence gathering and spreading propaganda

Leila Halawi, *Embry Riddle Aeronautical University, halawil@erau.edu*

Abstract

The analysis of American intelligence as an academic discipline exhibits an excellent level of integration regarding subject matter and methods from military history and strategic studies. The knowledge and information revolution steered a different online culture of sharing and oversharing. While the study of intelligence has primarily been associated with historical methods thus far, opportunities for innovation are also afforded by advances in theoretical and conceptual thinking about intelligence. Such revolutions can help intelligence history while concurrently enlightening the disputes on intelligence in the twenty-first century. The takings from the information age consist of low cost for access to data and significant dependence on the Internet. Intelligence agencies profit from the Internet equally through open sources and concealed data gathering from networked computers (Haines, 2004). In addition, Information gathering through Twitter, Facebook, Snapchat, Instagram, blogs, and several social media sites, to name a few, facilitated intelligence gathering all over the world. While some researchers may argue that social media may be an intelligence-gathering tool, several reports revealed that it could also be used for propaganda and misinformation or is intelligence in support of secret operations. This project will investigate how the Internet and the use of Social Media in particular, along with the military strategy of a country, can affect the design of its market intelligence processes.

Keywords*:* Internet, intelligence gathering, propaganda, social media.

Introduction

The analysis of American intelligence as an academic discipline exhibits a significant level of integration regarding subject matter and methods from military history and strategic studies (Haines, 2004). The knowledge and information revolution steered a different online culture of sharing and oversharing. While the study of intelligence has primarily been associated with historical methods thus far, opportunities for innovation are also afforded by advances in theoretical and conceptual thinking about intelligence. Such revolutions can help intelligence history while concurrently enlightening the disputes on intelligence in the twenty-first century.

Muller (2014) conducted a study to compare democratic media performance of 47 countries using a framework that compared the role of the media that ranged from watching and reporting only to the actual representation of people's views. She noted a significant variation across the 10 to 47 countries surveyed and identified different patterns. This project will investigate how the Internet and the use of Social Media in particular, and the military strategy of a nation can affect the design of its market intelligence processes.

Exploring methodological issues describing the use of primary sources, epistemology related to bias and Neutrality, and reporting explaining how scholars form their arguments.

This study explores methodological issues describing the use of primary sources, epistemology related to bias and Neutrality, and reporting explaining how scholars form their arguments. The structure of this paper is as follows: Section 2 presents the literature review outlining intelligence gathering, propaganda and misinformation, and the use of the Internet and social media to spread propaganda. Section 3 summarizes the conclusion, presents the recommendation, current state of research, and future work area.

Literature Review

This part of the research outlines the literature about the topic broken into four themes.

Intelligence Gathering

Intelligence has been a military discipline for nearly a half-century; its focus, technique, and collecting practices have been transformed. In the Cold War period, general power derived merely from the military authority, and intelligence occurred to disclose the competencies of the enemy. Then, military abilities were the main aim in that period (Bayraktar, 2014). The U.S. has been collecting intelligence since the revolutionary war. At the time, George Washington demanded that Congress found a top-secret service reserve for concealed events. Agreeing with the Duke of Marlboro, Washington stated that for any war to be successful initial and reliable intelligence is needed (Keegan, 2004, p. 7).

According to Ronczkowski (2017), intelligence investigation units were in law enforcement for numerous periods. Ronczkowski adds that, in criminal analysis, Marilyn Peterson offers historical background on reports, details, and intelligence that were discovered by law enforcement in the 1920s and 1930s and were the response to the need to gather information on radicals and gangsters. After the Cold War, the meaning of opponent, security, and risk assessment transformed. Consequently, technology increased, and traditional intelligence collecting techniques revolved into particular intelligence techniques.

Intelligence units functioned intermittently in the United States until the introduction of P.C.s and implemented an investigation by several public and local organizations in the early 1980s. In the 1990s, the most evolution and configuration of intelligence pieces was noticed and the establishment of many professional associations devoted to intelligence and analysis, several of which are still operating nowadays. Moreover, there were numerous books authored on the subject, and training programs started to develop. Later, the new millennium started, and just preceding the finish of the era, everybody was chomped with the Y2K error and computer failures. Law enforcement staff were occupied training for turmoil and anarchism. Intelligence groups were operating around the clock to prevent a disastrous outcome. Nowadays, these agencies or groups are training for affairs associated with terrorism, violence, and risks to homeland security. Since introducing computer technology, law enforcement groups wanted to improve their competencies to augment competence and efficiency by employing technological initiatives inside their territories.

Propaganda and Misinformation

The precise fights of the Cold War between the United States and the Soviet Union were argued on the theoretical front: opposing democracy and capitalism together with totalitarianism and communism. A segment of the psychosomatic conflict encompasses the use of propaganda (Senn, 2015).

Outlining the usage of propaganda and disinformation longitudinally from Soviet intelligence attacks in Afghanistan in the 1980s to FSB and GRU intelligence attacks in Georgia in 2008, a thorough examination of Russian intelligence acts in Ukraine from 2013–2015 demonstrates how the conventional influence of propaganda and disinformation has developed and multiplied, leading to truth misrepresentation and bias both within the aimed zone and outside. Still, it also explains how the ultimate aims of handling a populous's collective attitudes by manipulating significant symbols have endured. This manipulation allows for the creation of policy contestation both domestically and internationally where none previously existed. It takes facts and makes them fictions and preys on the conditions and foundations of how humans make decisions. The considerable exploitation of information may tilt rational biases and change inclinations to tolerate risk and return.

Conventionally, the use of propaganda was restricted to a controlled fixed trajectory for intelligence and news distributions. Newspapers, radio, perhaps television, and oral communication necessitate the aim to be in attendance when communicating the information. Predictable propaganda and misinformation entailed that the recipient captures the story; the associations were rare and far between.

As the number of sources of information accessible in daily life has increased, so too has the number of nodes at which to manipulate the overall information environment. As that environment has become increasingly polluted, targets are now required to have a filtering mechanism. People can consume information 24 hours a day from various information sources that often provide contradictory information. They want to try to shape reality out of an excess of resources. Propaganda, whether white, gray, or black, and disinformation are exceptionally problematic to differentiate. Combined with the intricacy are bot cognizant and insensible initiators of information falsification in a worldwide interchange fixed to several bits of information. Generally, any newspaper report circulated online has added a remarks piece, filled with hundreds and sometimes even thousands of comments, that can overpower or alter the meaning of a story or demonstrate information. Signing in to social media networks, such as Facebook, Twitter, Instagram, or whichever others provides a gate to narratives intended to influence and manipulate the circumstances. In this modern information setting, different devices for picture maneuvring, video editing, text, and voice exploitation exist and are utilized to change all qualities of information to originate propaganda and disinformation.

Giannetti (2017) argues that it is a duty to alert to support America's fight against Russian disinformation. He states that this is the start of a different era regarding how individuals interconnect personally to a national level. He noted the absence of protections to preclude the diffusion of disinformation for DOD networks or public networks. He also highlights the technical complexities inside Russia's cyberattacks and modes of political warfare in addition to Moscow's main motives. He thinks we can learn from looking at Estonia or Ukraine as the issues can happen here in the U.S. unless we start protecting our systems.

Fitzgerald & Brantly (2017) conducted a study on the role of propaganda in the 21st century where they examine three cases to reveal different stages of success when involved with hostile propaganda and disinformation campaigns throughout clash situations. Individually, the cases demonstrate the significance of countries, and in those occurrences, the Russian Federation put on fruitful falsification of the information situation.

The first case highlights the Ukraine case with Russia that started in November 2013. Mobile devices were practically abundant in Ukraine and Russia, and the increasing number of smart devices with photo and video capabilities was extensive. Equally, both nations had useful Internet. Ukraine has been subjected to wide-ranging Russian deception and propaganda efforts. Those raids were planned to conceal the subjugation of independent grounds, biasing voting processes and election results, hiding the supply and usage of arms, the number of refugees, and the configuration and use of forces. In the second case, the authors highlight some tales from the 2008 Georgia war. In 1988, a minor clash exploded between Georgia and Russia over the fate of South Ossetia. The general objective of the aggressions between Russia and Georgia was the determination of political power over Abkhazia and South Ossetia. Equally, both countries had reasonable access to the Internet, and by extension, global information environments. In the last case, the Soviets employed propaganda to attain three main goals supporting combat operations in Afghanistan. The authors conclude that propaganda and disinformation inserted into the worldwide information system, recognized as cyberspace, have substantial implications in today's digital environment. Strategically employed, they may assist major political movements that break or weaken policy responses. They moreover present a direct and significant threat to national security locally and internationally. Individually, the cases demonstrate the significance that countries, and in those occurrences, the Russian Federation, put on fruitful falsification of the information situation. Confronting and combatting Russian disinformation in the United States will not necessarily take hauling out agencies past, or will it take an entirely novel approach.

Internet

We know in today's world, the Internet is so significant. The Internet is part of our modern society and future, and countries should always protect human rights for sure. In the Philippines, Senator Miriam Defensor-Santiago presented a bill creating a Magna Carta for Philippine Internet Freedom (MCPIF) that replaced the enacted and controversial Republic Act No. 10175 Cybercrime Prevention Act of 2012. Brazil developed some laws to protect and expand the right of internet users to open, universal, and free web use. The impact of the Magna Carta lies in its account as the initial case where a printed manuscript controlled the influence of a ruler. As we know, the U.N. human rights council passed a non-binding resolution this past June to condemn countries that intentionally take away or disrupt their citizens' internet access. This resolution was opposed by countries including Russia, China, Saudi Arabia, South Africa, and India.

The economics of net Neutrality is sensitive (Gants, 2015). Net Neutrality is a disputed term with competing definitions (Gants, 2015). Net Neutrality, also denoted as the Open Internet, is a belief that forbids ISPs from speeding up, slowing down, or obstructing any subject on the Internet. Net Neutrality offers clients the liberty they desire as they glance across web pages, applications, or any other matters accessible through the Internet. In 2011, Hart conducted a study on the net neutrality debate in the U.S. The purpose was to communicate and rationalize the views behind the U.S. net neutrality debate for the period between 2006 and 2010 and to forecast its likely potential path. Those in support of net Neutrality contented for the regulation actions of the proprietors of Internet infrastructure to conserve free speech, preclude any possible exploitation of power by telecommunications and telephone companies, and encourage internet-based commercial innovation (Hart, 2011). Among the support were Elie Noam, the FCC chairman Michael Powell, and Tim Berners-Lee, the chief architect of the World Wide Web and the inventor of the hypertext markup language (HTML). Arguments against Net Neutrality were on the rise as well. In 2006, the U.S. Internet Industry Association(USIAA) opposed net Neutrality, claiming that the concept was vague and its definitions are always; thus, legislation to control or ban certain access and type of information may be hard. Opposition to net Neutrality fit nicely within the antiregulatory frame that permitted Republicans to win the Presidency and control Congress.

As we've witnessed in the news, repressive regimes are using censorship and blocking and trying to keep the media in control, not to say intimidating witnesses, blocking some websites, among other practices. While one should argue for government control in most cases, we cannot but wonder whether total control is a good approach.

A netizen contributes to the growth and use of the Internet, which is not well received by authoritarian regimes. In 2011, netizens were at the heart of the political revolutions in the Arab world and another place too. Tunisians learned about the vendor who set himself on fire in Sidi Bouzid, thanks to the Netizens. The report mentioned many ways countries can block people from the Internet. Some instances may be arbitrary; others may be due to violations such as intellectual property; others may be political and not forget cyber-attacks.

Countries and some states did restrict and manipulate content from the Internet without any legal law or justifications. The report mentioned time blocking and banned people from accessing the Internet during critical political events and country unrests.

According to Segal (2013), China has been drawing unwanted attention with its hostile attempts to breach U.S. government and industries networks to sneak information. Given the lack of disruptive innovations, Chinese leaders took actions to reduce their chances of being stragglers in worldwide competition; this is why we did see an increased number of attacks and a growth in the targets of cyber espionage from army networks to high-tech and even progressive industrial businesses. The strikes were intended to give China a competitive financial and commercial advantage, among other benefits. The Chinese have repudiated accountability for cyber espionage, and their President Xi said that China too is a target of attacks.

The U.S. and China have mutual concern in defending nationwide infrastructure from third-party strikes. However, they both are not giving up cyber espionage. One of the problems relates to the way they are defining the act. For instance, the United States separates the attacks from those dealing with intellectual and industry types that may be military and threaten the country. On the other hand, Beijing condemns Washington for being the first to militarize cyberspace by establishing the U.S. Cyber Command and advancing provoking cyber abilities. There are many problems, but the mistrust between countries is escalating the issues. Often, the intelligence community gathers classified information, and most often, some of this information is not that classified and/or not interpreted right. So many costly mistakes happened due to the lack of clear policies, people's incompetence, lack of credibility and accountability, and often due to some people's egos and own political agendas and personal gains and/or corruption. The way we vote or elect is going to be affected too. If television ads aim to inspire viewers to vote, volunteer, or donate money, thanks to the Internet, there appear to be far superior methods to influence people (Cary, 2010).

Social Media

With changes and advances in technology, we will always have challenges. According to Clay, social media's actual capability rests in reinforcing civil society and the public, and change will come over time. Social media is and will continue to be a principal part of our political debates as it found a level of transparency that was missing in our country. There are surely unintended effects, too, one of over-democratization. There's a domino effect, too, in terms of transparency.

Shirky (2011) presented two arguments against the idea that social media will make a difference in politics and change. The very first can be attributed to the tools that may be ineffective, and the second is that the outcome is harmful as governments with repressive regimes are suppressing these changes well.

The propagation of information through social media has steered in different intelligence gathering and investigation (Morgan, 2016). Social Media Intelligence (SOCMINT) is often booming as an added open-source intelligence career or perhaps under the growing cyber sectors. Morgan (2016) investigated the strategic and tactical connotation of collecting and assessing the increasing volume of information accessible amongst various social media platforms. His research suggests a key methodology to improve and apply SOCMINT into the Intelligence Community (I.C.) to challenge this mounting pattern change in intelligence collection.

With predictive analytics and other real-time tools in place, the U.S. I.C. will gather and interpret real-time information published from everywhere in the world. Still, they will also integrate it into planned actions and strategic policy sanctions sooner than any recognized restraint executed historically by the I.C.

No one can deny that social media did advance. Indeed, we witness state, local, and even international governments using analytics to reduce traffic congestion, supervise public utilities, appraise and predict crime and potential terrorist activities, and follow trends in almost every topic.

The digital information background creates challenges for traditional practitioners of propaganda. The transmission of the information has made it further problematic to catch the thoughts of a target populace throughout independently published pieces or news reports on radio or television. Furthermore, the current information environment is not containable geographically as information diffusion through disparate networks is rapid.

Conclusion

The Internet opened up our economy, changed the way we communicate, destroyed barriers, and defied time. It is easy and convenient to find any news across the globe and any critical information. The Internet shapes our perceptions and conceptions of right and wrong and opens our eyes to many neglected issues and problems. It is also creating additional and new problems too, not just overlooked opportunities.

These are different times and technologies and evolution and require a different outlook and a different perspective on governance, regulations, and what rights a person should have. With the rise of wars across the planet, we often see decreased rights for some minorities and unprivileged people. Our declaration of independence's basic premise is the freedom of speech, among other rights. Often, we seem to live in a zoo, where the powerful and corrupt often eat and destroys innocents and sadly go unpunished. I would assume that it is fair to say that since everything and in particular information is within reach when it comes to the Internet, people should have the right to freely assess the credibility of the information presented and make their own decisions. However, we need to be careful, as too much freedom is not always healthy, so we need balance.

Recommendation & Area for Future Work

According to Taddeo (2017), the foreign ministers of the G7 countries supported a 'statement on reliable countries conduct in Cyberspace' (G7 Declaration, 2017). The statement tackles an increasing unease about international loyalty and the security of our civilizations after the fast-paced increase of cyber attacks. Technology can easily detect the difference between what they call intelligence gathering as opposed to cyber attacks. These technologies that generated mistrust between the two countries (the U.S. versus China), among others, can similarly offer resolutions. Our National Security Council and State Department officials should open a line of communication with the Chinese Ministry of Foreign Affairs, especially when the Chinese did open an office for cybersecurity issues.

A cyber attacker's usage of bits and bytes impends the same network impairment as missiles and grenades. Assaults through the fifth element are constant nowadays. Stevenson & Prevost (2013) recommends four acts in parallel, starting with a resolute action by business and government to safeguard our country's electrical grid and infrastructure. The leaders should establish a culture of change. Incentives must be initiated to promote a further sensible and vigorous portioning of information by electricity and other critical infrastructure companies. In addition, Congress must hold its cybersecurity role. The Securities Exchange Commission must maximize its powers to guarantee organizations every quarter sufficiently reveal cyberattacks, cyber risks, and actual mitigation plans.

For sure, though, the current way of thinking in politics is not working; our strategies and policies are far from perfect and just. We need a reform on many levels and need to have an entire education system and other things for the Netizens to grow and progress. It does not hurt to revisit the bill of rights and update it.

This research motivates the need to conduct a detailed comparison and analysis on intelligence gathering and policy issues across the country and selected parts of the world. This article offers the first comprehensive examination of the use of the Internet to spread misinformation and the emerging interplay between social media and the rise of misinformation and propaganda as the most pressing issues of our time.

References

Bayraktar, G. (2014). The new requirement for the fifth dimension of war: Cyber intelligence. *International Conference on Cyber Warfare and Security*, 9.

Beato, G. (2014). From petitions to decisions. *Stanford Social Innovation Review*, 12(4), 20

Cary, K**. (**2010).5 Ways New Media Are Changing Politics: Emerging communications phenomena have transformed the political process.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cybersecurity investment. *Decision Support Systems*, 86, 13-23. doi:10.1016/j.dss.2016.02.012

Fitzgerald, C. W., & Brantly, A. F. (2017). Subverting reality: The role of propaganda in 21st-century intelligence. *International Journal of Intelligence and Counter-Intelligence*, 30(2), 215-240. doi:10.1080/08850607.2017.1263528

Haines, G. R (2004). An Emerging New Field of Study: U.S. Intelligence', Diplomatic History 28 (3), .441–450

Hart, J. A. (2011). The net neutrality debate in the united states. Journal of Information Technology & Politics, 8(4), 418-443. doi:10.1080/19331681.2011.577650

Iasiello, E. (2016). China's three warfares strategy mitigates fallout from cyber espionage activities. *Journal of Strategic Security, 9*(2), n/a. doi:http://dx.doi.org.ezproxy.libproxy.db.erau.edu/10.5038/1944-0472.9.2.1489

Giannetti, W. (2017). A duty to warn: How to help America fight back against Russian disinformation. *Air & Space Power Journal*, 31(3), 95.

Greiman, V. (2018). Cyber espionage: The silent crime of cyberspace. Paper presented at the

245-251, XIII.

Maher, D. (2017). Can artificial intelligence help in the war on cybercrime? *Computer Fraud & Security*, 2017(8), 7-9. doi:10.1016/S1361-3723(17)30069-6

Morgan, M. F. (2016). The necessity for social media intelligence in today's evolving battlefields. *Military Intelligence Professional Bulletin, 42*(2), 40-42,45.

Muller, L. (2014). The impact of the mass media on the quality of democracy within a state remains a much-overlooked area of study. An overlooked area of study. Euro Crisis in the Press. http://blogs.lse.ac.uk/eurocrisispress/2014/12/10/the-impact-of-the-mass-media-on-the-quality-of-democracy-within-a-state-remains-a-much-overlooked-area-of-study/

Ronczkowski, M. R. (2017). Terrorism and organized hate crime: intelligence gathering, analysis, and investigations CRC Press.

Segal, A. (2013). The code not taken: China, the united states, and the future of cyber espionage Bulletin of the Atomic Scientists, 69(5), 38-45. doi:10.1177/0096340213501344

Senn, S. (2015). All propaganda is dangerous, but some are more dangerous than others: George Orwell and the use of literature as propaganda. *Journal of Strategic Security, 8*(5), n/a. doi:http://dx.doi.org.ezproxy.libproxy.db.erau.edu/10.5038/1944-0472.8.3S.1483

Shirky, C. (2011). The political power of social media: Technology, the public sphere, and political change. Foreign Affairs, 90(1), 28-I.

Stevenson, J., & Prevost, R. J. (2013). Securing the grid: Information sharing in the fifth dimension. *The Electricity Journal*, 26(9), 42-51. doi:10.1016/j.tej.2013.10.003

Taddeo, M. (2017). Deterrence by norms to stop interstate cyber attacks. Minds and Machines, 27(3), 387-392. doi:10.1007/s11023-017-9446-1

Taub, A & Fisher, M. (2017). The "deep stat state." *Defense Journal*, 20(9), 90.