ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 6| June 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

THE IMPACT OF DISINFORMATION ON NATIONAL SECURITY POLICYMAKING: A REVIEW

Mohammed Hafiz Nabila[a], Matilda Thompson[b*]
[a] *East Tennessee State University, Johnson City, TN, USA*
[b] *Department of English, University of Ghana, Ghana*
Corresponding Author: Matilda Thompson

Article DOI: https://doi.org/10.36713/epra22781
DOI No: 10.36713/epra22781

ABSTRACT

With the United States being the target of sustained disinformation campaigns from its adversaries in the last few years, it is obvious that national security and policy formulation have been saddled with a different kind of challenge- one that attacks the fabric of the U.S. society by directly influencing perceptions and actions of Americans. This review highlights the different information terminology, traces the beginnings of disinformation, and its implications on national institutions and national security. This paper examines disinformation within the context of Information Warfare and Cognitive Warfare. Policymaking to counter disinformation must be deliberate and sustained, involving all stakeholders in American society, and avoid overconcentration on foreign actors while internal elements cause deep divisions and continue to alienate segments of the society. This balanced focus on internal and external threats will enhance the United States' chances of winning this war.

KEYWORDS: *Disinformation, National Security, Information Warfare, Cognitive Warfare*

INTRODUCTION

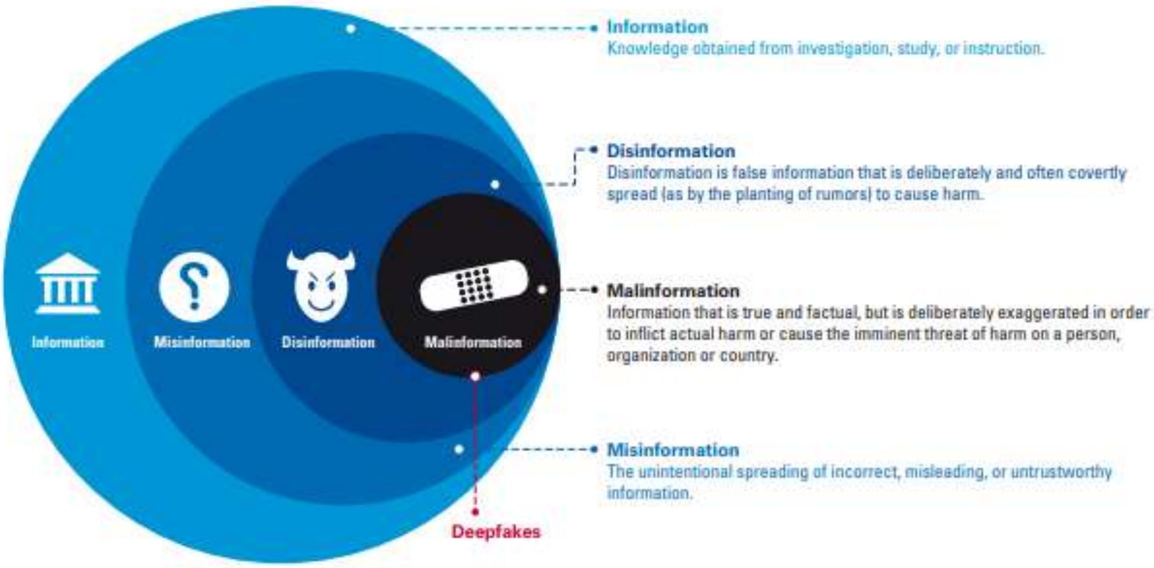
According to Wardle and Derakhshan (2017), disinformation is "information that is false and deliberately created to harm a person, social group, organization or country" (Wardle & Derakhshan, 2017, p. 20).

According to the European Commission (2018), disinformation is understood as verifiably false or misleading information that is created, presented, and disseminated for economic gain or to intentionally deceive the public, and may cause public harm (p.3). According to the American Psychological Association (APA), disinformation is inaccurate information that is intentionally used to influence public opinion through the systematic misrepresentation of facts (APA, 2025).

The European Commission has developed a concept of disinformation around 3 key criteria: it is false or misleading, can be verified as such, has been created or shared maliciously rather than accidentally, and serves either (financial) interests or a malicious intention to mislead the public. Notably, the definition put forth by the Commission adds a consequentialist dimension by framing the potential for public harm as a defining feature, acknowledging the importance of the societal impact of disinformation, beyond mere factual inaccuracy. This all-inclusive definition takes note of the purpose of disinformation campaigns and their ability to impact the real world (European Commission, 2018).

There are three broad reasons (and acts) for disinformation. First, there's a financial incentive: Creators can cook up clickbait or divisive content to zero in on clicks, views, and advertisement money. Second, there is the political dimension, as disinformation is used as a weapon to manipulate public perceptions, electoral results, or policy choices, whether by domestic actors or by foreign agents seeking to meddle in the affairs of another country. A third motivation for disinformation describes a different psychological and social phenomenon, wherein individuals or groups intentionally propagate false information, with disruption as the end itself (Northeastern University Library, 2024).

Disinformation can also be termed as false or manipulated information created and deliberately spread to intentionally mislead the recipient. Such communication includes demonstrably false information or the strategic distortion of factual information to mislead target groups. Although it is sometimes described colloquially as propaganda or fake news, disinformation is a specific kind of deceptive communication, one that involves intentional and not just prejudicial falsification of information (Massachusetts Institute of Technology [MIT] Libraries, 2025).



Information
Knowledge obtained from investigation, study, or instruction.

Disinformation
Disinformation is false information that is deliberately and often covertly spread (as by the planting of rumors) to cause harm.

Malinformation
Information that is true and factual, but is deliberately exaggerated in order to inflict actual harm or cause the imminent threat of harm on a person, organization or country.

Misinformation
The unintentional spreading of incorrect, misleading, or untrustworthy information.

Figure 1: Differences in information terminology by Boevink, Pronk, & Mok (2023)

A Brief History

Fake news isn't a new phenomenon — it dates back to the very idea of news itself, 500 years ago, with the invention of print. It has been around longer than verified, "objective" journalism, which only became the norm a little more than a century ago. From the beginning, fake news has been sensationalist and extreme, made to induce strong emotions and confirmation biases (Snyder, 2016).

Fake news emerged around the same time as the Gutenberg printing press (1439) and grew with mass communication. Information came from official and eyewitness accounts, but with no journalistic standards, so readers had to develop critical evaluation skills. Before the French Revolution, many pamphlets containing divergent financial statistics circulated in Paris, originating from many political sides. Eventually, leaks from the government allowed the public to better understand everything that was happening, though good analysis still relied on a person's ability to analyze and decipher factual from fake information. The newspapers of the early 19th century gave birth to both investigative journalism and sensationalism. Publications that were mere fabrications and exaggerations produced to provoke widespread anger or sympathy were characteristic of the sort of journalism practiced in the Gilded Age. Repercussions from these dishonest tactics fueled a backlash and a demand for fact-based reporting. By the 20th century, objective journalism had developed into a successful business model that ideally put dedicated reporters on the beat, thereby building trust with the public. While partisan reporting continued, objectivity remained the ideal. Journalists of the 1960s upended establishment narratives but still operated based on facts. This journalism framework lasted until digital media transformed the industry. Particularly in today's world of fast-moving internet and social media, networks for transmitting unverified information have operated easily, leading to conditions in which fake news grows using methods similar to those of yellow journalism in the past (Snyder, 2016).

Distinguishing Disinformation from Misinformation

Wardle & Derakhshan (2017) distinguished between misinformation and disinformation using intent. Misinformation is non-intentional and may be born out of error or negligence, while disinformation is, by definition, a deliberate act of deception to harm. Information warfare theory and cognitive hacking are among the theoretical models encompassing how adversaries systematically weaponize disinformation to exploit weaknesses in their target's information ecosystem. Historical examples, like Soviet-era active measures and more modern Russian influence operations — like those in the 2016 U.S. elections — have shown how disinformation can impact national security outcomes (Rid, 2020).

Modern and Historical Examples of Disinformation with National Security Implications

The 1796 presidential election was an early manifestation of the weaponization of false news and disinformation to achieve political ends. This was an election between John Adams and Thomas Jefferson. Both candidates resorted to the deliberate spread of false information. They used newspapers and writers of these media and generated their false claims about their opponents from their camps (National Constitution Center, 2023). While there were no foreign influences during this period in history, this is an example of the utility of fake news to achieve political aims.

In modern times, Russian interference in the 2016 U.S. elections stands out as one of the most notable examples of a coordinated disinformation campaign with far-reaching consequences for national security. A Russian government-led action using the Internet Research Agency generated fake social media accounts, spread false information, and used other strategies to sow deep division within the populace. The integrity of the process before, during, and after the election was called into question (U.S. Senate Select Committee on Intelligence, 2019; Mueller, 2019).

The COVID-19 pandemic was another recent occurrence in which the effects of disinformation were felt in the United States and beyond. This disinformation campaign was characterized by false information about treatment, the source of the virus, and how it spreads (European Commission). The United States was targeted by Chinese state-backed disinformation operations, which sought to shift the origins of the virus to a U.S. military visitor to Wuhan (patient zero) and a U.S. Army laboratory in Maryland. China later retracted these claims about the origins of the virus (Wendler, 2021). Regardless of this retreat from their earlier claims, this is yet another example of how disinformation fuels global panic and chaos during times of uncertainty.

Implications of Disinformation on National Security

The increase in digital platforms, the rise and rapid development of Artificial Intelligence, and a deeply divided political landscape have made the impact of disinformation more pronounced.

Disinformation campaigns have led to a reduction in public trust of the political system. As a result of these campaigns, the integrity and independence of constitutionally mandated bodies and processes have been questioned, and doubts have been cast on the sanctity of their work (Sanchez & Middlemass, 2022).

The Collaborative Multi-Racial Post-Election Survey (CMPS, 2021) found that 57% of the white population in America suspected voter fraud in the U.S. presidential election of 2020, while 26% of this demographic believed there was fraud. Also, an NPR/Ipsos survey revealed the impact of disinformation, as 70% of Republican respondents are of the view that the 2020 presidential election was manipulated in favor of Joe Biden (Rose & Baker, 2022; Newall, Jackson, & Diamond, 2022)

When marginalized groups and minorities are targeted with disinformation campaigns, it aggravates grievances these groups have long held and reinforces their distrust of socio-political establishments as a result of these partialities (Kuo & Marwick, 2021). For instance, from political actors using disinformation to advance policies that promoted discrimination, to campaigns that targeted immigrants as taking jobs from non-immigrants (Covert, 2019), and media depictions of Black people as criminals being transplanted played out in legal and other public systems (Noble, 2014).

14% of people interviewed in a survey admitted to sharing political information they knew to be false. There is a relationship, this study found, between people who are willing to share false information and their encouragement of acts of political violence and negative social disruptions. The people who admitted to sharing false information online were also inclined towards violent behavior from radical sets (Littrell et al., 2023).

Social harmony, trust in democratic institutions and systems, public health and safety, and economic stability – all these are under threat through disinformation. People living on the margins of society bear the weight of these campaigns. Their plight is exacerbated by deep-rooted systemic imbalances, and the mechanisms that govern the workings of social media platforms also leave them at the receiving end of disinformation campaigns, as they are among the worst affected.

THEORETICAL FRAMEWORKS

Information Warfare Theory

“Information warfare is a process of achieving strategic goals (interests) of any organization by offensive and defensive activities in the information space (infosphere) inspired and carried out against other organizations for self-protection and self-defense” (Białoskórski, 2023, p. 8)

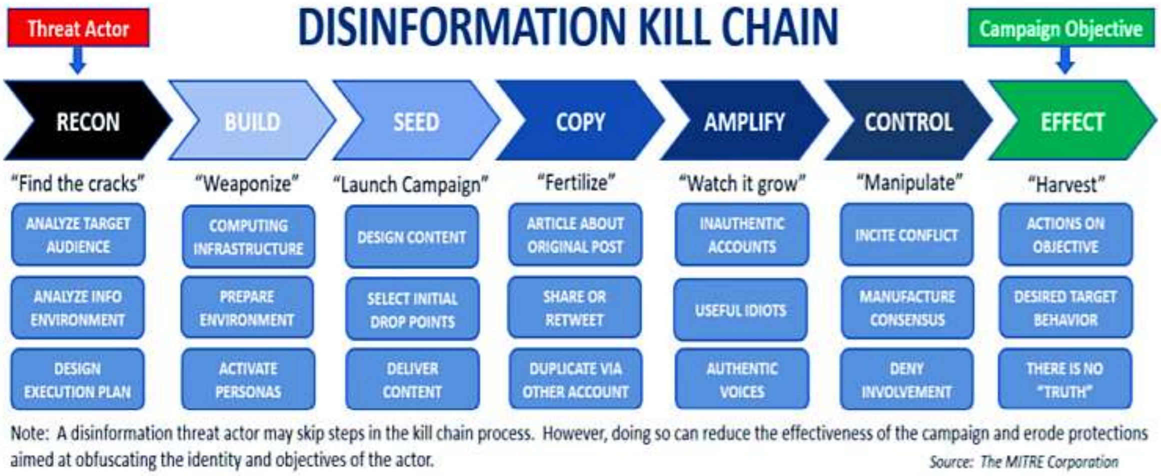
“The integrated employment during military operations, of IRCs in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own” (Department of Defense, 2012, page I-1). IRCs refer to Information Related Capabilities.

Disinformation in Information Warfare

Disinformation is one of the strategies adopted in Information Warfare. Disinformation is employed to create division, raise questions about the integrity and independence of state institutions, and disturb the balance of society. It is targeted towards both domestic and foreign publics.

Cyberattacks, strategies that affect the economies of territories, and disinformation are some features of Information Warfare. The success of disinformation campaigns stems from the fact that they take advantage of people’s preconceived ideas about others, issues, and their world, magnify existing conflicts, disagreements, and strife, and flourish in the domain of social technology platforms where news spreads fast. The financial and technical demands of carrying out an online disinformation operation are relatively lower, leading to a surge in users and the volume of false information that is produced and spread online (CB Insights, 2020).

The United States Department of Homeland Security has demonstrated how disinformation is operationalized using a Figure by Adam Cambridge of the MITRE Corporation.



Note: A disinformation threat actor may skip steps in the kill chain process. However, doing so can reduce the effectiveness of the campaign and erode protections aimed at obfuscating the identity and objectives of the actor.

Source: The MITRE Corporation

Figure 2: How disinformation is operationalized using a figure by Adam Cambridge of the MITRE Corporation (Department of Homeland Security, 2021).

On a global level, in 2019, 70 countries- representing an upturn of 150% from 2017- used social media to disseminate false information to muzzle opposing voices and discredit political opponents (Bradshaw & Howard, 2019).

In the same research conducted by Bradshaw and Howard (2019), Twitter and Facebook were the most prominent platforms for disinformation in the United States. Additionally, government agencies, political parties, and private contractors were identified as the agents using online platforms to manipulate public opinions.

Apart from the low cost of online-driven disinformation campaigns, another major driver of the success of disinformation operations is access to the internet (CB Insights, 2020). The whole operation of online disinformation hinges on access to the internet, and with countries like the U.S., which have a high internet penetration. According to the Pew Research Center (2024), 96% of adults in America use the internet.

Cognitive Warfare

"Cognitive Warfare" is the convergence of "Cyber-Psychology," "Weaponization of Neurosciences," and "Cyber-Influence" for a provoked alteration of the perception of the world and its rational analysis in the military, politicians, and other actors and decision makers, for the purpose of altering their decision or action, for a strategic superiority at all levels of tactical intervention concerning individual or collective natural intelligence, as well as artificial or augmented intelligence in hybrid systems"(Claverie, Prébot, Buchler, & du Cluzel, 2022, p. xiv)

"Cognitive Warfare is the most advanced form of human mental manipulation, to date, permitting influence over individual or collective behavior, with the goal of obtaining a tactical or strategic advantage. In this domain of action, the human brain becomes the battlefield. The pursued objective is to influence not only what the targets think, but also the way they think and, ultimately, the way they act. Cognitive Warfare is necessarily associated with other modes and domains of action for reaching targeted brains, such as Cyber Warfare and Information Warfare" (Claverie & du Cluzel, 2022, p. x).

Avila (2024) describes Cognitive Warfare as "a conflict domain targeting human cognition through disinformation, neuro technologies, and algorithmic amplification" (p.1)

"Cognitive warfare (CW) exploits the convergence of nanotechnology, biotechnology, information technology, and cognitive science (NBIC) to manipulate perception, decision-making, and behavior" (Avila, 2024, p.1)

Cognitive warfare involves "psychological tactics, information manipulation, and cognitive strategies (narratives, semiotics, iconographies) to influence emotions, beliefs, perceptions, and behaviors of individuals, groups, or whole populations" (Nikoula & McMahon, 2024, p. 2). The contention or warfare takes place in an individual's mind. "Ideas," "emotions," and "perceptions" are the domains in which Cognitive Warfare works (Nikoula & McMahon, 2024).

Disinformation in Cognitive Warfare

A key strategy of cognitive warfare is disinformation. It consists of the erection of false narratives and the distortion of truth. This impacts people's understanding of issues and makes them more prone to believe untruths. This manipulation of people's biases in perception can lead them to align with certain factions, associations, or sects based on shared beliefs and set them on a collision course with other bodies whose views they strongly oppose (Nikoula & McMahon, 2024).

Cognitive Warfare takes place with the combination of the following: cyber, information, psychological, and social engineering functions all working in harmony to control individuals or groups (Claverie, Prébot, Buchler, & du Cluzel, 2022).

How Disinformation Spreads

Bradshaw & Howard (2019) note that the use of data, automated systems, and algorithms in conjunction with mental manipulation to influence decisions, perceptions, and attitudes on social networks ("computational propaganda") has become a popular mode of influencing and interacting with people, not just by disinformation agents but by political actors as political promotional strategy.

The CISA (Cybersecurity and Infrastructure Security Agency [CISA], 2022) has identified strategies used to spread disinformation. People engaged in disinformation generate false online profiles and internet sites. They arrogate to themselves false qualifications and manufacture membership and/or leadership positions of non-existent policy or educational entities. This is to enhance their authenticity and make their claims genuine. Online materials like audio, videos, and photos are digitally forged with the use of AI to look almost the same as the original, with the sole intent to deceive consumers of this information. Another strategy to spread disinformation is the presentation of false information as closely guarded secrets that are revealed to a group of people. While these stories are false, they are crafted to build on false perceptions that some people may have about issues, events, and personalities to fortify that report to the select audience. Fake profiles are also used to saturate the online environment with huge volumes of the same information. This is described by CISA as "astroturfing (Zhang, Carpenter, & Ko, 2013). CISA also describes "flooding" as a deluge of online posts on online platforms. What "astroturfing" and "flooding" seek to do is create a false impression of complete endorsement or rejection of whatever issue is in discussion. This also suppresses organic or genuine voices from being heard. Disinformation also thrives when there are insufficient and unsatisfactory responses to problems, complaints, or situations. These merchants of disinformation create false information to fill this void and create a demand for this false information. When people search for information, all they get is this carefully engineered false information. This aids believability because of the absence of verifiable and credible information to counter these false claims. Sometimes, disinformation is spread by unwitting agents. These are people and entities who are targeted by the disinformation agents to spread this false information by virtue of the prestige, respect, and credibility they have built for themselves over a period.

Disinformation agents are able to spread false information on social networks because the technological mechanisms of these networks make it possible for these agents to carry out their agenda. In a study that analyzed activity on Facebook, Instagram, Twitter, and Reddit, researchers identified legitimate methods ("official APIs") and illegitimate methods ("unofficial APIs"). These "unofficial APIs" were used to spread disinformation. Application Programming Interfaces (APIs) allow interaction between 2 different programs. From an analysis of these tools, the study found features that showed that unapproved methods involved replicating how humans acted on social media platforms. This method of copying human actions is employed when disinformation agents can no longer access the programming interfaces of social media networks through code repositories (Ng & Taeihagh, 2021).

Among the types of accounts used to spread disinformation on social networks are computer-generated accounts that behave like human beings in their social media activity (bots), false accounts created by disinformation agents (fake accounts), accounts created by actual people, and accounts that combine human and computer features (cyborg accounts) (Bradshaw & Howard, 2019).

Policy-Altering Incidents of Disinformation

The U.S. government imposed sanctions on "Russian security personnel and agents" for offences including disinformation and their meddling in the 2016 U.S. elections (Rosen, 2022). In response to these acts by Russia, the Cybersecurity and Infrastructure Security Agency developed the Shields Up Technical Guidance. These are guidelines for individuals, families, organizations, and heads of institutions to conduct themselves on the internet to protect themselves from cyber threats (CISA, n.d.; CISA, 2022).

In the wake of the COVID-19 pandemic, disinformation campaigns were launched targeting Americans with false information about vaccines. Russia orchestrated this campaign (Green, 2021). According to the U.S. Department of State, flooding online platforms with different versions of reports to disinform allowed Russia the leeway to deny responsibility for these campaigns. It also enhanced the spread of these false reports and deepened their impact on the public (U.S. Department of State, 2020). People were recruited to magnify issues with the vaccines and spread false information about them. These agents created documents that combined some factual information with stark untruths. When this campaign was uncovered, 65 accounts were removed from Facebook and 243 from Instagram. They were found to have originated from Russia, and they targeted the AstraZeneca and Pfizer vaccines (Meta, 2021). This was a classic case of Coordinated Inauthentic Behavior (CIB) where people organize themselves to mislead others about who they are, what they stand for, their motives, and actions (Meta, 2018). Facebook credited collaborative efforts between media organizations for the discovery and exposure of this campaign (Meta, 2021).

As a result of disinformation, many people were reluctant to get vaccinated for COVID-19. This reluctance was hinged on misgivings about the possible implications of the vaccine on their health (Neely et al., 2022; Daly, Jones, & Robinson, 2021; Rief, 2021). This fear, expressed by sections of the American public, aligns with targeted disinformation campaigns created by foreign actors online that have been discussed in earlier sections of this paper.

In response to issues of election meddling by Russia in the 2016 U.S. election, the Honest Ads Act was introduced to enhance laws on how individuals and parties fund their political campaigns, especially in relation to online advertisements. This Act was to lay bare before the public all who sponsored online advertisements for politicians. This was a measure to curb foreign interference in political campaigning and elections (Lau, 2020; Honest Ads Act, 2017).

The Department of Homeland Security recognized the physical and non-physical systems and structures that facilitated the organization of elections as essential facilities. As such, any operation that causes these systems and facilities to not work in the interest of the United States will have severe consequences for the country and its security. The Cybersecurity and Infrastructure Security Agency (CISA) was established to secure these systems and structures and address anything that threatens their integrity (CISA, n.d.).

Safeguards Against Disinformation

As the discussions in preceding sections have demonstrated, disinformation is an operation that targets people's minds. Therefore, it has the potential to and has impacted a range of sections of American life. There have been responses and counteractions from federal and non-federal bodies to acts of disinformation.

The Department of Homeland Security started tackling disinformation on social networks in 2018. These initial countermeasures were directed towards election-related issues or to what they described as "distinct mission operations". The establishment of the Cybersecurity and Infrastructure Security Agency (CISA) was to secure elections and election-related infrastructure (U.S. Department of Homeland Security, Office of Inspector General, 2022).

The Departments of State, Homeland Security, and Defense have adopted strategies to detect disinformation campaigns aimed at the American public or audiences abroad. These departments check social media activity to spot disinformation activities and those behind them. These departments counteract these disinformation operations by detecting, sensitizing, and investigating these acts. They educate the United States citizenry and foreign allies about these operations. For disinformation activities that emerge within the United States territory from Americans, these departments adopt wide public education and sensitization strategies and provide the public with factual information on the issue for which they are being misinformed (U.S. Government Accountability Office [GAO], 2024).

Some pieces of legislation have been passed to address disinformation. The National Defense Authorization Act for fiscal year 2017 established the Global Engagement Center (GEC) as an agency within the Department of Homeland Security to oversee the work of government institutions countering foreign disinformation operations (U.S. Congress, 2016). It must be noted that the center was closed down in 2024 after complaints from political actors that their work amounted to censorship and a violation of democratic freedoms (Guo, 2025).

California has media literacy legislation that incorporates media literacy training into K-12 curricula (California State Legislature, 2018). Bills like the Honest Ads Act, Educating Against Misinformation and Disinformation Act, and the Platform Accountability and Transparency Act have not been passed into law. West (2017) urged the United States to be an example for other countries to emulate by not curtailing the media's freedom to report the news. Journalists should be free to report on happenings in all aspects of national life.

Media literacy has been identified as a proven countermeasure against disinformation. This involves teaching people how to detect falsehoods and identify sources of these falsehoods (Bulger& Davidson, 2018; Adjin-Tettey, 2022). Media literacy is defined as "The ability to access, analyze, evaluate, create, and act using all forms of communication" (National Association for Media Literacy Education, n.d.). Media literacy programs and policies from federal to state governments for students to make them adept at identifying disinformation strategies, education and outreach programs for marginalized communities, and ethnic/racial minorities make them less susceptible to disinformation strategies that reinforce deep-seated mistrust, historical tensions, false perceptions about policy biases that have led to deep divisions over the years, and gender biases often targeting women in public office.

It must be noted that implementing these countermeasures has not been without challenges.

The First Amendment, which guarantees free speech, is a major drawback to countermeasures and the passage of legislation against disinformation in the United States. In *Reno v. ACLU* (Reno v. American Civil Liberties Union, 1997) and *Packingham v. North Carolina* (Packingham v. North Carolina, 2017), the court reinforced the supremacy of the First Amendment rights (Prendergast, 2019).

The short-lived Disinformation Governance Board, an agency of the Department of Homeland Security, also faced resistance based on concerns about the Board's threats to First Amendment rights, leading to its dissolution (Sperry, 2024; Sands, 2022).

Future Directions

States should be deliberate about providing citizens with accurate information on high-stakes issues, including elections. Some states have put mechanisms in place to do this (New Mexico Secretary of State, 2022; North Carolina State Board of Elections, n.d.; Kang, 2022; Santa Clara County Registrar of Voters, n.d.), and it would be beneficial for states that do not have such structures to emulate. States should deliberately target public education from a young age on how to evaluate news on their veracity or otherwise. States that have not already integrated media literacy in the curricula of schools should be encouraged to do so.

There is a lot of concentration on foreign disinformation campaigns from foreign actors like China, Iran, and Russia. While there is some focus on disinformation campaigns within the United States, that focus is largely on politics and political actors. With disinformation operations targeting race, ethnicity, gender, and marginalized communities, divisions have continued to deepen, mistrust has persisted, and false narratives and perceptions among these groups have continued to gain traction. There is a need to direct more action to internal disinformation campaigns that are leaving the country sharply divided along political and racial lines, and encouraging mistrust of democratic processes and institutions. While acknowledging rights granted by the First Amendment, leadership at the federal level must exhibit dexterity and creativity in policy formulation and implementation that tackles disinformation within the United States and by American citizens without compromising free speech.

CONCLUSION

The threat of disinformation is unique; it is a battle for the human mind; it requires logistics that are too difficult to find or build; and it is inexpensive. The potential of planting seeds of false information in a human mind, manipulating that human to act through a series of well-defined and calculated actions that could lead to the toppling of an entire government, leading people to sabotage their personal health and safety and that of others, and the potential to cause complete breakdown of law and order of a society through civil unrest is explosive. This is a threat that is continually evolving and whose actors are continually pushing the boundaries of technological insight and creativity to attack their adversaries. It is essential for the federal government of the United States to work in concert with state governments to bring uniformity to their response to this complex warfare. This calls for sustained, intentional action spearheaded by the federal government, in collaboration with stakeholders from all levels of American society, to significantly minimize the effects of disinformation campaigns while taking steps to forestall others.

REFERENCES

1. *Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policymaking (Vol. 27, pp. 1–107). Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c*
2. *European Commission. (2018). Tackling online disinformation: A European approach (COM(2018) 236 final). European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236*
3. *American Psychological Association. (2025) Misinformation and disinformation. https://www.apa.org/topics/journalism-facts/misinformation-disinformation*
4. *European Commission. (2018). Tackling online disinformation: A European approach (COM(2018) 236 final). European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236*
5. *Northeastern University Library. (n.d.). Fake news, misinformation, and disinformation. Northeastern University. https://subjectguides.lib.neu.edu/fakenews*
6. *Massachusetts Institute of Technology [MIT] Libraries. (n.d.). Misinformation, disinformation, and fake news. MIT. https://libguides.mit.edu/disinfo*
7. *Boevink, J., Pronk, M., & Mok, E. (2023). How disinformation might hurt your business. Compact Magazine. https://www.compact.nl/pdf/C-2023-1-Boevink.pdf*
8. *Snyder, T. (2016, December). The long and brutal history of fake news. Politico. https://www.politico.com/magazine/story/2016/12/fake-news-history-long-violent-214535/*
9. *Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.*
10. *Białoskórski, R. (2023). The theoretical concept of information warfare: A general outline. Humanities and Social Sciences Research Journal, 30(4, Part I), 7–24. https://doi.org/10.7862/rz.2023.hss.39*
11. *Department of Defense. (2012, December 10). Department of Defense Strategy for Operations in the Information Environment. Defense Innovation Marketplace. https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf*
12. *U.S. Senate Select Committee on Intelligence. (2019). Report of the Select Committee on Intelligence on Russian active measures campaigns and interference in the 2016 U.S. election: Volume 2: Russia's use of social media. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf*
13. *Mueller, R. S., III. (2019). Report on the investigation into Russian interference in the 2016 presidential election: Volume II. U.S. Department of Justice. https://www.justice.gov/archives/sco/file/1373816/download*
14. *National Constitution Center. (2023, November 4). On this day: The first bitter contested presidential election takes place. https://constitutioncenter.org/blog/on-this-day-the-first-bitter-contested-presidential-election-takes-place*
15. *European Commission. Tackling coronavirus disinformation. Retrieved April 17, 2025, from https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_en*
16. *Wendler, J. R. (2021, December 29). Misleading a pandemic: The viral effects of Chinese propaganda and the coronavirus. Joint Force Quarterly, 104, 32–40. National Defense University Press. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2884217*
17. *Sanchez, G. R., & Middlemass, K. (2022, July 26). Misinformation is eroding the public's confidence in democracy. Brookings Institution. https://www.brookings.edu/articles/misinformation-is-eroding-the-publics-confidence-in-democracy/*
18. *Collaborative Multiracial Post-Election Survey [CMPS]. (2021). 2020 survey overview. UCLA Center for the Study of Race, Ethnicity, and Politics. https://cmps.ss.ucla.edu/2020-survey/*
19. *Rose, J., & Baker, L. (2022, January 3). 6 in 10 Americans say U.S. democracy is in crisis as the 'Big Lie' takes root. NPR. https://www.npr.org/2022/01/03/1069764164/american-democracy-poll-jan-6*
20. *Newall, M., Jackson, C., & Diamond, J. (2022, January 3). Seven in ten Americans say the country is in crisis, at risk of failing. Ipsos. https://www.ipsos.com/en-us/seven-ten-americans-say-country-crisis-risk-failing*
21. *Kuo, R., & Marwick, A. (2021, August 12). Critical disinformation studies: History, power, and politics. Harvard Kennedy School Misinformation Review. https://misinforeview.hks.harvard.edu/article/critical-disinformation-studies-history-power-and-politics/*
22. *Covert, B. (2019, July 2). The myth of the welfare queen. The New Republic. https://newrepublic.com/article/154404/myth-welfare-queen*
23. *Noble, S. U. (2014). Teaching Trayvon: Race, Media, and the Politics of Spectacle. The Black Scholar, 44(1), 12–29. https://doi.org/10.1080/00064246.2014.11641209*
24. *Littrell, S., Klofstad, C., Diekman, A., Funchion, J., Murthi, M., Premaratne, K., Seelig, M., Verdear, D., Wuchty, S., &*

Uscinski, J. E. (2023, August 25). Who knowingly shares false political information online? Harvard Kennedy School Misinformation Review, 4(4). https://misinforeview.hks.harvard.edu/article/who-knowingly-shares-false-political-information-online/

25. *CB Insights. (2020, October 21). Disinformation that kills: The expanding battlefield of digital warfare. https://www.cbinsights.com/research/future-of-information-warfare/*
26. *Department of Homeland Security. (2021, August). Combatting targeted disinformation campaigns: A whole-of-society issue – Part Two. https://www.dhs.gov/sites/default/files/publications/phase_ii_-_combatting_targeted_disinformation.pdf*
27. *Bradshaw, S., & Howard, P. N. (2019, September). The global disinformation order: 2019 global inventory of organised social media manipulation (Working Paper 2019.2). Oxford Internet Institute, University of Oxford. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/09/CyberTroop-Report19.pdf*
28. *Pew Research Center. (2024, November 13). Internet/Broadband fact sheet. https://www.pewresearch.org/internet/fact-sheet/internet-broadband/*
29. *Claverie, B., Prébot, B., Buchler, N., & du Cluzel, F. (Eds.). (2022). Cognitive warfare: The future of cognitive dominance – Proceedings of the first NATO scientific meeting on cognitive warfare, Bordeaux, France, 21 June 2021. NATO Science and Technology Organization.*
30. *Claverie, B., & du Cluzel, F. (2022, March). "Cognitive Warfare": The advent of the concept of "cognitics" in the field of warfare. NATO Science and Technology Organization. https://www.researchgate.net/publication/359991886_Cognitive_Warfare_The_Advent_of_the_Concept_of_Cognitics_in_the_Field_of_Warfare*
31. *Ávila, F. de J. (2024, August 22). Cognitive warfare in the digital age: A systems approach to disinformation and neural manipulation.*
32. *Nikoula, D., & McMahon, D. (2024, July). Cognitive warfare: Securing hearts and minds. Information Integrity Lab, University of Ottawa. https://infolab.uottawa.ca/common/Uploaded%20files/PDI%20files/InfoLab%20-%20Cognitive%20Warfare,%20Securing%20Hearts%20and%20Minds.pdf*
33. *Cybersecurity and Infrastructure Security Agency. (2022, October 18). Tactics of disinformation. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf*
34. *Zhang, J., Carpenter, D., & Ko, M. (2013, January). Online astroturfing: A theoretical perspective. Paper presented at the 19th Americas Conference on Information Systems (AMCIS 2013), Hyperconnected World: Anything, Anywhere, Anytime, Chicago, IL. https://www.researchgate.net/publication/286729041_Online_astroturfing_A_theoretical_perspective*
35. *Ng, L. H. X., & Taeihagh, A. (2021). How does fake news spread? Understanding pathways of disinformation spread through APIs. Policy & Internet, 14(1), 153–186. https://doi.org/10.1002/poi3.268*
36. *Rosen, J. (2022). Senate Letter to DHS Regarding Efforts to Prevent Disinformation & Propaganda. https://www.rosen.senate.gov/wp-content/uploads/sites/default/files/2022-03/3290%20FINAL.pdf*
37. *Cybersecurity and Infrastructure Security Agency. (n.d.). Shields Up. U.S. Department of Homeland Security. https://www.cisa.gov/shields-up*
38. *Cybersecurity and Infrastructure Security Agency. (2022, April). Shields Up Technical Guidance. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/news/shields-technical-guidance*
39. *Green, J. (2021, September 27). COVID Conspiracy: Foreign disinformation driving American vaccine resistance. WTOP News. https://wtop.com/j-j-green-national/2021/09/covid-conspiracy-foreign-disinformation-driving-american-vaccine-resistance/*
40. *U.S. Department of State. (2020, August 4). Pillars of Russia's disinformation and propaganda ecosystem. Global Engagement Center. https://content.govdelivery.com/attachments/USSTATEBPA/2020/08/05/file_attachments/1512230/Pillars%20of%20Russias%20Disinformation%20and%20Propaganda%20Ecosystem_08-04-20%20%281%29.pdf*
41. *Meta. (2021, July). July 2021 coordinated inauthentic behavior report. Meta Platforms, Inc. https://about.fb.com/wp-content/uploads/2021/08/July-2021-CIB-Report.pdf*
42. *Meta. (2018, December 6). Coordinated inauthentic behavior explained. Meta Platforms, Inc. https://about.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/*
43. *Neely, S. R., Eldredge, C., Ersing, R., & Remington, C. (2022). Vaccine hesitancy and exposure to misinformation: A survey analysis. Journal of General Internal Medicine, 37(1), 179–187. https://doi.org/10.1007/s11606-021-07171-z*
44. *Daly, M., Jones, A., & Robinson, E. (2021). Public trust and willingness to vaccinate against COVID-19 in the US from October 14, 2020, to March 29, 2021. JAMA, 325(23), 2397–2399. https://doi.org/10.1001/jama.2021.8246*
45. *Rief, W. (2021). Fear of adverse effects and COVID-19 vaccine hesitancy: Recommendations of the treatment expectation expert group. JAMA Health Forum, 2(4), e210804. https://doi.org/10.1001/jamahealthforum.2021.0804*
46. *Lau, T. (2020, January 17). The Honest Ads Act, explained. Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/honest-ads-act-explained*
47. *Honest Ads Act, S.1989, 115th Cong. (2017). https://www.congress.gov/bill/115th-congress/senate-bill/1989/text*
48. *Cybersecurity and Infrastructure Security Agency. (n.d.). Election security. U.S. Department of Homeland Security. https://www.cisa.gov/topics/election-security*
49. *U.S. Department of Homeland Security, Office of Inspector General. (2022, August). DHS needs a unified strategy to counter disinformation campaigns (OIG-22-58). https://www.oig.dhs.gov/sites/default/files/assets/2022-09/OIG-22-58-Aug22.pdf*
50. *U.S. Government Accountability Office. (2024). National security: Preliminary observations on State and DOD efforts to counter foreign propaganda and disinformation (GAO-24-107600). https://www.gao.gov/assets/gao-24-107600.pdf*

51. *U.S. Congress. (2016). National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, 130 Stat. 2000. https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf*
52. *Guo, E. (2025, April 16). U.S. office that counters foreign disinformation is being eliminated, say officials. MIT Technology Review. https://www.technologyreview.com/2025/04/16/1115256/us-office-that-counters-foreign-disinformation-is-being-eliminated-say-officials/*
53. *California State Legislature. (2018). Assembly Bill No. 155: State government: Department of Technology. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB155*
54. *West, D. M. (2017, December 18). How to combat fake news and disinformation. Brookings Institution. https://www.brookings.edu/articles/how-to-combat-fake-news-and-disinformation/*
55. *Bulger, M., & Davison, P. (2018). The Promises, Challenges, and Futures of Media Literacy. Journal of Media Literacy Education, 10(1), 1-21. https://doi.org/10.23860/JMLE-2018-10-1-*
56. *Dame Adjin-Tettey, T. (2022). Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education. Cogent Arts & Humanities, 9(1). https://doi.org/10.1080/23311983.2022.2037229*
57. *National Association for Media Literacy Education. (n.d.). Media literacy is defined. https://namle.org/resources/media-literacy-defined/*
58. *Reno v. American Civil Liberties Union, 521 U.S. 844 (1997). https://supreme.justia.com/cases/federal/us/521/844/*
59. *Packingham v. North Carolina, 582 U.S. ___ (2017). https://www.supremecourt.gov/opinions/16pdf/15-1194_08l1.pdf*
60. *Prendergast, S. (2019, March). It must be true, I read it on the internet: Regulating fake news in the digital age. Michigan Technology Law Review. https://mttlr.org/2019/03/it-must-be-true-i-read-it-on-the-internet-regulating-fake-news-in-the-digital-age/*
61. *Sperry, B. (2024). Knowledge and decisions in the information age: The law & economics of regulating misinformation on social media platforms. Gonzaga Law Review, 59, 319–380.https://laweconcenter.org/resources/knowledge-and-decisions-in-the-information-age-the-law-economics-of-regulating-misinformation-on-social-media-platforms/*
62. *Sands, G. (2022, August 24). DHS has shut down its controversial disinformation board, months after it was paused. CNN. https://edition.cnn.com/2022/08/24/politics/dhs-disinformation-board-shut-down/index.html*
63. *New Mexico Secretary of State. (2022, May 31). Rumor vs. reality website fact-checks misinformation about New Mexico's voting and elections. https://www.sos.nm.gov/2022/06/01/rumor-vs-reality-website-fact-checks-misinformation-about-new-mexicos-voting-and-elections/*
64. *North Carolina State Board of Elections. (n.d.). Mythbuster archive: Combating misinformation. https://www.ncsbe.gov/about-elections/election-security/combating-misinformation/mythbuster-archive*
65. *Santa Clara County Registrar of Voters. (n.d.). Key actions to protect our elections. County of Santa Clara. https://vote.santaclaracounty.gov/key-actions-protect-our-elections*