BIPSS Commentary
www.bipss.org.bd
September -2024
BIPSS Towards a Secure World

# The Rise of Disinformation in Global Politics: Threats to Democracy and Security

**Saraf Wasima**[1]

Source: Stanford University Report

**Introduction:**

The term "disinformation" was initially coined by Joseph Stalin and is derived from the Russian word "dezinformatsiya." It is defined as "false information intentionally disseminated to deceive the public" in the Great Soviet Encyclopaedia (1952). It is crucial to recognise that disinformation is intentional; it is intended to deceive and manipulate.

Disinformation is fundamentally distinct from misinformation and malinformation, as malinformation is founded on reality but is intended to cause harm. In contrast, misinformation is

[1] Saraf Wasima is a Research Assistant at the Bangladesh Institute of Peace and Security Studies (BIPSS). She completed her BSS & MSS in International Relations from the Bangladesh University of Professionals (BUP).

false information that is not intended to endanger anyone. Conversely, disinformation is false information that is intended to harm a person, group, or society. According to the 2024 Global Risk Report, disinformation is the most significant global risk among all other risks.

The global political landscape is characterised by an increase in disinformation, which poses a threat to both global security and the democratic process.[2] This commentary aims to investigate the global proliferation of disinformation, which poses a threat to security and democracy.

## The Role of Disinformation in Global Politics

### Historical Background

Throughout history, disinformation has been a potent instrument for the manipulation of public opinion and the shaping of political narratives. Governments employed propaganda extensively to regulate the dissemination of information and shape public opinion during World War I and II. False reports of hostile atrocities were employed to mobilise public support for the war effort, for instance.

The Cold War was a significant period for the use of disinformation, as both the United States and the Soviet Union engaged in psychological warfare and propaganda to undermine each other. The Soviet Union employed "active measures" to incite political instability in the West by disseminating false narratives. For instance, the infamous "Operation INFEKTION" disseminated the false assertion that the United States had created the HIV/AIDS virus.

In order to rationalise their control and exploitation of resources, European powers frequently employed disinformation to justify colonial domination, portraying indigenous populations as inferior or uncivilised.

[2] McLennan, Marsh. "The global risks report 2022 17th edition." Cologny, Switzerland: World Economic Forum, 2022.

## Threats to Democracy


Source: OHCHR /UN

### Undermining Free and Fair Elections

The manipulation of electoral processes through disinformation campaigns is one of the most grievous threats to democracy.[3] These initiatives are designed to undermine public trust in election outcomes, disseminate fallacies, and distort public opinion.

### Erosion of Public Trust in Institutions

Disinformation not only aims at elections but also deliberately undermines trust in essential institutions, including the media, government, and the democratic process.[4]

[3] McKay, Spencer, and Chris Tenove. "Disinformation as a threat to deliberative democracy." *Political research quarterly* 74, no. 3 (2021): 703-717.
[4] Tenove, Chris. "Protecting democracy from disinformation: Normative threats and policy responses." *The International Journal of Press/Politics* 25, no. 3 (2020): 517-537.

**How Disinformation Weakens Trust:**

• The capacity of individuals to distinguish between credible and non-credible sources is diminished by their continuous exposure to manipulated information and false news. In the event that trust in the media is compromised, citizens become more susceptible to disinformation, which further fragments society.

• Disinformation campaigns frequently depict governments as corrupt or incompetent, which contributes to a narrative that undermines confidence in governmental processes and institutions. This, in turn, results in a decrease in public confidence in democracy and elected officials.

• Citizens' confidence in the legitimacy of outcomes is diminished when disinformation undermines elections or other critical democratic processes.[5] Even in elections that are highly regulated, voter fraud allegations, which are frequently fuelled by disinformation, generate uncertainty.

Disinformation exacerbates societal divisions by fostering a "us versus them" mentality, which exacerbates hostility between opposing political factions and complicates the process of compromise.

**Consequences:**

• Disinformation exacerbates societal divisions by fostering a "us vs. them" mentality, which complicates compromise and heightens animosity between opposing political factions.[6]

• As individuals lose confidence in the integrity of political systems and elections, they are less inclined to engage in political activities or vote, resulting in a decline in voter confidence.

• The democratic system is weakened when citizens no longer trust institutions and withdraw from the political process wholly.

---

[5] Humprecht, Edda. "The role of trust and attitudes toward democracy in the dissemination of disinformation—a comparative analysis of six democracies." *Digital Journalism* (2023): 1-18.

[6] Hameleers, Michael, Anna Brosius, and Claes H. de Vreese. "Whom to trust? Media exposure patterns of citizens with perceptions of misinformation and disinformation related to the news media." *European journal of communication* 37, no. 3 (2022): 237-268.

**Manipulation of Public Opinion**

Voters' emotions and opinions can be manipulated by targeted disinformation campaigns, which frequently direct them away from facts and towards emotionally charged, deceptive narratives.

Targeted Campaigns:

• Emotional Manipulation: Disinformation campaigns frequently employ fear, wrath, and other powerful emotions to influence public opinion. For example, divisive issues such as immigration, race relations, and national security are frequently exploited to incite fear or outrage, thereby influencing electors without regard for factual accuracy.[7]

• Policy Debate Misinformation: o Climate Change Denial: Disinformation campaigns have long been employed to undermine efforts to implement environmentally favourable policies and sow doubt about scientific consensus in the climate change debate.

• Vaccine Hesitancy: An additional illustration is the increase in vaccine misinformation, which has resulted in vaccine hesitancy. False claims regarding vaccine safety are disseminated through campaigns, which result in a decrease in public health initiatives and contribute to preventable disease outbreaks.

[7] Koistinen, Pekka, Milla Alaraatikka, Teija Sederholm, Dominic Savolainen, Aki-Mauri Huhtinen, and Miina Kaarkoski. "Public Authorities as a Target of Disinformation." In *European Conference on Cyber Warfare and Security*, vol. 21, no. 1, pp. 123-129. 2022.

**Case Studies of Disinformation Campaigns:**

Source: CBS news

**US 2016 Election:**

The 2016 US Presidential election became a key example of how disinformation could be weaponized. Russian-linked groups were found to have spread misinformation through social media, influencing the election in favor of one candidate. Tactics included fake news, misleading advertisements, and using bots to amplify divisive content.[8]

**Brexit Referendum (2016):**

The Brexit referendum saw similar tactics, with false information like the infamous "£350 million NHS pledge." Pro-Brexit groups used social media campaigns to sway public opinion, often

[8] Galeano, Katrin, Rick Galeano, Samer Al-Khateeb, and Nitin Agarwal. "Studying the Weaponization of Social Media: Case Studies of Anti-NATO Disinformation Campaigns." *Open Source Intelligence and Cyber Crime: Social Media Analytics* (2020): 29-51.

through fabricated stories targeting voter emotions, which led to widespread polarization and confusion among the electorate.[9]

**Security Implications of Disinformation:**

**Role of Foreign Actors and State-Sponsored Disinformation**

Foreign actors are increasingly employing disinformation to destabilise adversary nations by undermining their social cohesion, political stability, and trust in government institutions. State-sponsored disinformation campaigns are a critical element of contemporary hybrid warfare, which combines psychological operations with digital tactics to undermine rival states.

**Disinformation campaigns conducted by Russia in Eastern Europe:**

Source: The New York times

Disinformation has been employed by Russia as a geopolitical instrument in countries such as Estonia, Lithuania, and Ukraine for an extended period. Elections, ethnic tensions, and national sovereignty are frequently the focus of these campaigns. For instance, during the 2014 annexation

[9] Wilson, Tom, and Kate Starbird. "Cross-platform disinformation campaigns: lessons learned and next steps." *Harvard Kennedy School Misinformation Review* 1, no. 1 (2020).

of Crimea in Ukraine, Russian disinformation portrayed the Ukrainian government as authoritarian, thereby justifying Russian intervention and causing confusion among Ukrainian citizens.

**Chinese Information Warfare**: Both domestic and international audiences have been the targets of China's disinformation campaigns. It involves the dissemination of narratives that promote disunity among global powers and undermine the credibility of democratic governments, while also showing favour for Chinese political ideologies.[10] In the context of the Hong Kong protests, the Taiwan Strait tensions, and, more recently, global narratives around COVID-19 and the Belt and Road Initiative, Chinese disinformation efforts have been evident.

**Cybersecurity Threats**


Source: Security Magazine

**How Disinformation Intersects with Cyberattacks, Hacking, and Data Manipulation:**

Disinformation is becoming more closely associated with cyberattacks, resulting in a perilous intersection between cybersecurity and information warfare. Cyberattacks frequently function as

[10] Bradshaw, Samantha, Ualan Campbell-Smith, Amelie Henle, Antonella Perini, Sivanne Shalev, Hannah Bailey, and Philip N. Howard. "Country case studies industrialized disinformation: 2020 global inventory of organized social media manipulation." *Oxford Internet Institute.* (2021).

an entry point for disinformation, as hackers acquire sensitive information that is subsequently weaponised through manipulated or fabricated disclosures.

• Data Breaches and Manipulation: Cybercriminals may infiltrate government or corporate databases, manipulate the data, and subsequently use disinformation to propagate false narratives. For instance, the 2016 US election saw the dissemination of disinformation influenced by stolen emails as a result of the hacking of the Democratic National Committee (DNC), which exacerbated political divisions.[11]

• Hybrid Warfare: The integration of disinformation campaigns and cyber espionage is a defining characteristic of hybrid warfare.[12] In this context, digital attacks are employed to disrupt critical infrastructure, while disinformation campaigns are employed to cultivate societal distrust and confusion. Russia has been at the forefront of this strategy, integrating hacking, disinformation, and military actions into its geopolitical maneuvers.

**Combatting the Threat of Disinformation**


[11] Petratos, Pythagoras N. "Misinformation, disinformation, and fake news: Cyber risks to business." *Business Horizons* 64, no. 6 (2021): 763-774.
[12] Moses, Joseph. "Disinformation as part of Modern Warfare's Cyber-attacks." (2022).

Source: American Psychological Association

• Disinformation detection and removal necessitate sophisticated technologies such as artificial intelligence (AI) and machine learning. These tools are capable of analysing immense quantities of data in real time, thereby identifying patterns that suggest the presence of false or misleading content. Machine learning enables the system to continually enhance itself by learning from previous instances of disinformation, while AI-powered algorithms can raise red flags regarding suspicious content.[13]

• Social media platforms are essential for the implementation of fact-checking mechanisms and the moderation of content. They are increasingly utilising AI tools to automatically detect and eradicate disinformation in conjunction with third-party fact-checkers. Nevertheless, these platforms are also confronted with the challenge of harmonising content moderation with free speech, which requires the implementation of transparent policies.

**Responses of the Government and Policy**

a) Governments are devising strategies, including the implementation of legislation that is designed to hold platforms accountable for the dissemination of disinformation. Counter-disinformation units have been implemented in certain countries to refute deceptive narratives, particularly during crises or elections. For instance, the Digital Services Act of the European Union mandates that platforms be accountable for addressing detrimental content.
b) Global cooperation is frequently required as disinformation frequently cross national borders. Cross-border disinformation campaigns are addressed through international forums such as the Global Forum on Cyber Expertise (GFCE) and other consortia, which

[13] Teremetskyi, Vladyslav, Kseniia Tokarieva, Iurii Dziuba, Nikolay Shelukhin, Oleh Predmestnikov, and Ulyana Parpan. "Combatting disinformation and cyber threats in the European Union and United States: Lessons for Ukraine." *J. Legal Ethical & Regul. Isses* 24 (2021): 1.

facilitate collaboration among nations[14]. These initiatives encourage the coordination of counter-disinformation policies and the exchange of best practices among nations.

c) The long-term solution to disinformation is to educate the public. Media literacy programs in schools, universities, and communities assist individuals in conducting a critical assessment of the information they ingest.[15] Media literacy campaigns are designed to enhance the resilience of society to disinformation by instructing individuals on how to differentiate between credible news sources and false or biassed information.

d) Countering disinformation necessitates independent journalism. Investigative journalists and fact-checking organisations dedicate themselves to the task of exposing falsehoods and verifying the truth. It is essential to support independent media and fact-checkers in order to ensure that the public is well-informed.[16]

## Conclusion

In the digital era, disinformation is a substantial and increasing hazard to public trust, security, and democracy. Technological advancements and social media have the potential to amplify the dissemination of false information, which can distort public perception, undermine democratic processes, and destabilise societies.[17] This challenge necessitates the implementation of robust government policies, the promotion of public awareness through media literacy and education, and the utilisation of technological solutions such as AI. It is imperative to establish resilience against disinformation through global collaboration and independent journalism.

A multi-stakeholder approach that includes governments, social media platforms, independent fact-checkers, educators, and civil society is necessary to address disinformation. Each stakeholder is essential in the fight against the dissemination of disinformation and in the enhancement of the public's capacity to identify credible information. It is essential to take immediate and coordinated

[14] Calvo-Gutiérrez, Elvira, and Carles Marín-Lladó. "Combatting Fake News: A Global Priority Post COVID-19." *Societies* 13, no. 7 (2023): 160.

[15] Matasick, Craig, Carlotta Alfonsi, and Alessandro Bellantoni. "Governance responses to disinformation: How open government principles can inform policy options." (2020).

[16] Tenove, Chris. "Protecting democracy from disinformation: Normative threats and policy responses." *The International Journal of Press/Politics* 25, no. 3 (2020): 517-537.

[17] Miyamoto, Inez. "Disinformation: policy responses to building citizen resiliency." *Connections: The Quarterly Journal* 20, no. 2 (2021): 47-55.

action in light of the rapidly evolving digital technology and the rapidly expanding global scope of disinformation campaigns.

It is imperative that global efforts be coordinated in order to protect democratic institutions and preserve international security. In order to fortify society's ability to combat disinformation, it is imperative that countries, organisations, and platforms collaborate to establish robust policies, technological defences, and educational programs. The protection of our democratic values and the establishment of a more secure and informed world can only be achieved through unified global cooperation.