RESEARCH ARTICLE

The Use of Electronic Bots to Spread Rumors via Social Media in Cyber Warfare to Control Public Opinion

Noureddine Dahmar

Researcher

University of Mohamed El Bachir El Ibrahimi -Bordj Bou Arreridj

Algeria

Email: noureddine.dahmar@univ-bba.dz, https://orcid.org/0009-0006-4108-6615

Radhouane Moumene

Doc Researcher tor

University of Mohamed El Bachir El Ibrahimi -Bordj Bou Arreridj

Algeria

Email: radhouane.moumene@univ-bba.dz, https://orcid.org/0009-0003-3620-7652

Abdelhafid Lameche

Researcher

University of Mohamed El Bachir El Ibrahimi -Bordj Bou Arreridj

Algeria

Email: abdelhafid.lameche@univ-bba.dz, https://orcid.org/0009-0008-4053-9111

Baghdad Bendida

Researcher

Nour Bachir University Centre of El Bayadh

Algeria

Email: b.baghdad@cu-elbayadh.dz, https://orcid.org/0009-0000-9580-2206

Abdellatif Bouzir

Researcher

University of Moulay Tahar Saida

Algeria

E-mail: Abdellatif. bouzir@uni-saida.dz, https://orcid.org/0000-0002-2575-1754

Doi Serial https://doi.org/10.56334/sei/8.5.75

Keywords Cyber warfare, electronic bots, rumors, social media, public opinion

Abstract

The concept, tools, and theater of warfare have evolved significantly in the modern era. With the widespread use of advanced communication technologies in societies, several concepts related to cyber warfare have emerged. This research paper seeks to examine the concept of electronic bots (commonly referred to as "electronic flies") and their strategic employment by states in cyber warfare to disseminate rumors through one of the most widely used digital communication platforms—social media. These platforms play a crucial role, based on precise strategies, in spreading disinformation and shaping public opinion within the virtual environment, by mobilizing electronic armies.

Citation

Noureddine Dahmar N., Moumene R., Lameche A., Bendida B., Bouzir A. (2025). The Use of Electronic Bots to Spread Rumors via Social Media in Cyber Warfare to Control Public Opinion. *Science, Education and Innovations in the Context of Modern Problems*, 8(7), 738-743; doi:10.56352/sei/8.7.75. https://imcra-az.org/archive/365-science-education-and-innovations-in-the-context-of-modern-problems-issue-7-volviii-2025.html

Licensed

© 2025 The Author(s). Published by Science, Education and Innovations in the context of modern problems (SEI) by IMCRA - International Meetings and Journals Research Association (Azerbaijan). This is an open access article under the **CC BY** license (http://creativecommons.org/licenses/by/4.0/).

Received: 06.03.2025 | Accepted: 04.05.2025 | Published: 15.06.2025 (available online)

Introduction

The world is undergoing significant transformations in warfare and the management of conflicts between states. The concepts, arenas, and weapons of war have fundamentally changed. Communication and media technologies—most notably the Internet—have contributed to the emergence of a new form of warfare whose battleground is the digital environment. This form is referred to as *cyber warfare*, and it has acquired a global dimension. It does not require the deployment of heavy weapons such as aircraft, tanks, armies, warships, or submarines. Instead, it relies on computers, internet connectivity, and cyber-attack operatives. These tools are capable of inflicting damage on targeted entities at any time and from any location.

This affirms that traditional warfare has become parallel to another form of war whose theater is the digital space, employing all available technologies to influence the enemy—including rumors and fake news.

Electronic bots represent one of the newly developed tools of cyber warfare, with their activities primarily concentrated on social media platforms. These bots employ a variety of methods and techniques aimed at manipulating and controlling public opinion.

This article investigates the phenomenon of rumor dissemination across social media and examines the role of electronic bots in spreading such content. It seeks to answer the following research question: **How are electronic bots used to spread rumors via social media in the context of cyber warfare to control public opinion?**

1. The Concept of Cyber Warfare

It is important to note that the term cyber warfare has emerged as a result of the rapid development of communication and media technologies in modern societies. It refers to a new type of warfare that takes place in the digital environment and whose primary weapon is technology—an idea that will be clarified further in this section.

When examining the history of warfare throughout human civilization, it becomes evident that technological advancements have always played a crucial role in enhancing combat capabilities, achieving strategic goals, and securing vital interests. Armed conflict has consistently served as a real and often bloody testing ground for the knowledge and innovations developed by nations.

With the advent of the modern technological era, a new form of combat system emerged—one that relies heavily on electronic technologies and computer systems to manage battles. This form of warfare later came to be known as electronic warfare or cyber warfare.[1]

[1] Samer Muayyad Abd Al-Latif, "War in Dig*ital Space: A Future Perspective," Journal of Law, College of Law, University of Karbala, Iraq, Issue No. 02, 2015, p. 76.*

The roots of cyber warfare can be traced back to the science of *cybernetics*, which refers to the study of control systems in machines. In this context, the Soviet military is considered the first to apply this science during the leadership of Nikita Khrushchev, under whom significant achievements were made in the field of space exploration.[2]

More specifically, the English term *cyber* can be translated into Arabic as "imaginary" or "virtual." The word *cyber* is commonly used to describe the space that encompasses computer-based networks, communication and information systems, and remote control technologies. The uses of cyberspace vary from one country to another depending on national priorities—ranging from security, political, intelligence, civil, professional, to informational domains.

In general, the cyber infrastructure of any state is composed of three fundamental components: physical hardware, digital software systems, and human elements, including programmers and users.[3]

2. Characteristics of Cyber Warfare

Cyber warfare possesses distinct characteristics that differentiate it from traditional forms of warfare. These can be summarized as follows:

- Traditional wars are waged within clearly defined geographical battlefields and theaters of operation, whereas cyber warfare takes place in cyberspace, thereby eliminating physical and territorial boundaries.
- Cyberattacks are executed using tools and weapons specific to cyber warfare, commonly referred to as instruments of aggression. These tools vary depending on the intended objectives of the attack.
- The targets of cyber warfare are not limited to military sites alone; rather, they often extend to civilian infrastructure, impacting various aspects of societal life.
- In cyber warfare, the attacker enjoys a significant advantage over the defender. These forms of conflict are marked by speed, flexibility, evasion, and the difficulty of implementing effective defenses.
- Cyber warfare is a highly advanced form of digital and technological conflict, representing the peak of progress achieved by the information revolution—of which the electronic computer is a central component.[4]

3. Types of Threats Used in Cyber Warfare

The threats resulting from the use of cyber warfare between states, societies, and individuals take various forms depending on their objectives and the power of the entity managing them. The most prominent types of cybercrimes can be outlined as follows:

A. Data Corruption or Alteration:

This refers to gaining access to a victim's information through the Internet or private networks and modifying important data without the victim's awareness. The data remains present but becomes misleading, which can lead to catastrophic outcomes—especially when it involves military plans, schedules, or classified maps.

B. Network Espionage:

This involves unauthorized access and surveillance of enemy networks without destroying or altering any data. The goal is to obtain sensitive information, which may include military strategies or classified military, economic, financial, or political secrets—potentially compromising the adversary's operations.

C. Data Destruction:

[2] *Heba Hashem Mohamed, "A Proposed Program Based on the Geography of Cyber Wars to Raise Awareness of Their Risks and Promote Digital Citizenship Values among Student Teachers at the Faculty of Education,"* Journal of the Faculty of Education*, Ain Shams University, Egypt, Issue No. 44, Part 3, 2020, p. 96.*

[3] Ahmad Allo, *Cyber Wars and Digital Violence: A New Global Reality*, www.lebarmy.gov.lb, 03/10/2022, 20:00.

[4] Hanan Dreesi, *Cyber Warfare: A Shift in Combat Methods with Consistent Principles and Objectives, Journal of Legal and Political Thought,* Faculty of Law and Political Science, Ammar Thliji University – Laghouat, Vol. 06, No. 01, 2022, pp. 917–918.

This entails the complete erasure or destruction of assets, data, and information stored on a network. Often referred to as a "threat to content integrity," it involves unauthorized individuals modifying data by deleting or destroying it.[5]

4. Electronic Bots: A New Weapon in Digital Space

The term *electronic bots* (or *electronic flies*) has come to encompass various designations, such as “electronic brigades,” “black cells,” “bots,” “electronic armies,” “hackers,” and “cyber pirates.” This term has been widely circulated in recent years and remains confined to the realm of virtual reality in its various forms. This is particularly relevant in light of the growing influence played by electronic committees in political conflicts and crises between states.[6]

The term *electronic bots* refers to a group of automated accounts programmed to disseminate a specific post or tweet with the aim of influencing public opinion or drawing attention to a particular idea while marginalizing others that may be of greater importance. These bot accounts operate using code that can range from simple to complex, depending on the nature and scope of the assigned task.[7]

It is also defined as the intensive use of fake accounts in a specific direction—either to support a particular point of view or to attack an opposing one. This strategy is commonly employed on social media platforms such as Facebook and Twitter, and it is used across various domains, including political, social, and economic issues, as well as matters related to art and technology.[8]

Electronic bots—through fake accounts and coordinated online brigades—work to create instability within nations and societies by exploiting any event or crisis to spread toxicity. Their aim is to disrupt public life and generate widespread discontent within society by fabricating news, spreading rumors, distorting facts, selectively quoting statements, violating privacy, and sharing offensive images or videos for purposes such as defamation, score-settling, or various forms of extortion. All these practices seek to undermine societal values and national constants.[9]

With the rapid spread of social media platforms, the rise in user numbers, and their growing precedence over traditional journalism, new tools have emerged that aim to confuse users and disrupt their perceptions, ultimately seeking to manipulate public opinion. The activity of electronic bots has intensified, relying on both fake and real accounts directed by specific entities to carry out systematic media campaigns against individuals, organizations, or states. Their primary function lies in amplifying selected views and adopting particular stances on social media in a way that simulates widespread public consensus—as if a large number of users were voicing a unified opinion.[10]

Social media platforms have thus transformed from mere tools for peaceful communication and expression into mechanisms for coercive opinion imposition, digital intimidation, and the concealment of genuine public sentiment. These platforms are now used for exposure, defamation, misinformation, and reputation smearing, contributing significantly to the spread of media chaos.[11]

the Gulf region during the ongoing Gulf crisis involving Qatar, Saudi Arabia, and the United Arab Emirates. This phenomenon also drew significant attention in the controversy surrounding suspected Russian interference in the 2016 U.S. presidential elections. Russia was accused of manipulating American public opinion by hacking into the Democratic National Committee’s network and leaking information online to influence voter behavior. Moreover, electronic bots played a pivotal role in the Syrian crisis, transforming social media platforms into arenas

[5] Ismail Zarouqa, *Cyberspace and the Transformation in Concepts of Power and Conflict, Journal of Legal and Political Sciences*, University of Hamma Lakhdar – El Oued, Vol. 10, No. 01, April 2019, p. 1024.
[6] Omar Abu Daf, *The Arab Electronic Bots*, https://www.sasapost.com/opinion/, accessed on 03/10/2022 at 18:30.
[7] Fatima Mohammed Saleh Al-Badrani, *Electronic Bots as a Tool of Cyber Warfare*, https://portal.arid.my/ar-LY, accessed on 05/10/2022 at 12:45.
[8] Amnay Afshko, *Everything About Electronic Bots and Their Connection to Fake News and Hate Speech*, https://www.amnaymag.com/, accessed on 03/10/2022 at 17:00.
[9] Ahmed Al-Tayeb, *Electronic Bots: The Most Dangerous Scourge of the Virtual World*, https://www.youm7.com, accessed on 03/10/2022 at 19:00.
[10] Omar Abu Daf, *The Arab Electronic Bots*, https://www.sasapost.com/opinion/, accessed on 03/10/2022 at 18:30.
[11] Muhannad Abdul Jawad Rahi, *The Phenomenon of Electronic Bots: A Disruption of Publishing Systems and the Expansion of Media Chaos*, https://www.ahewar.org/, accessed on 03/10/2022 at 19:30

of mobilization, sectarian incitement, and hatred. These platforms became virtual battlegrounds led by both supporters and opponents of the Syrian regime.[12]

5. How Electronic Bots Use Social Media to Spread Rumors

Rumors are considered one of the most devastating tools of psychological warfare. Their creators strategically plan both in the short and long term to create conditions conducive to weakening the enemy's internal security. This includes inciting internal strife, social fragmentation, and distrust among individuals, ultimately undermining social cohesion and stability.[13]

A rumor can be defined as the dissemination of false or unfounded information, or the deliberate exaggeration, distortion, or sensationalism of a report that may contain a grain of truth. It may also involve adding false or misleading elements to otherwise factual information or interpreting a true event in a deceptive manner. The ultimate objective is to psychologically influence public opinion—whether local, regional, national, or international—serving political, economic, or military agendas across single or multiple nations, or even on a global scale.[14]

There are several factors that contribute to the acceptance and spread of rumors, including the following:

- **Credible Source**: Hundreds of studies on persuasive communication emphasize the central role of the source—namely, the person transmitting the information. Multiple elements shape trust in a source, the most important of which is the recipient's perception of the source's expertise, credibility, integrity, dynamism, and charismatic personality.

- **Nature of Reference Frameworks**: The acceptance of the truthfulness of any piece of information is often linked to the personal reference framework used by each individual to evaluate that information. When information aligns with one’s internal framework, the likelihood of considering it truthful increases.

- **Repetition**: The more frequently a rumor is repeated, the more convincing it becomes. Initially, it might circulate for entertainment purposes, but over time, it is likely to be perceived as a confirmed truth. Persuasion is formed when individuals hear the same message from different people, making it easier to infer that it must be true.

- **Desire to Believe**: Sometimes, the desire to believe something becomes so intense that it overrides usual standards of realism and logic. A rumor will not gain traction unless the transmitted information fulfills a desire, responds to a hidden fear, or offers a psychological resolution. The more the rumor reflects our own beliefs, the more likely we are to accept it as truth. This illustrates how many rumors—despite being implausible—are believed simply because they reinforce personal intuition, emotions, or opinions.[15]

Social media platforms are among the most influential forms of new media. They have not only transformed the nature of interpersonal and group communication but also profoundly affected its outcomes and influence. These platforms have expanded the scope of media beyond traditional limits, offering users unprecedented opportunities for influence and unrestricted cross-border communication.

Despite the positive contribution of social media to the rise of what is now known as the “citizen journalist,” the lack of news verification and difficulty in confirming the accuracy and credibility of sources have made these platforms powerful tools for the rapid spread and acceptance of rumors, leading people to believe in their truth and build ideas and opinions based on them.[16]

The growing use of various social media platforms has opened the door to the dissemination of misleading and false information. The ease of spreading content on these platforms has created a fertile environment for malicious

[12] Boualem Razik, *Digital Propaganda: How Do Electronic Bots Operate?*, https://www.aljazeera.net/blogs, accessed on 04/10/2022 at 17:00.

[13] Sharaf Eddine Ben Harith, *Rumors and Their Impact on the Security and Political Stability of the State: Facts from Algerian Facebook Pages*, https://manifest.univ-ouargla.dz, accessed on 04/10/2022 at 13:00.

[14] Mohamed Mounir Hegab, *Rumors and Ways to Confront Them*, Dar Al-Fajr for Publishing and Distribution, Cairo, 2006, pp. 19–20.

[15] Rehab Mohamed Anwar, *The Use* of Official Infographics on Social Media to Confront Rumors, The Egyptian Journal for Journalism Research, Faculty of Mass Communication, Cairo University, Issue 1, July 2021, p. 73.

[16] Sherif El-Labbane & Sally El-Shalqani, *Mechanisms for Confrontation and Response: Social Media Networks and Rumors*, http://www.acrseg.org/40856, Accessed: 12/10/2022 at 12:00.

actors to circulate rumors that threaten societal security. Although social media, as a form of new media, is effective in delivering real-time updates, it simultaneously provides an ideal environment for the proliferation of rumors.

The growing use of various social media platforms has opened the door to the widespread dissemination of false and misleading news. The ease of circulating information across these platforms has created a fertile environment for malicious actors to spread rumors that undermine societal security. Despite the effectiveness of social media as a form of new media in transmitting events in real time, it remains a fertile ground for the growth and proliferation of rumors.[17]

Electronic bots (known as "electronic flies") engage in hashtag poisoning, wherein they target trending hashtags and create opposing ones. These are then promoted by multiple accounts that flood social media with counter-content and ideas, effectively overwhelming the original hashtag in terms of visibility and activity. This tactic is often accompanied by a coordinated campaign of rumors that distract from the main issue by creating secondary or fabricated controversies—thus framing them as public concerns representing the majority, while portraying the original cause as the concern of a mere minority. As a result, the hashtag becomes "poisoned," preventing regular users from easily finding or interacting with authentic information shared by real individuals.[18]

Naturally, electronic flies can either act proactively or reactively by generating counter-hashtags. They can also deploy multiple persuasive strategies based on the targeted objectives—ranging from seriousness to mockery, logic to emotion, or even combining conflicting tactics. Accordingly, there is a close relationship between electronic flies and fake or fabricated news. These bots rely heavily on spreading rumors, fake news, and doctored images; they fabricate events and statements, manipulate old videos and photos, and present them as recent or authentic. Due to their widespread dissemination, recipients often perceive this content as real. This is why we speak of *disinformation*—which refers to the intentional manipulation of public awareness.[19]

6. Strategies for Combating Electronic Flies' Rumors on Social Media

Based on the foregoing discussion, a set of recommendations can be proposed to counter the spread of rumors by electronic flies on social networks:

Nasr Ramadan Harbi, *Rumors and Their Dissemination via Social Media*, Paper presented at the International Conference on Law and Rumors, Faculty of Law, Tanta University, Egypt, April 2, 2019, p. 37.

- Raising public awareness of the risks posed by rumors circulated via social media platforms.
- Encouraging both official and unofficial media institutions to establish and develop dedicated media platforms for confronting and refuting social media rumors.
- Urging international, Arab, and Islamic cooperation to enact legal frameworks regulating social media platforms.
- Enabling relevant authorities to monitor, track, and publicly expose accounts that promote rumors.
- Ensuring that official media commit to conveying accurate information to the public, avoiding any withholding of facts that might later become the subject of rumors across social networks.

Conclusion:

Day by day, the world is witnessing continuous developments in the field of information and communication technologies. Despite their crucial role in the lives of nations, societies, and individuals, and across all areas of life, the use of these technologies—particularly social media—in disseminating rumors and false information has become increasingly alarming. This trend poses serious threats to societal security, both during normal times and amid cyberwars and interstate conflicts, where electronic flies are deliberately deployed as part of technological warfare.

[17] Ietimad Khalaf Maabed, Teenagers' Exposure to Rumors on Social Media and Its Relationship to Their Political Attitudes, https://jsc.journals.ekb.eg, Accessed: 11/10/2022 at 18:00.

[18] Boualem Razik, *Digital Propaganda: How Do Electronic Flies Operate?*, Al Jazeera Blogs, https://www.aljazeera.net/blogs/, Accessed: 04/10/2022 at 17:00.

[19] Nacereddine Bouziane, *Fake News, Electronic Flies, and the Fabrication of Awareness: Prevention and Confrontation Strategies*, *Akademia Journal of Political Studies*, Hassiba Ben Bouali University, Chlef, Vol. 6, No. 5, 2021, pp. 40–41.

To safeguard society and individuals and preserve national unity and core values, raising awareness and sensitizing the public to the dangers of electronic flies—and their calculated role in spreading confusion and misinformation—is essential. These tactics are strategically designed to manipulate and mislead public opinion and steer it in specific directions. In parallel, the legal dimension remains vital in confronting and curbing this phenomenon. This requires concerted international efforts and collaboration with social media platform owners to counter all parties involved in spreading rumors and fake news—actions that ultimately threaten social cohesion and global peace.

References:

1. Al-Tayeb, A. (n.d.). *Electronic flies: The most dangerous plague of the virtual world.* Retrieved from https://www.youm7.com/
2. Allou, A. (n.d.). *Cyber wars and digital violence: A new global reality.* Retrieved from https://www.lebarmy.gov.lb
3. Afchakou, A. (n.d.). *Everything about electronic flies and their relation to fake news and hate speech.* Retrieved from https://www.amnaymag.com/
4. Zerrouga, I. (2019). *Cyberspace and the transformation of power and conflict concepts.* Journal of Legal and Political Sciences, University of Hamma Lakhdar – El Oued, Vol. 10(1), April 2019.
5. Khalaf Maabad, I. (n.d.). *Teenagers' exposure to social media rumors and their relation to political attitudes.* Retrieved from https://jsc.journals.ekb.eg
6. Mohamed, H. H. (2020). *A proposed program based on the geography of cyber wars to raise awareness of their risks and promote digital citizenship values among student-teachers at the Faculty of Education.* Journal of the Faculty of Education, Ain Shams University, Issue 44, Part 3.