Revista Infoacceso
e-ISSN 2311-7605 (Online)
infoacceso.org/index.php/ri

Volume 13 · Issue 3 · 2026
Pages 3638–3646

The Security Communication Role in Safeguarding Algeria's National Security amid Digital Transformation and Information Threats

Dr. Nassim Henad

Lecture (class b) , Media and communication sciences, University of Algiers 3 Ibrahim Sultan Cheibout, Algeria, nassim.henad@univ-alger3

Received: 19/06/2026 | **Accepted:** 05/10/2026 | **Published:** 21/11/2026

***Abstract*—**Security communication has become an integral part of national security as one-way communication has given way to an interactive digital environment. News now comes from many sources and can circulate within minutes. A country's security therefore depends in part on how well the state and the public protect their information environment and respond to rumors, false reporting, and online influence campaigns.

This study examines how security communication in Algeria contributes to prevention, public awareness, and crisis management. It considers how digital platforms have changed the spread of false information and the conditions under which public institutions can respond. The legal context includes Organic Law Nº.23-14 on information and the legislation governing the print and online press and audiovisual activity.

The study proceeds from the premise that the effectiveness of security communication depends on the accuracy and credibility of the information provided, the ability to anticipate rumors, and the public's capacity to recognize risks. Monitoring and digital verification can support these efforts while protecting media freedom and citizens' right of access to information.

***Keywords*—**security communication, Algerian national security, digital transformation, information threats…

Introduction

Over the past few decades, changes in media and communications have reshaped relations among the state, the public, and the press. Internet access and the spread of social media have given individuals unprecedented opportunities to produce and distribute information. A citizen can now publish an account of an event and reach a large audience without going through a newsroom.

Wider participation and easier access to information have also created favorable conditions for rumors, false news, and misleading accounts. The information environment itself has become a site of conflict, particularly when people use information to sway public opinion, undermine confidence in institutions, or create fear and confusion. Recent research increasingly treats disinformation as a matter of national security and social stability and as a feature of hybrid threats.

These concerns have particular relevance in Algeria, where the expansion of digital platforms has changed the media landscape and more people turn to social networks for news. As a form of institutional communication, security communication can help people understand the risks they face, correct inaccurate reports, and provide an official account during a crisis. How institutions carry out these tasks affects the trust citizens place in them.

Earlier Algerian studies have linked security communication to prevention, education, and changes in public behavior. Research on counterterrorism in Algeria, for example, suggests that the media can help citizens recognize threats to themselves, their communities, and the state. A more recent Algerian study argues that fabricated digital content can spread fear, undermine social stability, and affect political and economic life.

These developments call for a broader understanding of security communication in Algeria. Reporting the activities of security agencies is one part of a larger responsibility that includes preventing harm, managing crises,

© 2026 The Author(s). Published by Revista Infoacceso.

responding to information threats, and strengthening society's capacity to withstand disruption.

Research Problematic

How does security communication help protect Algeria's national security amid digital transformation and information threats? Five questions guide the discussion:

- *What is security communication, and what functions does it perform in the field of national security?*
- *How can it help prevent security threats?*
- *What role does it play in managing security crises?*
- *How can it counter false news and online rumors?*
- *How should Algeria reconcile media freedom with the requirements of national security?*

Study Objectives

- To encourage conduct that promotes public safety and peace of mind. Public information campaigns can explain citizens' responsibilities and the practical steps they can take to protect their lives and property from crime and from harm arising from unfamiliarity with safety precautions.
- To give citizens access to information about public security issues that affect their lives now or may affect them in the future.

Methodology

The study adopts a descriptive and analytical approach to examine security communication and the circumstances in which Algeria seeks to protect national security. Descriptive research provides a framework for collecting data from individuals when a study calls for such evidence (Abd al-Hamid, 2004, p.158).

One aim of descriptive research is to understand present conditions well enough to inform future action. Its findings can guide proposed changes by identifying relationships both between phenomena and among the elements of a single phenomenon (Melhem, 2002, p.353). It examines phenomena as they occur and can describe them qualitatively, in terms of their characteristics, or quantitatively, in numerical terms (Bouhouche & Al-Dhunaybat, 1995, p.129).

1. Conceptual Framework for Security Communication and National Security

1.1. Defining Security Communication

The Arabic term *al-i'lam al-amni*, rendered here as "security communication," brings together two fields often treated separately. Asiri (2000, p.21) observes that although Arabic- and English-language scholarship has long examined the relationship between media and security, the use of a single term for the two is largely a development of Arabic scholarship.

The term initially referred chiefly to the internal security of the state and society. Its scope was more closely associated with public safety and social stability than with economic, environmental, or food security. In this understanding, security communication draws on a society's intellectual and cultural traditions (Asiri, 2000, pp.148-149).

Definitions vary among researchers and practitioners, but three recurring concerns help explain the emergence of this field.

- How can media technology, professional skill, and editorial experience make knowledge about security accessible to the widest possible audience?
- How does security communication fulfill the educational function of the media by introducing audiences to new information, ideas, and events?
- How can specialist reporting respond to developments in different areas of public life and meet audiences' changing interests and information needs (Umar, 1997, p.18)?

The principal definitions in the literature emphasize different aspects of the work.

- Aljahni (1994, p.161) includes reporting, public outreach, and awareness activities undertaken by the relevant bodies to protect individuals, communities, the nation, and its achievements in keeping with recognized purposes and interests.
- A second definition emphasizes the experience of security. Individuals should know how to seek protection and feel secure in their lives, religious beliefs, honor, property, and other fundamental rights,

free from intimidation, coercion, or injustice.

- Another definition emphasizes truthful reporting of security matters and the views surrounding them. By explaining risks and responsibilities, security communication can reassure the public and enlist its support in addressing crime and recognizing harmful conduct (Abd Allah, as cited in Naji, 1997, p.7).
- A further definition stresses the public's need for comprehensive, timely, and relevant information about events, conditions, and laws affecting the security and stability of society.
- An institutional definition highlights the reciprocal relationship between security agencies and the media. Their cooperation can help agencies use the media effectively to communicate with the public (Al-Shahri, 2001, p.187).

1.2. Characteristics of Security Communication

Specialist knowledge. Reporting on security requires a precise understanding of the legal, institutional, and operational concepts involved.

Accuracy. An error in a public security announcement can have consequences well beyond those of an ordinary reporting mistake.

Timeliness. During a crisis or major incident, a delay in releasing official information gives rumors time to spread.

Responsibility. Inaccurate or incomplete accounts of security issues can frighten and confuse the people who depend on them.

Anticipation. Sustained public education can help prevent harm before a crisis occurs.

1.3. Functions of Security Communication

A. Prevention

One of the principal functions of security communication is to help citizens recognize risks and take precautions. Its preventive work includes the following activities.

- Supporting crime prevention.
- Helping prevent terrorism and extremism.
- Explaining the risks associated with drugs.
- Protecting children and young people from online exploitation.
- Raising awareness of cybercrime.
- Alerting the public to online fraud.
- Explaining the harm that rumors can cause.

B. Public Awareness

Security messages can build a shared understanding of public safety. In practical terms, citizens need enough knowledge to do the following.

- Recognize risks.
- Respond appropriately during a crisis.
- Verify information.
- Avoid sharing unreliable reports.
- Report dangerous content.
- Protect their personal data.
- Use social media responsibly.

C. Communication During Crises

During a security incident, disaster, or other major event, people need information urgently. If they cannot find a reliable official account, they may turn to informal sources. In the resulting information vacuum, several kinds of material can circulate.

- Unconfirmed reports.
- Old photographs presented as current.
- Videos removed from their original context.

- Posts from fictitious accounts.
- Conflicting accounts of the same event.

A prompt official account serves the public's immediate need for news and can also form part of the measures that authorities take under the law to protect public safety.

1.4. Defining National Security

Three broad approaches have shaped definitions of national security: classical realism, an economic perspective, and a comprehensive approach. Classical accounts generally emphasize military or "*hard*" security. In the realist account considered here, independence and sovereignty depend on military strength, and external aggression constitutes the threat against which the state must defend itself (Abd al-Wahid, 2014, p.32).

An exclusively military definition has difficulty accounting for all the conditions a state needs to survive. The ability to maintain and increase military strength matters, but less tangible aspects of security also shape a country's prospects. Excessive concentration on military capacity can itself put national security at risk.

In the Algerian context, national security encompasses the political, security, economic, social, and informational capacities through which the state protects vital national interests. These capacities help preserve sovereignty, unity, and stability and enable the country to respond to conventional threats as well as threats arising in the digital environment.

1.5. The Relationship Between Media and National Security

Media coverage can influence how people understand an event and how they respond to it. Responsible journalism can help individuals form considered judgments and understand the society on which their own future depends (Al-Hawshan, 2014, p.45). By making knowledge accessible, the media can strengthen social ties, mutual support, and the conditions in which people feel secure.

The media therefore have a responsibility to identify threats to a society's beliefs, values, cohesion, and security. Explaining the motives behind a threat and its likely consequences can help the public recognize the risks of social fragmentation, anxiety, and confusion.

Security also has a subjective dimension. The way the media report an incident can quickly affect whether people feel safe and how they regard the officers responsible for protecting them. Coverage can foster reassurance and respect. An inaccurate portrayal of an institution can equally weaken confidence in its ability to do its work. Hashem et al. (n.d., p.16) identify several reporting practices that may have this effect.

- Covering only the shortcomings of security work while overlooking achievements.
- Misreporting the facts of a security incident.
- Overlooking officers' efforts to maintain public safety and investigate crime.
- Giving disproportionate prominence to officers' mistakes.

2. Security Communication and the Response to Information Threats

2.1. False News and Disinformation

One of the greatest difficulties in responding to a false report is the speed at which it reaches an audience. By the time a newsroom has checked the facts, the original claim may already be widely accepted (Bouziane, 2021, p.34).

The expression "fake news" can obscure an important distinction about intent. A person who shares a false story may believe it to be true. Disinformation involves deliberately producing or circulating misleading information to influence public opinion in a direction favorable to those behind it. Misinformation refers to inaccurate information that can also be created or shared in good faith (Escande-Gauquié & Naivin, 2019, p.55).

Conspiracy narratives alleging hidden institutional or malicious activity develop through the efforts of those who believe them. People interpret and combine accounts, elaborate on them, and pass them on in different forms (Asselin, 2021, p.31). In this environment, one individual can consume, produce, and distribute news. Cognitive biases may reinforce the conviction that one has uncovered something powerful interests have concealed and that other must be warned. The reach of any such warning, however, varies considerably from one person to the next.

Psychological and social factors also help explain why false reports can intensify polarization over political and social issues or reinforce allegiance to a public figure. A story that attracts international attention can draw people into a debate simply because others are participating. Users may knowingly or inadvertently recirculate fabricated

accounts originating in Western media environments. Digital platforms give those accounts opportunities to reach new audiences.

False news thus overlaps with rumor, fabrication, and other forms of misleading communication. Disinformation can mix genuine facts with invented material. It can also involve networks of fictitious followers that make a claim appear more widely accepted than it is. Understanding its influence requires attention both to who produces the content and to who amplifies it.

2.2. Digital Rumors and Their Effects on National Security

One account of rumor describes it as a form of social aggression that can express underlying anxieties and shape what people say and do. Rumors about matters central to daily life can leave people uncertain about their livelihoods, safety, or social relations. Their effects may be particularly acute when people lack reliable knowledge or confidence in sources of stability such as public security, religious beliefs, and shared values. In psychological warfare, rumors can be used to damage individual reputations and weaken public morale (Kafi, 2015, pp.98-99).

Digitization has changed both the reach of rumors and the chances of exposing them. Websites and email allow accurate and inaccurate accounts to travel with comparable ease, across distances and at speeds difficult to achieve through earlier channels (Al-Harbi, 2012, pp.114-115). The same access also makes it easier for readers to discover that a picture, report, or story has been fabricated.

Two conditions are especially important in explaining why a rumor spread.

- **Importance.** The subject matters to the community in which the rumor circulates.
- **Ambiguity.** The information leaves significant questions unresolved, and its credibility is difficult to establish.

The more consequential a subject appears, the larger its potential audience. Uncertainty can accelerate transmission as people try to make sense of what they have heard. The two conditions interact. Even an important story may gain little traction as a rumor where information is readily available and the public can evaluate it. Conversely, uncertainty alone is unlikely to give a story wide appeal if few people care about its subject.

Ready access to a communication channel can accelerate transmission, while access to several channels can extend a rumor’s reach. The extent of that effect depends on how far those channels lend themselves to misuse (Uwaydah, 1996, p.27).

2.3. Deepfakes and Synthetic Content

A distinction drawn in the literature on falsification is between fabricating an object in its entirety and altering part of an existing object to misrepresent it (Waqi Allah, 2014, p.107). Both possibilities are relevant to contemporary digital media.

Advances in artificial intelligence (AI) have made it possible to generate remarkably convincing images, video, and sound. A deepfake uses AI, particularly deep learning, to create or manipulate audiovisual material. Examples include substituting a face, imitating a voice, or assembling a scene that never took place. Synthetic content is a broader category. It includes text, illustrations, photographs, music, speech, and video produced wholly or partly by AI systems. Such material has legitimate uses in education, media production, training, and simulation. It can also be used to mislead people or influence public opinion.

Deepfakes exploit the evidentiary weight that audiences give to seeing and hearing an event. A fabricated recording can appear to show a political figure, security official, or journalist making a statement that person never made. Its circulation could create confusion or affect political, security, or economic decisions. Other potential harms include financial fraud, impersonation, online extortion, defamation, and breaches of privacy. Organized propaganda campaigns may use synthetic material to discredit institutions or influence public attitudes.

For journalists, the difficulty extends to the credibility of sources and of news itself. A recording can spread on social media before anyone has established its origin. Repeated exposure to fabrications can erode trust in both news organizations and official institutions. It can also make it easier for someone confronted with a genuine recording to dismiss it as AI-generated, a problem sometimes described as the denial of digital evidence.

A coordinated response would combine technical detection with checks on a recording’s origin and integrity, clear disclosure of AI-generated material, and cooperation among news organizations, security institutions, and technology providers. It would also address the legal treatment of digital crime and the protection of personal data. Media and digital literacy remain essential. People can learn to compare a claim with independent, reliable

sources and to pause before circulating controversial material. Visual anomalies, irregularities in a voice, and automated detection scores may provide clues, but any one of them may be insufficient to establish authenticity.

Deepfakes and other synthetic media consequently raise questions for information security, national security, and public trust. The challenge is to retain the benefits of AI for development and innovation while limiting uses that harm individuals and institutions or undermine confidence in public debate.

2.4. Media Monitoring and Information Verification

Information includes facts, concepts, and knowledge that can guide action or inform a decision. Sources include books, journals, research papers, and reports, as well as maps, photographs, microforms, sound recordings, and films (Tuaymah, 1975, p.58). Access to information supports activity across society and provides a foundation for scientific, industrial, and cultural development (Naif Arab Academy, 2014, p.33).

Media monitoring draws on several types of publicly circulating material.

- News media.
- Social networks.
- Websites.
- Public forums.
- Digital content shared across platforms.

Its purpose is to identify information relevant to public safety and understand how it circulates, within the limits established by law. Monitoring the public itself falls outside that purpose.

Before publishing information about a security matter, a newsroom or public institution should check the following details.

- The original source.
- The date.
- The context in which the material first appeared.
- Any accompanying photographs.
- Any video footage.
- The identity of the account that published it.
- How the account compares with available official information.

3. Toward a National Strategy for Security Communication in Algeria

3.1. Building a Proactive Security Communication System

Rapid changes in technology and communication have made security communication central to national security and social stability. Agencies that once concentrated on reporting incidents must also communicate during crises, respond to rumors and disinformation, and help citizens recognize risks before they materialize.

For Algeria, regional and international developments, growing digital threats, and the influence of social media give particular urgency to this task. Military and institutional capacity remain important. National security also depends on the state’s ability to manage information, protect the digital environment, communicate constructively with the public, and earn citizens’ trust.

An integrated national strategy would bring together strategic planning, coordination among institutions, investment in technology, and specialist training. It would allow security communicators to anticipate information needs and protect national interests as circumstances change, extending their work beyond issuing statements in response to events.

3.2. Training Journalists in Security and Digital Reporting

Digital journalism requires information-handling skills and the ability to publish across media. The conventional newsroom now coexists with mobile and digitally integrated newsrooms. Mobile journalism, algorithmic journalism, augmented reality, and holographic presentation illustrate the range of technologies entering news production.

Applications in the newsroom include editing, production, distribution, cloud computing, investigative and solutions journalism, audience sentiment analysis, the detection of misleading reports, and smart imaging. Blockchain technology, a distributed database that maintains a growing sequence of records, is another development discussed in this context. For journalism educators, the challenge is to keep pace with these changes

and design courses that reflect the work graduates will undertake.

Media employers and journalism schools face practical constraints. Limited training budgets restrict access to up-to-date equipment, and institutions responsible for education and professional training do not always coordinate with the organizations that employ their graduates (Abd al-Ghani, 2008, p.320).

3.3. Using Artificial Intelligence

AI can support security communication in several tasks.

- Analyzing large volumes of content.
- Tracking relevant keywords.
- Classifying news reports.
- Assisting verification teams.

Decisions on sensitive matters still require human judgment. Professionals must assess the evidence, the editorial implications, and the applicable legal requirements before acting on an automated result.

3.4. Strengthening Cooperation Between Security Institutions and the Media

Security agencies perform social, humanitarian, political, economic, and developmental functions alongside their responsibility for public safety. Under a comprehensive understanding of security, protecting citizens and the country extends beyond criminal investigation into many aspects of everyday life.

The media likewise reach across areas of public life and social groups. They disseminate knowledge, shape public awareness, and influence the values and conduct a society encourages. In doing so, they draw on standards intended to serve the public interest and sustain social life.

These overlapping responsibilities provide a basis for cooperation and coordination. Isolation can leave security agencies less able to reach the public and journalists less able to explain security matters. Khaddour (2014, pp.85-86) argues that cooperation has become necessary because public security is a concern shared by both institutions.

3.5. Building Trust and Credibility with the Public

Security communication can strengthen ties between agencies and citizens by explaining how the agencies work, reporting on security conditions, and describing efforts to protect life and property. It can also show citizens how to protect themselves against crime and how they can support the institutions responsible for justice and public safety (Naji, 1987).

Reporting can make the public service performed by police officers visible and explain how their work contributes to everyday safety. When people understand that contribution, their confidence can translate into practical cooperation with officers carrying out their duties.

This relationship matters in contemporary societies because stability and personal safety are goals that citizens and the police share. A citizen who understands what security work involves is better placed to recognize when cooperation is needed and how to assist.

Conclusion

Security communication now forms part of the protection of national security. Alongside reporting the activities of security agencies, it contributes to prevention, public awareness, crisis management, and the work of building trust and correcting disinformation and rumors.

In Algeria, the rapid shift toward digital communication has expanded the number of news sources and the reach of social networks. The speed at which false reports, misleading accounts, and manipulated media can circulate presents a particular challenge for journalists and security institutions alike.

Protecting national security in this environment requires the ability to produce reliable information, detect emerging concerns, verify digital material, respond promptly, and help the public assess the information it encounters. Algeria’s security communication system would benefit from a more anticipatory and professional approach linking journalism, strategic communication, technology, and information analysis. Its credibility also depends on protecting media freedom and citizens’ right of access to information.

Findings

The analysis yields the following theoretical findings.

- Security communication has become part of strategic communication on matters of national security.

- Prevention, public education, crisis communication, and the correction of inaccurate information all contribute to national security.
- The speed of digital circulation has increased the importance of timely security communication.
- False reporting and digital disinformation can affect social stability and national security as well as the media themselves.
- Open-source intelligence (OSINT) and AI can strengthen monitoring and analysis when used lawfully and in accordance with professional standards.
- Security communication depends on a credible relationship with citizens.
- Digital monitoring and analysis are essential functions of contemporary security communication.
- Algeria needs the capacity to anticipate information threats and intervene before widely shared falsehoods become harder to correct.
- Media law helps define the relationship between press freedom, professional responsibility, and the public interest. Organic Law No. 23-14 is a central part of this framework.

Recommendations

- Adopt an integrated national strategy for security communication and public information.
- Establish or strengthen specialist units for monitoring and verifying digital information.
- Expand cooperation among security agencies, news organizations, universities, and research centers.
- Develop specialist training for journalists in digital security and news verification.
- Include media and digital literacy in public awareness programs.
- Strengthen the online presence of public institutions.
- Establish procedures for correcting false reports promptly, particularly during crises.
- Use AI and data analysis in accordance with legal and ethical standards.
- Develop the use of OSINT in research, verification, and media analysis.
- Build public trust through transparent, clear, and timely communication.
- Balance national security requirements with media freedom and citizens' right of access to information.
- Support Algerian research on security communication, information security, digital disinformation, strategic communication, and information warfare.

References

Abd al-Ghani, A. S. (2008). E-learning in Arab media education and training: New media and the second digital wave. Cairo, Egypt: Itrak.

Abd al-Hamid, M. (2004). Scientific research in media studies. Cairo, Egypt: The Books' World.

Abd al-Wahid, I. (2014). A theoretical foundation for the components and policies of national security. *International Political Journal, 50*(197), 32-44. doi:10.12816/0024093

Al-Harbi, H. (2012). Rumors and the role of the media in the information age. Amman, Jordan: Usamah Publishing House.

Al-Hawshan, B. Z. (2014). Security communication and media security. Amman, Jordan: al-Hamid House for Publishing.

Aljahni, A. F. (1994). Security communication: Concepts and foundations. *Security Journal*, (8), 161-203.

Al-Shahri, F. A. (2001). Internet use in Arab security communication. *Journal of Security Researches, 10*(19).

Asiri, A. M. (2000). Security communication in the Arab world. Riyadh, Saudi Arabia: Naif Arab Academy for Security Sciences.

Asselin, C. (2021). *Fake news: 5 points importants à connaître pour les comprendre et les combattre* [Fake news: Five key points for understanding and combating it]. Paris, France: Digimind.

Bouhouche, A., & Al-Dhunaybat, M. M. (1995). Scientific research methods and the preparation of research papers. Algiers, Algeria: Office des Publications Universitaires.

Bouziane, N. (2021). Fake news, online trolls, and the manipulation of public awareness: Prevention and responses. *Academia*, *6*(5), 28–46. Retrieved from https://asjp.cerist.dz/en/article/172970

Escande-Gauquié, P., & Naivin, B. (2019). *Comprendre la culture numérique* [Understanding digital culture]. Paris, France: Dunod.

Hashem, S., et al. (n.d.). Shortcomings of media organizations and their impact on security. Unpublished manuscript, Officers' Training Institute, Cairo, Egypt.

Kafi, M. Y. (2015). Wartime media, propaganda, rumor, and psychological warfare. Amman, Jordan: Usamah Publishing House.

Khaddour, A. M. (2014). Ways to strengthen trust between Arab security and media institutions. Amman, Jordan: al-Hamid House for Publishing.

Melhem, S. M. (2002). Research methods in education and psychology. Amman, Jordan: al-Masirah Publishing House.

Naif Arab Academy. (2014). Rumors in the information age. Amman, Jordan: al-Hamid & Al-Akadimiyyun Publishing House.

Naji, I. (1987). The state of security awareness in Arab countries. Paper presented at the Symposium on Security Awareness in the Arab World, Riyadh, Saudi Arabia.

Naji, I. (1997). The role of the media in combating and reducing crime. Paper presented at the Naif Arab Academy Symposium on Security Communication: Problems and Solutions, Cairo, Egypt.

Tuaymah, S. (1975). Knowledge in the approach of the Holy Qur'an. Beirut, Lebanon: al-Jabal Publishing House.

Umar, A. A. (1997). Specialist media. Benghazi, Libya: Garyounis University.

Uwaydah, M. (1996). The psychology of rumor. Beirut, Lebanon: Scientific Books Publishing House.

Waqi Allah, M. A. (2014). Methods of counterfeiting and forgery and how to detect them. Amman, Jordan: al-Hamid Publishing House.