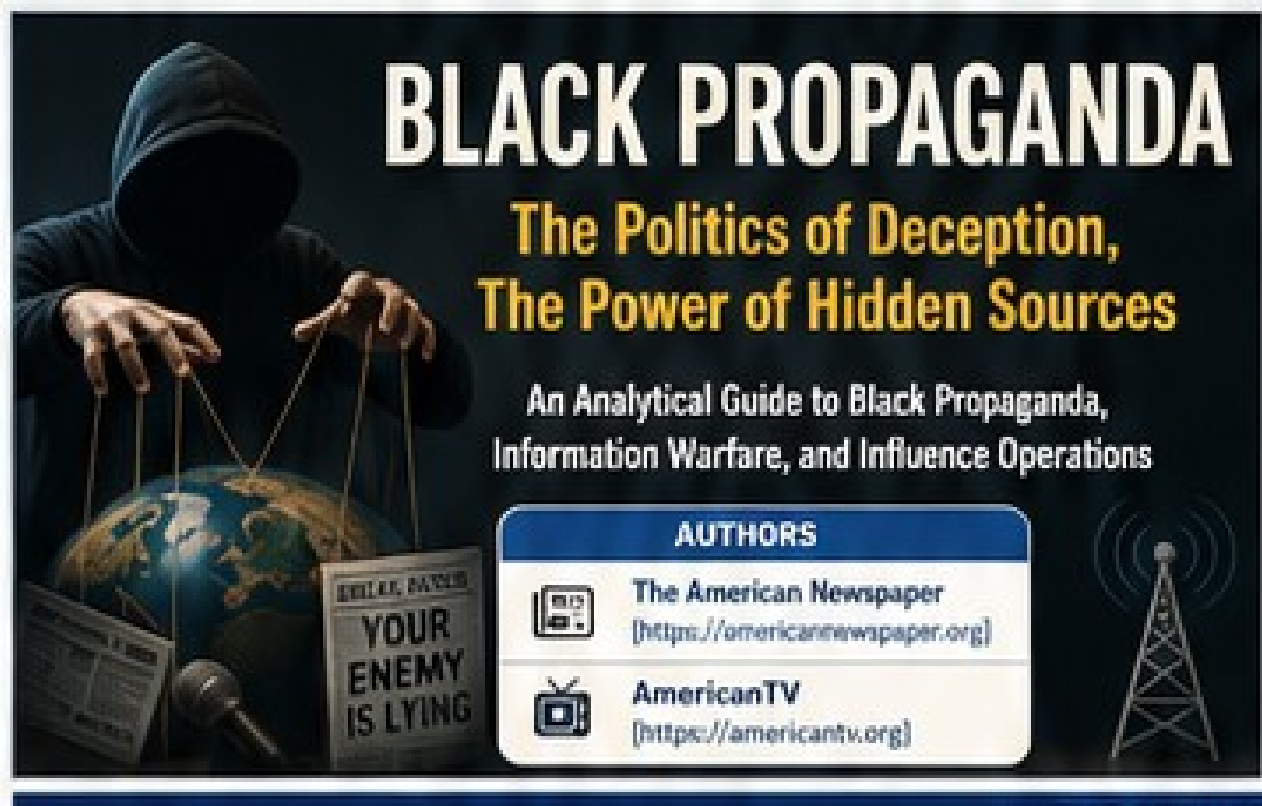


BLACK PROPAGANDA

Source Deception, Covert Influence, Psychological Warfare, and the Manipulation of Trust

A Systematic Guide to Concepts, History, Psychology, Detection, Law, and the AI Era



Original AI-generated editorial illustration created for this report. It is conceptual artwork, not historical evidence.

Authors

The American Newspaper <https://americannewspaper.org>

AmericanTV <https://americantv.org>

Research edition - August 2026

Scope and safety This report analyzes black propaganda for historical, journalistic, policy, forensic, and defensive purposes. It intentionally does not provide a procedural playbook for conducting covert deception, impersonation, illegal election interference, market manipulation, or other unlawful operations.

Executive Summary

Black propaganda is best understood as an attributional deception system: the defining manipulation concerns who appears to be speaking. A black-propaganda message is deliberately made to seem as though it came from an adversary, dissident faction, independent outlet, grassroots group, expert, neutral third party, or other source different from the real sponsor. Its factual content may be true, partly true, misleading, fabricated, or a changing mixture of all four. This is why “black propaganda” should not be used as a synonym for “false information.”

The central analytical rule Classify the truth status of the content and the authenticity of the source on separate axes. Content falsity asks: “Is the claim false or misleading?” Source falsification asks: “Who is really speaking, and is that identity authentic?” Black propaganda is principally about the second question.

- White, grey, and black propaganda are primarily source-attribution categories. White identifies the sponsor; grey leaves the sponsor uncertain or unstated; black deliberately attributes the message to a false source. [1][2]
- Disinformation and black propaganda overlap but are not identical. Disinformation requires intentional deception through false or misleading information; black propaganda requires false attribution. A genuine leaked fact can be used in black propaganda if its provenance is deliberately falsified, while a government can publish disinformation openly under its real name without making it black propaganda. [3]
- Black propaganda works through credibility transfer: the operator borrows the presumed credibility, identity, grievance, access, or legitimacy of the impersonated source. The principal target is therefore not only factual belief but the target audience’s trust map - whom it trusts, distrusts, fears, or regards as “one of us.”
- Historical black propaganda moved from forged documents, clandestine leaflets and pseudo-enemy radio stations to covert sponsorship, front organizations, fabricated personas, hacked-and-leaked material, cloned news sites, bot-assisted distribution, influencer laundering, and AI-generated media.
- Psychological effects depend heavily on pre-existing conditions. Polarization, war, economic crisis, distrust, censorship, uncertainty, identity conflict, and information overload can make attributional deception more plausible, but exposure does not automatically produce persuasion or behavioral change.
- Digital platforms reduce the cost of identity manufacture and multilingual content production, but recent platform and government investigations also show that many covert networks achieve little authentic engagement. Scale of output should not be confused with scale of influence. [11][12][13]
- Detection is fundamentally a provenance problem: identify the earliest traceable source, validate the sender’s identity, reconstruct the diffusion path, compare account behavior, authenticate media and documents, and distinguish evidence of coordination from mere ideological similarity.
- In U.S. law, false or deceptive political speech sits at the intersection of strong First Amendment protections, defamation and fraud doctrines, election rules, foreign-national restrictions, FARA disclosure obligations, impersonation statutes, platform policies, and national-security authorities. There is no general federal crime called “black propaganda.” [19][20][21][22][23]
- In armed conflict, a communications false attribution is conceptually different from a military false flag involving the improper use of enemy flags, insignia, uniforms, or protected emblems. International humanitarian law regulates the latter more specifically, especially when used in connection with attacks. [25]
- AI will make fabrication cheaper and faster, but the hardest part of successful black propaganda remains social: acquiring trusted distribution, choosing narratives that resonate with existing beliefs, surviving verification, and converting exposure into durable behavior.

Report map

1. Definition, etymology, and the white-grey-black taxonomy
2. Conceptual distinctions: propaganda, disinformation, PSYOP, influence operations, deception, and related terms
3. The architecture of black propaganda and the primacy of source deception
4. Historical evolution from World War I to the AI era
5. Ten representative historical and contemporary cases
6. Psychological mechanisms and social conditions of susceptibility
7. Source laundering, digital networks, bots, fake personas, influencers, and generative media
8. Black propaganda and false flags
9. Democracy, elections, corporate reputation, and financial markets
10. U.S. law, platform rules, international law, and law of armed conflict
11. Detection and defensive analysis framework
12. Common analytical errors and standards of evidence
13. Twenty core concepts; ten scholars; twenty authoritative sources
14. Comparative tables and future assessment of AI-enabled black propaganda

Evidentiary labels used in this report

Label	Meaning
Documented	The sponsorship, attribution, or event is supported by primary records, declassified material, court filings, official archives, or strong scholarly consensus.
Official allegation	A government indictment, complaint, intelligence assessment, or public attribution asserts the claim; it may not have been adjudicated in court.
Scholarly interpretation	A credible historian or researcher offers an interpretation that may be debated or depend on incomplete archives.
Impact uncertain	The operation is documented, but causal claims about persuasion, voting, morale, policy, or social harm cannot be quantified confidently.
Contested	Serious competing interpretations exist; the report states the disagreement rather than presenting one side as settled fact.

1. Definition, Etymology, and the White-Grey-Black Taxonomy

1.1 Propaganda: definition and etymology

The modern word “propaganda” derives from the Latin *propagare*, “to spread” or “to propagate,” and from the Catholic Congregatio de Propaganda Fide, established in 1622 under Pope Gregory XV to coordinate the propagation of the faith. The secular political sense developed later and became especially prominent during the era of mass politics and World War I. Propaganda, in the broad scholarly sense, is organized communication designed to shape perceptions, interpretations, emotions, attitudes, or behavior in ways that advance the objectives of a sponsor. It is not defined solely by factual falsity. [1]

Source note: Springer Nature Encyclopedia of Political Communication, “Propaganda” (2026); Etymonline, “propaganda.”

1.2 What makes propaganda “black”?

The most rigorous source-based typology treats white, grey, and black as categories of attribution. White propaganda comes from the source it claims to come from. Grey propaganda leaves the source unidentified, ambiguous, or difficult to establish. Black propaganda is deliberately attributed to a false source - often a source within the target group, an adversary institution, a dissident movement, a supposedly independent media outlet, or a neutral third party. Air University’s classic PSYOP text makes the distinction explicit: black material is produced by one source but purports to have emanated from another. Contemporary scholarship likewise describes the taxonomy as source-based. [1][2]

Type	Truth/falsity of content	Authenticity of source	Sender disclosed?	Deception level	Typical purpose
Propaganda in general	May be true, selective, misleading, or false	May be open or concealed	Varies	Varies	Influence perceptions, attitudes, agendas, or behavior for a sponsor’s objective
White propaganda	Often accurate or selectively accurate, but not guaranteed	Authentic	Disclosed/identifiable	Low source deception	Persuade or mobilize while retaining overt sponsorship
Grey propaganda	Variable	Unknown, ambiguous, or not established	Not clearly disclosed	Moderate attribution ambiguity	Create plausible distance, uncertainty, or deniability
Black propaganda	May be true, partly true, misleading, false, or mixed	Deliberately false attribution / impersonation	Real sponsor concealed	High source deception	Borrow another source’s credibility or identity; divide, discredit, demoralize, confuse, or induce behavior

Why truth is not the defining axis A true statement can be black propaganda if a state secretly writes it and presents it as the authentic statement of an enemy soldier, dissident group, independent journalist, or grassroots movement. Conversely, a state can openly publish a false claim under its own name: that is disinformation, but not necessarily black propaganda.

1.3 Two-axis classification: content and source

Source / Content	Mostly true or verifiable	Selective / misleading	Fabricated / false
Authentic and disclosed	White propaganda or ordinary advocacy	White propaganda / strategic framing	Open disinformation or false propaganda
Unclear / unattributed	Grey propaganda	Grey propaganda, rumor, or unattributed influence	Grey disinformation
Falsely attributed	Black propaganda using truthful content	Black propaganda using selective/manipulated content	Black propaganda + disinformation

1.4 Why source falsification is especially powerful

- **Credibility borrowing:** the message inherits the perceived trustworthiness, access, authenticity, or social identity of the impersonated source.
- **Identity penetration:** a message that appears to come from “one of us” can bypass defenses normally activated against an acknowledged adversary.
- **Attributional sabotage:** the operator can cause the target to distrust a real institution by issuing embarrassing, extreme, incompetent, or contradictory messages in that institution’s name.
- **Plausible deniability:** the real sponsor gains distance from the message and may avoid political, diplomatic, reputational, or legal costs until attribution is established.
- **Network laundering:** each repost, translation, quotation, screenshot, or mainstream-media citation can separate the audience farther from the original source.
- **Behavioral ambiguity:** even after a factual claim is corrected, the false identity can leave durable suspicions about who is authentic, who is compromised, and what institutions can be trusted.

2. Conceptual Distinctions: The Information-Influence Vocabulary

Analytical precision matters because adjacent concepts classify different things: some classify truth status, some classify sponsorship, some describe military missions, some describe organizational secrecy, and some describe distribution tactics. Treating them as interchangeable produces false attribution and weakens forensic analysis.

Concept	Operational distinction
Propaganda	Organized communication intended to shape perceptions, attitudes, or behavior in line with a sponsor's objectives. Truthfulness and disclosure vary.
Disinformation	False or misleading information deliberately created or disseminated to deceive. The defining axis is intentional content deception. [3]
Misinformation	False information shared without the sharer intending to cause the relevant harm or deception. [3]
Malinformation	Genuine information used or disclosed in a harmful manner, commonly through decontextualization or release of material meant to remain private. [3]
Psychological warfare / PSYWAR	The broader wartime use of psychological means to weaken an adversary's will, cohesion, confidence, or decision-making; historically wider and less doctrinally precise than modern PSYOP.
Psychological operations / PSYOP	Planned activities directed at selected audiences to influence emotions, motives, reasoning, attitudes, and behavior in support of objectives. Modern U.S. terminology has also used Military Information Support Operations. [2]
Information operations / IO	Coordinated employment of information-related capabilities to affect information, information systems, decision processes, or the information environment, usually integrated with operations.
Influence operations	A broad family of coordinated activities intended to shape perceptions, preferences, decisions, or behavior. May be overt or covert, truthful or deceptive.
Perception management	A Cold War/post-Cold War policy term for efforts to influence how selected audiences interpret events and actors. It can include truthful information, deception, and psychological techniques depending on context.
Deception	Intentional action designed to cause a target to form a false belief about facts, capabilities, intentions, identity, or circumstances.
Strategic communication	Coordinated communication intended to align words, actions, narratives, and policies with strategic objectives; it is not synonymous with deception and often emphasizes credibility.
Fake news	A politically overloaded and analytically imprecise label. Scholars and the Council of Europe caution that it collapses distinct phenomena and is often used to dismiss disliked reporting. [3]
Rumor	Unverified information circulating under uncertainty. Rumor can be spontaneous, accurate, false, or deliberately seeded; rumor is not automatically propaganda.
Conspiracy theory	An explanatory narrative attributing events to secret coordination by powerful actors, typically resistant to ordinary disconfirmation. It can arise organically or be strategically amplified.
Astroturfing	The manufacture of an appearance of grassroots support, opposition, or spontaneous public sentiment when the activity is actually coordinated or sponsored.
False-flag communication	A message or communication event attributed to an adversary or third party while being produced by another actor. This is a communication analogue to - but legally distinct from - physical military false flags.
Front organization	An organization that appears independent but is covertly created, financed, directed, or substantially influenced by another sponsor. A front may conduct real activities while concealing sponsorship.
Covert influence operation	An influence campaign in which the sponsor, operational role, or coordination is deliberately hidden; the content itself need not be false.

Concept	Operational distinction
Source laundering	A process by which material moves through intermediaries so that its real origin becomes obscure and later audiences encounter it through seemingly independent sources.
Narrative laundering	The transformation of a claim from suspicious origin into apparently normal discourse through repetition, recontextualization, translation, citation, expert commentary, or media recirculation.

2.1 Disinformation vs. black propaganda

Dimension	Disinformation	Black propaganda
Primary object classified	Content / informational claim	Source attribution / identity
Necessary condition	Intentional falsehood or material misleadingness	Deliberate misattribution or impersonation of source
Can the message contain true facts?	Sometimes selective true facts support the deception, but the core claim is intentionally false/misleading	Yes. It can be entirely true in content if the origin is falsely attributed
Can the real source be openly disclosed?	Yes	No, not while the operation remains black
Typical deception	What happened? What is true?	Who is speaking? Who sponsors this? Where did it originate?
Typical overlap	Openly sponsored false narratives	Falsely attributed fabricated narrative = both disinformation and black propaganda
Best detection question	Can the claim be verified?	Can the claimed source and provenance be verified?

3. The Architecture of Black Propaganda

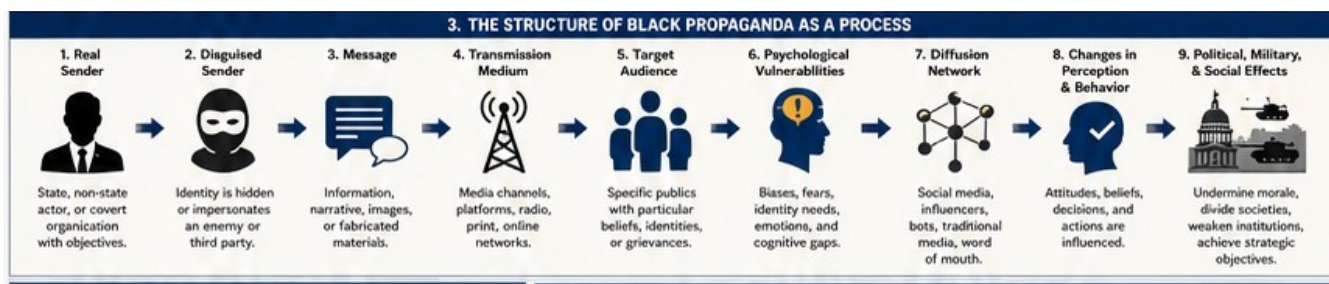


Figure 1. Conceptual process model for black propaganda. The image was generated for this report and is used as an explanatory diagram, not as evidence for any historical case.

Stage	Analytical questions
1. Real sender	The actual state, intelligence service, military unit, political organization, company, network, or non-state actor setting objectives or providing direction/resources.
2. Disguised sender	The identity presented to the audience: adversary broadcaster, dissident, local citizen, independent outlet, expert, activist, whistleblower, grassroots organization, or neutral third party.
3. Message	A narrative, claim, document, image, recording, meme, quotation, leak, rumor, or mixture of facts and fabrications calibrated to the target's beliefs.
4. Transmission medium	Historically: leaflets, radio, forged letters, newspapers, front publications. Digitally: websites, social platforms, messaging apps, video, podcasts, synthetic media, cloned outlets.
5. Target audience	Enemy troops, civilians, elites, diaspora groups, voters, activists, consumers, investors, journalists, policymakers, or specific communities.
6. Psychological vulnerabilities	Existing grievances, identity conflict, fear, uncertainty, distrust, ideology, prejudice, status anxiety, information scarcity, or demand for simple explanations.
7. Diffusion network	Intermediaries that reproduce the message: real users, influencers, bots, fake personas, front organizations, sympathetic media, aggregators, search/recommendation systems.
8. Perception and behavior	Possible outcomes include changed beliefs, distrust, hesitation, demoralization, social conflict, abstention, protest, policy pressure, reputational harm, or market behavior.
9. Political/military/social effects	Strategic outcomes are contingent. Some campaigns create measurable disruption; many produce noise without durable behavior change. Exposure can also create backlash against the sponsor.

3.1 Trust is the hidden resource

The disguised sender is not merely camouflage. It is a mechanism for reallocating trust. The operator attempts to make the audience evaluate the message under the credibility assumptions attached to the impersonated identity. A clandestine “enemy soldier” can appear to possess insider access; an “independent local journalist” can appear free of foreign interests; a “fellow activist” can appear motivated by shared identity; a forged official document can appear backed by institutional authority. The source is therefore part of the message.

3.2 Black propaganda as a systems mechanism

A useful systems formulation is: strategic objective × attribution deception × narrative resonance × trusted distribution × repetition × network adaptation, constrained by forensic exposure, counter-messaging, audience skepticism, and institutional resilience. No single variable guarantees effectiveness. Attribution deception can increase initial receptivity but also creates a catastrophic vulnerability: once exposed, the operation can discredit both the message and the sponsor.

4. Historical Evolution: From Mass Propaganda to Synthetic Personas

4.1 World War I: industrialized persuasion and the institutional foundations

World War I transformed propaganda into a mass governmental function. States created specialized offices, coordinated press and censorship systems, produced leaflets and atrocity narratives, and learned that modern communications could shape domestic morale, enemy morale, and neutral opinion. The later white-grey-black taxonomy became more explicit in professional psychological-warfare practice, but the war established the institutional logic: centralized message production, audience segmentation, credibility management, and integration of information with military and diplomatic objectives.

*Source note: U.S. Army historical accounts of World War I psychological warfare; Harold D. Lasswell, *Propaganda Technique in the World War* (1927).*

4.2 World War II: black radio, forged media, and false attribution at scale

World War II produced some of the clearest classic examples. Nazi Germany used staged incidents and propaganda to justify aggression. Britain's Political Warfare Executive (PWE), formally created in 1941, developed covert stations that sounded German and aimed to create division and distrust inside the Reich. Sefton Delmer's operations mixed authentic details, soldiers' gossip, music, news, and damaging allegations to make the broadcasts feel indigenous rather than British. The U.S. Office of Strategic Services used forged mail and documents in operations such as Cornflakes. These campaigns show why factual accuracy and source authenticity must be separated: high credibility often required substantial amounts of accurate information around strategically deceptive elements. [4][5]

Source note: UK National Archives, records of the Political Warfare Executive (FO 898); National WWII Museum, Operation Cornflakes.

4.3 Early Cold War: covert cultural and political influence

After 1945, the United States and Soviet Union institutionalized covert political warfare. U.S. programs included covert support for publications, cultural institutions, broadcasting, political groups, and anti-Communist networks. The CIA's sponsorship of the Congress for Cultural Freedom is a prominent case of concealed sponsorship: the organization and many intellectual activities were real, but CIA funding and direction were not disclosed to audiences. This is analytically adjacent to black propaganda but does not fit every strict definition because the CCF was not simply an invented enemy identity; it demonstrates the broader continuum from grey sponsorship concealment to full false attribution.

The Soviet KGB and allied services developed "active measures" that included forgeries, front organizations, planted stories, agents of influence, covert support, and disinformation. The goal was often not immediate belief in a single lie but the activation of existing distrust and conflict. Later archival research has clarified some operations while also correcting popular labels and myths about their codenames. [6]

4.4 Korean War: PSYOP expansion and contested allegations

The Korean War accelerated the permanent institutionalization of U.S. psychological operations. Leaflets, loudspeakers, radio, prisoner-related messaging, and battlefield persuasion were employed by multiple belligerents. One of the era's most consequential information controversies concerned Communist allegations that the United States used biological weapons. U.S. officials called the charges fabricated propaganda; later scholarship has continued to debate aspects of the documentary record. Because the underlying historical question remains contested, this report does not present the allegation as a settled example of black propaganda. The case is useful precisely as a warning against labeling disputed claims "black propaganda" before both falsity and source manipulation are demonstrated.

4.5 Vietnam: black PSYOP and the Sacred Sword legend

In Vietnam, U.S. covert psychological operations included the Sacred Sword of the Patriots League (SSPL), a notional anti-Communist resistance movement presented as an indigenous North Vietnamese organization. Declassified CIA material describes the Voice of the Sacred Sword broadcasting as if it emanated from an anti-Party resistance group inside North Vietnam. The operation illustrates a classic black structure: real U.S./South Vietnamese sponsorship, fictitious internal resistance identity, radio and other media, and a target population within the adversary state. Its strategic effects are difficult to quantify and historians disagree over its efficiency relative to resources committed. [8]

*Source note: CIA Reading Room declassified records on covert psychological warfare and the Sacred Sword Patriots' League; Richard H. Shultz Jr., *The Secret War Against Hanoi* (1999).*

4.6 Late Cold War: Soviet forgeries and AIDS disinformation

Soviet active measures often used source laundering: a claim or forged document would first appear in a small foreign outlet, be repeated by other intermediaries, and then be cited by Soviet media as though it were independent foreign reporting. The forged "FM 30-31B" document purported to be a secret U.S. Army manual advocating destabilizing actions in allied countries. U.S. authorities identified it as a forgery, and it circulated internationally for years. The AIDS disinformation campaign, known in Stasi records as Operation Denver and often - imprecisely - called "Operation INFEKTION," alleged that HIV/AIDS was produced by U.S. military biological-weapons research. Archival evidence from Eastern European services supports direct KGB involvement in the campaign. [6]

*Source note: Thomas Boghardt, *CIA Studies in Intelligence* 53(4), 2009; Mark Kramer / Douglas Selva discussion of Operation Denver, MIT Press Reader, 2020.*

4.7 Non-state actors: propaganda, pseudo-identities, and the importance of classification

Non-state actors - insurgent movements, extremist organizations, hacktivist networks, criminal groups, private intelligence contractors, political movements, and commercial influence firms - can use the same attributional techniques as states. The Islamic State, for example, became notorious for sophisticated online propaganda and recruitment, much of which was overtly branded rather than black. That distinction matters: violent or extremist propaganda is not automatically black propaganda. It becomes black when the actor deliberately impersonates another source, manufactures an apparently independent grassroots or media identity, or launders sponsorship through deceptive fronts. Research on jihadist social-media ecosystems illustrates the scale and network effects of non-state propaganda while also underscoring that sponsorship and truth status must be analyzed separately.

Source note: For non-state digital propaganda, see Badawy & Ferrara, "The Rise of Jihadist Propaganda on Social Networks" (2017), and broader literature on extremist strategic communication.

4.8 Post-Cold War and the internet: personas, leaks, cloned media, and networked influence

Digital communication changed the economics of black propaganda. Operators no longer needed a powerful transmitter or printing infrastructure to manufacture apparent social actors. False personas, anonymous accounts, cloned sites, compromised accounts, coordinated networks, and selective leaks could be combined with authentic user participation. Russian operations targeting the United States and Europe have included fake American personas, hack-and-leak personas, social-media fronts, and domains that imitate legitimate news organizations. PRC-linked networks have used large numbers of accounts, copied or AI-generated profile images, and cross-platform posting, though Google's 2024 analysis found very low authentic engagement for much of the DRAGONBRIDGE/Spamouflage network. [9][10][11][12]

4.9 Generative AI: lower production costs, not automatic strategic success

Generative AI can accelerate translation, rewriting, persona creation, image generation, audio/video synthesis, and content variation. Yet investigations by OpenAI and major platforms indicate that known covert networks often use AI as a productivity layer on top of older tactics rather than as a fundamentally new form of influence. Some detected networks generated large volumes of material but failed to achieve significant organic reach. The strategic bottleneck remains distribution, trust, resonance, and conversion of attention into behavior. [12][13]

5. Ten Representative Cases

The cases below are selected to show different forms of attribution deception. “Success” is not treated as synonymous with reach, and reach is not treated as synonymous with persuasion. When causal effects are uncertain, that uncertainty is stated explicitly.

1. Gleiwitz incident / Operation Himmler (1939)

Evidence status Documented physical false flag; boundary case for black propaganda

Field	Assessment
Real sender	Nazi German SS / Sicherheitsdienst apparatus
Impersonated / disguised sender	Polish attackers
Target audience	German public and international audiences
Message	Staged Polish aggression was used within a broader narrative that Germany faced Polish provocations before the invasion.
Delivery mechanism	A real-world staged attack at the Gleiwitz radio station and other fabricated border incidents; propaganda exploitation followed.
Trust-generating devices	Physical staging, planted evidence, immediacy of radio/news claims, state control of domestic media.
Observed / claimed effects	Helped provide a propaganda pretext, but historians do not treat it as the decisive cause of war or proof that international audiences accepted the story.
How exposed	Postwar testimony and documentation, including evidence associated with Nuremberg-era investigations.
Analytical lesson	Illustrates the distinction between a military/physical false flag and black communication: the physical event was staged, then communicated through overt Nazi channels.

2. Gustav Siegfried Eins (Britain, 1941-1943)

Evidence status Documented British black radio

Field	Assessment
Real sender	British Political Warfare Executive; Sefton Delmer's German-section operation
Impersonated / disguised sender	A clandestine nationalist German insider broadcaster (“Der Chef”)
Target audience	German listeners
Message	Anti-Nazi, anti-corruption, morale-undermining material presented through an apparently German patriotic voice rather than a British voice.
Delivery mechanism	Clandestine radio with convincing German idiom and insider tone.
Trust-generating devices	Cultural fluency, colloquial language, mixture of accurate details and damaging allegations, apparent in-group identity.
Observed / claimed effects	Precise behavioral effect is hard to quantify; historically important as a model of black radio and credibility engineering.
How exposed	British records, postwar memoirs, and PWE archival history.
Analytical lesson	The central deception was not merely factual but attributional: British messages were designed to appear indigenous to Germany.

3. Soldatensender Calais (Britain, 1943-1945)

Evidence status Documented British black radio

Field	Assessment
Real sender	British PWE
Impersonated / disguised sender	A German military entertainment/news station
Target audience	German soldiers and military-connected listeners
Message	Music, military news, rumors, and information intended to weaken confidence in Nazi leadership while sounding useful to soldiers.
Delivery mechanism	High-power medium-wave broadcasting; related shortwave programming for German forces.
Trust-generating devices	Timely operational detail, familiar broadcast style, entertainment, mostly plausible content surrounding subversive framing.
Observed / claimed effects	Widely remembered as sophisticated black propaganda; reliable quantitative estimates of morale impact remain limited.
How exposed	British archival records and postwar accounts.
Analytical lesson	Shows that effective black propaganda may depend on a high ratio of credible information to overtly manipulative content.

4. Operation Cornflakes (U.S. OSS, 1945)

Evidence status Documented covert forgery operation

Field	Assessment
Real sender	U.S. Office of Strategic Services
Impersonated / disguised sender	German postal and media ecosystem
Target audience	German civilians
Message	Anti-Nazi propaganda packaged to resemble ordinary German mail and print material.
Delivery mechanism	Forged mail placed into mailbags near bombed postal trains so German postal authorities could unknowingly deliver it.
Trust-generating devices	Authentic-looking envelopes, addresses, postal context, and German-format publications.
Observed / claimed effects	Some forged mail entered the postal system; direct strategic impact is difficult to measure.
How exposed	Declassified history and museum/archival documentation.
Analytical lesson	A classic example of exploiting trusted infrastructure as the disguised distributor.

5. Sacred Sword of the Patriots League (Vietnam, 1960s)

Evidence status Documented U.S./South Vietnamese black PSYOP

Field	Assessment
Real sender	CIA origins; later MACV-SOG psychological operations with South Vietnamese participation
Impersonated / disguised sender	An indigenous anti-Communist resistance movement inside North Vietnam
Target audience	North Vietnamese civilians, officials, military personnel, and selected captives
Message	A purported internal resistance existed and opposed Communist rule.
Delivery mechanism	Clandestine radio, letters, leaflets, constructed organizational identity, and supporting legend.
Trust-generating devices	Vietnamese cultural references, organizational symbols, an apparently internal source, repeated multimedia reinforcement.

Field	Assessment
Observed / claimed effects	Some evidence suggests the regime devoted attention to the supposed movement; broad strategic effectiveness remains uncertain.
How exposed	Declassified CIA and military records, later histories.
Analytical lesson	A textbook source-deception architecture: fictitious indigenous sponsor used to give external influence an internal voice.

6. Soviet-bloc AIDS disinformation / Operation Denver (1980s)

Evidence status Documented Soviet-bloc active measure; codename terminology clarified by archives

Field	Assessment
Real sender	KGB with assistance from Stasi and other allied services
Impersonated / disguised sender	Foreign media, purported scientific authority, and apparently independent third-party reporting
Target audience	Global audiences, especially communities predisposed to distrust U.S. institutions
Message	False claim that HIV/AIDS resulted from U.S. biological-weapons experiments, often associated with Fort Detrick.
Delivery mechanism	Planting, repetition, front/third-party channels, purported expertise, international media recirculation.
Trust-generating devices	Scientific-looking claims, foreign publication, third-party citation, exploitation of real histories of medical abuse and distrust.
Observed / claimed effects	The narrative became globally persistent; precise attributable health effects are debated and cannot be assigned solely to the original operation.
How exposed	Cold War counter-disinformation reporting, defectors, and later Eastern European archival documents.
Analytical lesson	Demonstrates source laundering: once repeated by apparently independent outlets, the Soviet origin became less visible.

7. FM 30-31B forgery (1970s-1980s)

Evidence status Widely identified by U.S. authorities and scholars as a Soviet-associated forgery

Field	Assessment
Real sender	Attributed by U.S. government and Cold War scholarship to Soviet active-measures channels
Impersonated / disguised sender	A purported secret U.S. Army field manual supplement
Target audience	Foreign publics and political movements, especially in allied countries
Message	The fake document suggested U.S. forces were instructed to manipulate domestic politics and carry out destabilizing actions.
Delivery mechanism	Forged document circulated through foreign publications and repeated internationally.
Trust-generating devices	Official-looking classification, bureaucratic style, apparent leaked-document status.
Observed / claimed effects	The forgery circulated for years and remained useful as a reference point in anti-U.S. narratives even after exposure.
How exposed	Document authentication analysis and U.S. government counter-disinformation work.
Analytical lesson	Shows how the forged-document format converts institutional authority into a credibility device.

8. Internet Research Agency personas targeting the United States (2014-2018)

Evidence status U.S. criminal indictment and extensive platform evidence; election-outcome effect unproven

Field	Assessment
Real sender	Internet Research Agency and associated Russian actors, as alleged by U.S. prosecutors
Impersonated / disguised sender	Americans, grassroots activists, political pages, and local social-media communities
Target audience	U.S. social-media users and political communities
Message	Polarizing political and social content across multiple ideological identities; advocacy for and against candidates and causes.
Delivery mechanism	Fake personas and pages, social ads, event organization, U.S.-based technical infrastructure, unwitting local participants.
Trust-generating devices	American-style identities, localized language, community themes, apparent peer-to-peer activism.
Observed / claimed effects	Substantial exposure and engagement were documented; DOJ did not allege that the operation changed the election result, and causal estimates remain contested.
How exposed	Platform investigations, intelligence/law-enforcement work, 2018 DOJ indictment.
Analytical lesson	Astroturfing and source deception made foreign state-linked activity appear as domestic political speech.

9. Russian “Doppelganger” network (2022-2024 and after)

Evidence status U.S. DOJ attribution/allegation plus platform and research reporting

Field	Assessment
Real sender	Russian government-directed actors and contracted organizations, according to U.S. court filings
Impersonated / disguised sender	Cloned or look-alike news brands, invented media outlets, and non-Russian social personas
Target audience	U.S. and European audiences
Message	Narratives intended to weaken support for Ukraine, deepen divisions, and influence political attitudes.
Delivery mechanism	Cybersquatted domains resembling major media, fake brands, fake profiles, influencer approaches, social ads, and AI-assisted content.
Trust-generating devices	Visual imitation of known outlets, local-language personas, headlines resembling legitimate news, third-party sharing.
Observed / claimed effects	The network achieved continuing output and required repeated disruption; the size of its persuasive effect remains difficult to establish.
How exposed	September 2024 DOJ domain seizures, affidavits, platform/security research.
Analytical lesson	A modern industrialized form of black propaganda: identity cloning plus network distribution rather than one clandestine transmitter.

10. DRAGONBRIDGE / Spamouflage (PRC-linked, contemporary)

Evidence status Platform attribution to a PRC-linked coordinated influence network

Field	Assessment
Real sender	PRC-linked operators, according to Google and other platform assessments
Impersonated / disguised sender	Local citizens, issue activists, commentators, and other inauthentic personas
Target audience	Global audiences including Taiwan and U.S.-focused political communities
Message	Pro-PRC narratives, attacks on critics, and attempts to engage divisive political and social topics.
Delivery mechanism	High-volume cross-platform accounts, copied material, fake personas, AI-generated imagery, repetitive posting.
Trust-generating devices	Apparent local identities and peer-to-peer participation; attempts to imitate organic community behavior.
Observed / claimed effects	Google reported extremely low authentic engagement across much of the network, showing that scale and activity do not equal influence.
How exposed	Repeated platform takedowns and public threat reports.
Analytical lesson	A strategically important failure mode: cheap identity/content manufacture can create volume without credibility or genuine audience uptake.

6. Psychological Mechanisms Exploited by Black Propaganda

Black propaganda does not require a uniquely “gullible” audience. It exploits normal cognitive shortcuts and social processes that help people operate under uncertainty. These mechanisms increase or decrease susceptibility probabilistically; they are not deterministic laws.

Mechanism	How it can be exploited
Confirmation bias	People more readily notice, accept, and recall material consistent with prior beliefs. Source impersonation is especially effective when the fake source appears to “confirm what insiders already know.”
Authority bias	Official-looking documents, uniforms, expert credentials, institutional logos, or insider titles can substitute for independent verification.
Repetition / illusory truth effect	Repeated statements tend to feel more familiar and therefore more plausible, including misinformation. Repetition can increase belief and sometimes sharing intentions. [18]
Conformity	Individuals may adjust judgments toward perceived group consensus, particularly under ambiguity or social pressure.
Social proof	Visible likes, reposts, endorsements, comments, or apparent peer agreement can signal that a claim is accepted by others even when engagement is manufactured.
In-group / out-group bias	Messages attributed to an in-group source can receive a credibility premium; messages portraying an out-group as threatening can intensify hostility.
Fear	Threat narrows attention, raises demand for protective action, and can reduce tolerance for ambiguity.
Anger and hatred	High-arousal moral and identity emotions increase willingness to share and punish; morally emotional language has been associated with greater diffusion in social networks. [17]
Moral shock	Graphic or identity-threatening events can trigger rapid mobilization before verification catches up.
Identity politics	People process claims through group identity, status, belonging, and perceived group threat, not only through factual evaluation.
Conspiratorial thinking	Source secrecy and ambiguous evidence can be reframed as proof that powerful actors are hiding the truth; failed predictions may be absorbed into larger conspiratorial narratives.
Uncertainty reduction	Rumors provide causal stories and actionable explanations when official information is scarce, delayed, or contradictory.
Information overload	When people cannot evaluate all available information, they rely more heavily on cues such as familiarity, source identity, social endorsement, or emotion.
Emotional contagion	Emotion expressed by peers and influencers can propagate through networks and change the perceived emotional climate around an issue.
Rumor diffusion	Unverified claims can mutate as they pass through communities, creating distance from the original source and making provenance reconstruction harder.
Hostile media effect	Strong partisans can perceive neutral or mixed reporting as biased against their side, making “independent” fact-checks less persuasive and opening space for alternative pseudo-media.
Motivated reasoning	People can apply more skepticism to identity-threatening evidence than to identity-confirming evidence.
Availability and vividness	Dramatic images, alleged leaks, audio, and personal anecdotes can dominate statistical or contextual evidence because they are cognitively vivid.
Source-memory failure	People may later remember a claim but forget where it came from, allowing a debunked or dubious source to lose its warning label over time.
Pluralistic ignorance	Artificially visible “consensus” can make individuals believe their private doubts are minority views, changing willingness to speak or act.

Source note: Repetition review: *Current Opinion in Psychology* (2024). Moral-emotional diffusion: Brady et al., *PNAS* (2017). False-news diffusion: Vosoughi, Roy & Aral, *Science* (2018).

6.1 Social conditions that increase vulnerability

Condition	Why it matters
Political polarization	Competing groups already possess incompatible trust networks and are prepared to accept damaging claims about opponents.
War, terrorism, or security crisis	Speed, fear, censorship, secrecy, and limited independent access create gaps that rumor and deception can fill.
Economic crisis	Loss, uncertainty, status threat, and demand for blame increase receptivity to simple causal narratives.
Low trust in government and media	Corrective institutions lack credibility, making alternative or pseudo-independent sources more attractive.
Social conflict	Ethnic, racial, religious, class, regional, or ideological antagonism provides pre-existing narratives to activate.
Censorship / information scarcity	Audiences cannot easily verify claims and may value clandestine sources precisely because official channels are controlled.
Collapse or fragmentation of media ecosystems	Local-news decline and fragmented audiences weaken shared verification and common factual reference points.
Algorithmic recommendation	Engagement-optimized systems can repeatedly expose users to high-arousal narratives, though effects depend on platform design and user behavior.
Echo chambers and selective networks	Homophilous networks can concentrate repeated claims and reduce cross-cutting correction.
Influencer networks	Trust can be transferred from a covert source to a familiar personality whose audience does not see the original provenance.
Information overload	Verification becomes costly; audiences use shortcuts.
Weak provenance norms	Screenshots, reuploads, clipped videos, and reposted documents circulate without reliable metadata or source history.



Figure 2. Generated conceptual illustration of conditions that can facilitate black propaganda. These are risk factors, not proof that a specific audience will be persuaded.

7. Source Laundering and the Digital Influence Ecosystem

7.1 Source laundering: what defenders should reconstruct

Source laundering occurs when the connection between content and its real origin becomes progressively obscured as material passes through intermediaries. The defensive problem is to reconstruct that chain without assuming that every intermediary is knowingly involved. Journalists, activists, influencers, or ordinary users can retransmit material in good faith after the original deception has already taken place.

- Anonymous or pseudonymous account: hides the initial sponsor or operational persona.
- Disguised news outlet: imitates independent journalism or a known brand while concealing sponsorship.
- Front organization: gives the material a durable institutional identity and an apparently independent reason to exist.
- Fake expert or fabricated credential: adds authority without verifiable professional history.
- Third-party organization or cutout: creates organizational distance between sponsor and message.
- Influencer or community account: transfers existing audience trust to the narrative.
- Bots, fake accounts, and Sybil networks: create artificial repetition, engagement, or apparent consensus.
- Leaked or forged document: shifts attention from "who says this?" to "what does the document appear to prove?"
- Memes, screenshots, and clipped media: remove context and provenance while preserving emotionally salient fragments.
- Translation and localization: can further obscure the original wording, source, and timestamp.
- Repeated retransmission: makes a claim appear independently corroborated when multiple outlets ultimately trace to one origin.
- Traditional-media recitation: once a story is covered as "something people are saying," the operation may gain a new layer of legitimacy even if the report is skeptical.

7.2 Contemporary digital architecture

A contemporary influence chain can be conceptualized as: social platforms → recommendation and search systems → fake or coordinated accounts → synthetic personas → AI-generated text/images/audio/video → edited or deepfake media → audience targeting → influencers and community brokers → repeated user sharing → recitation by larger media. This is not a deterministic pipeline and not every stage is present in every operation. The key analytical question is where provenance is lost and where apparent independence is manufactured.

Component	Defensive significance
Social media	Low-cost publication and access to targeted communities; also creates public traces useful for forensic reconstruction.
Algorithmic recommendation	Can amplify engaging or controversial material; exact causal effects vary by platform and are often difficult to observe externally.
Bots / Sybil networks	Can manufacture activity, test messages, or simulate popularity; crude networks are often detectable through behavior and coordination.
Fake personas	Provide durable social identities that can join groups, build followings, contact journalists, or pose as locals.
AI-generated text	Raises throughput, multilingual fluency, persona consistency, and variation; does not by itself create trust or reach.
AI images/audio/video	Lower the cost of producing synthetic evidence and identity assets; provenance and forensic authentication become more important.
Deepfakes	Can impersonate public figures or apparent witnesses; impact depends on timing, believability, distribution, and speed of authentication.
Microtargeting	Allows different messages to reach different audiences; limits public visibility and can complicate collective verification.
Influencers	Function as trust relays; they may be knowing participants, paid but unaware of ultimate sponsorship, or fully unwitting.
Online communities	Supply language, grievances, memes, and social validation; covert operators can exploit existing narratives rather than invent new ones.
Traditional-media recitation	Can transform a fringe narrative into a national agenda item, even when coverage is corrective; headline repetition can outlive caveats.

7.3 Why manipulated narratives can look like spontaneous public opinion

The appearance of spontaneity emerges when multiple visible actors seem independent even though their first-order inputs are coordinated. A cluster of personas posts related themes; real users react; influencers reframe the claims; news outlets report the online controversy; and later participants encounter only the downstream discussion. At that point the narrative has acquired real social participation even though the initial spark was inauthentic. This is why attribution analysis must distinguish the origin of a narrative from the later agency of authentic users who adopt it for their own reasons.

7.4 AI does not solve the credibility problem

OpenAI's 2024 investigations of covert influence operations found actors using AI for comments, articles, fake names and bios, translation, proofreading, research, and debugging. The disrupted networks generally failed to achieve significant audience growth. Google similarly reported that much of the PRC-linked DRAGONBRIDGE network attracted little or no authentic engagement. These findings caution against assuming that cheap synthetic content automatically produces mass persuasion. [12][13]

8. Black Propaganda and False Flags



Figure 3. Generated conceptual illustration contrasting false attribution in communication with military false flags and showing democratic/market contexts.

8.1 The relationship

Both black propaganda and false-flag operations involve attribution deception, but they operate in different domains. In black propaganda, the primary deceptive object is the origin of a communication: a broadcast, document, account, website, organization, leak, or persona is made to appear as though it belongs to someone else. In a physical false flag, an action is staged or conducted so that responsibility appears to lie with another actor. The two can be combined, as in a staged incident accompanied by communications designed to reinforce the false attribution.

8.2 Military false flags vs. false attribution in communication

Dimension	Military / physical false flag	Black / false-attribution communication
Primary object	Physical action, attack, presence, equipment, or operational identity	Message, source, publication identity, persona, organization, or provenance
Typical aim	Misattribute responsibility for an act; enable surprise, pretext, confusion, or intelligence purpose	Borrow credibility, discredit an adversary, conceal sponsorship, manufacture grassroots appearance
International-law relevance	Specific rules can govern enemy flags, uniforms, insignia, protected emblems, perfidy, and conduct during attacks	Propaganda/deception is not per se prohibited by IHL; legality depends on method, target, accompanying conduct, and other applicable law
Example	Gleiwitz staged border incident	British black radio posing as German; fake American personas; cloned news sites
Analytical warning	Not every disputed attack is a false flag	Not every anonymous or false claim is black propaganda

Source note: ICRC Customary IHL Rule 62 on improper use of enemy flags, military emblems, insignia, or uniforms.

9. Democracy, Elections, Corporate Reputation, and Financial Markets

9.1 Democratic and election effects

Black propaganda can be strategically attractive in democracies because political legitimacy depends on trust in authentic speakers, elections, media, and institutions. The goal need not be to persuade voters to support one candidate. It may be enough to increase uncertainty, reduce turnout among selected groups, intensify intergroup hostility, make compromise reputationally costly, or convince citizens that all political information is manipulated.

- Candidate reputation attacks: fabricated or falsely attributed statements can create scandals, force defensive coverage, and impose verification costs.
- Voter suppression and discouragement: false information about eligibility, procedures, polling, threats, or the futility of participation can reduce participation. Defensive agencies therefore treat election-process misinformation separately from ordinary political persuasion.
- Amplification of intergroup distrust: fake in-group accounts can provoke another group or post extreme material that makes a community appear more hostile than it is.
- Erosion of electoral legitimacy: repeated narratives alleging pervasive fraud or conspiracy can reduce acceptance of outcomes even without changing votes.
- Political cynicism: audiences may conclude that all actors lie, all media are propaganda, and verification is impossible - a strategically useful form of paralysis.
- Declining institutional trust: exposure to genuine covert operations can paradoxically make exaggerated claims about ubiquitous hidden control seem more plausible.

9.2 U.S. election context and foreign influence

U.S. federal law prohibits foreign nationals from making contributions, donations, expenditures, independent expenditures, and specified disbursements in connection with federal, state, or local elections, and also restricts foreign-national participation in election-related decision-making. The Foreign Agents Registration Act is principally a disclosure regime: it requires covered agents of foreign principals to register and label informational materials, while expressly not regulating the content of speech itself. In 2026, NCSL reported that 31 states had enacted laws regulating political deepfakes, mostly through disclosure requirements, while constitutional litigation continues over the boundaries of political-speech regulation. [19][20][21]

9.3 Corporate and financial-market analogues

Corporate black propaganda resembles political black propaganda when an actor conceals sponsorship or impersonates a competitor, analyst, customer, regulator, whistleblower, activist group, or independent news source in order to harm reputation or alter stakeholder behavior. The strategic target is often confidence: consumer trust, employee morale, lender perceptions, investor expectations, acquisition negotiations, or regulatory attention.

Pattern	Comparison with political black propaganda
Corporate reputation attack	A disguised campaign spreads damaging claims about a firm while concealing the sponsor. It resembles political black propaganda in its source deception; legal exposure may include defamation, unfair competition, fraud, or tort claims depending on facts.
Competitor impersonation	Communications appear to come from a rival company or executive. The central issue is identity/source falsification, with additional trademark, impersonation, computer-fraud, or commercial-law concerns possible.
False market rumor	A false claim about earnings, financing, merger activity, product failure, regulatory action, or insolvency can move prices if believed. This is disinformation; it becomes black-propaganda-like when the origin is also disguised.
Pump-and-dump / short-and-distort type conduct	Where deceptive statements are intentionally used in connection with trading or a scheme to defraud, securities-fraud and market-manipulation rules can apply. This report does not provide operational instructions.
Fake expert / analyst persona	An actor poses as an independent professional to create apparent third-party validation; source verification and conflicts-of-interest analysis become critical.
Compromised official account	A false statement issued through a hacked or impersonated trusted account can cause immediate market reaction because source authenticity initially appears strong.

Source note: SEC/Investor.gov warns that social media can spread false or misleading stock information and that fraudsters can conceal identities or impersonate credible sources. SEC enforcement actions illustrate that speech integrated into a fraudulent trading scheme can create securities-law liability. [26][27]

10. U.S. Law, Platform Policies, International Law, and the Law of Armed Conflict

Black propaganda is a descriptive category, not a single legal cause of action or crime. Legal analysis turns on the underlying conduct: defamation, fraud, impersonation, hacking, foreign-agent activity, election expenditures, threats, conspiracy, securities manipulation, unauthorized access, or violations of wartime rules. The First Amendment also sharply limits government power to prohibit speech merely because it is false.

10.1 Defamation

Defamation law addresses false statements of fact that injure reputation, subject to constitutional protections and state-law elements. Under *New York Times Co. v. Sullivan*, a public official seeking damages for defamatory falsehood relating to official conduct must prove “actual malice” - knowledge of falsity or reckless disregard for truth. Public figures are also subject to demanding constitutional standards in many contexts. Anonymous or foreign-backed propaganda is not automatically defamatory; the plaintiff must satisfy the relevant substantive and constitutional rules. [22]

10.2 False speech and the First Amendment

United States v. Alvarez rejected the idea that all false statements fall outside First Amendment protection. The Supreme Court emphasized that historically unprotected categories involve additional legally cognizable harms or contexts, such as fraud, defamation, perjury, threats, or speech integral to criminal conduct. This matters because a general government ban on “lies” or “propaganda” would raise major constitutional problems. [23]

10.3 Fraud

Fraud law does not criminalize deception in the abstract. Federal wire fraud, for example, requires a scheme or artifice to defraud or to obtain money or property by false or fraudulent pretenses and use of interstate or foreign wire communications for execution of the scheme. Political falsehood without the required fraudulent scheme is not automatically wire fraud. [24]

10.4 Election law and foreign nationals

Federal election law prohibits specified foreign-national contributions, expenditures, independent expenditures, and electioneering-related disbursements, as well as foreign-national participation in election-related decision-making. Application to a particular influence operation can be fact-intensive: it depends on who acted, what was spent or provided, whether conduct was “in connection with” an election, and whether other criminal or registration statutes apply. [20]

10.5 FARA and source disclosure

FARA is unusually relevant to black-propaganda analysis because its central policy rationale is provenance transparency. DOJ states that FARA seeks to ensure that government and the public know the source of certain information from foreign agents intended to influence U.S. public opinion, policy, and laws. Covered agents must register and label informational materials, subject to statutory exemptions. FARA does not itself prohibit the content of informational materials. [19]

10.6 State political-deepfake laws

States have moved faster than the federal government in regulating synthetic political media. NCSL reported in June 2026 that 31 states had enacted laws regulating deepfakes in political messaging, typically through disclosure requirements and, in a smaller number of states, prohibitions. Constitutional scrutiny is significant because political speech lies at the core of First Amendment protection. [21]

10.7 Platform policies

Major platforms generally regulate coordinated inauthentic behavior, impersonation, spam, fake engagement, and deceptive identity through private terms of service. Meta’s coordinated-inauthentic-behavior framework focuses on groups of accounts or pages that work together to mislead users about who they are or what they are doing, emphasizing behavior rather than viewpoint. X and YouTube likewise restrict inauthentic identities, platform manipulation, impersonation, and deceptive engagement. These private policies are distinct from constitutional limits on government censorship.

10.8 National security law

Foreign influence can implicate counterintelligence authorities, sanctions, computer-crime laws, conspiracy statutes, export controls, or laws concerning agents of foreign governments. U.S. law-enforcement responses to the IRA and Doppelganger networks illustrate a mix of indictments, asset/domain seizures, and public attribution. Those cases are specific legal actions, not a general license to treat controversial speech as a national-security operation.

10.9 International law and law of armed conflict

Propaganda and deception are not categorically prohibited in armed conflict. Ruses of war have a long lawful history, but specific forms of perfidy and misuse of protected status or enemy emblems can be unlawful. The ICRC’s customary-law formulation states that improper use of adversary flags, military emblems, insignia, or uniforms is prohibited, with Additional Protocol I specifically restricting such use while engaging in attacks or to shield, favor, protect, or impede military operations.

Communications source deception must therefore be analyzed separately from the law governing physical use of enemy military identity. [25]

Outside the law of armed conflict, international law does not contain a simple general rule that makes foreign propaganda unlawful. State-sponsored covert influence may raise questions of sovereignty, prohibited intervention, diplomatic law, human rights, or domestic jurisdiction. The non-intervention principle is most clearly implicated where conduct becomes coercive in matters reserved to a state, while the legal status of non-coercive propaganda, espionage, and influence remains more contested. Attribution, state responsibility, territorial effects, and the specific method therefore matter more than the label “black propaganda” alone.

10.10 The core legal tension

Democratic dilemma Open societies must protect themselves against covert foreign manipulation, fraud, impersonation, and unlawful interference without turning “propaganda” into a label for suppressing lawful dissent, satire, partisan advocacy, anonymous speech, or unpopular views. Provenance transparency and conduct-based rules are often easier to reconcile with free expression than broad truth-policing regimes.

11. Detection and Defensive Analysis Framework

11.1 The provenance-first checklist

1. Who is the original source - not merely the account or outlet from which I personally encountered the material?
2. Can the claimed source be independently verified through an official site, known contact channel, verified archive, or corroborated publication history?
3. Is the sender's identity authentic? Does the account's history, domain registration, biography, profile image, language, time zone, and prior behavior cohere?
4. What is the earliest known posting time? Are there earlier versions in another language, platform, image, document, or domain?
5. What is the diffusion path? Which accounts, outlets, or groups were early amplifiers, and which later sources merely copied them?
6. Are multiple accounts repeating unusually identical text, timing, links, images, hashtags, or narrative sequences?
7. Does the material depend heavily on emotional provocation - fear, humiliation, outrage, betrayal, disgust - before supplying verifiable evidence?
8. Does it appeal more strongly to identity, anger, or fear than to checkable facts?
9. Do independent information sources confirm the claim, and are those sources actually independent of one another?
10. Can images, video, audio, and documents be authenticated through metadata, reverse-search, geolocation, chronology, file analysis, provenance credentials, or comparison to originals?
11. Does the source possess the access it claims to possess? Are jargon, organizational procedures, seals, fonts, signatures, document numbers, and bureaucratic details authentic?
12. Who stands to gain strategically if the target believes the claim or merely becomes confused by it?
13. Is there evidence of source laundering - anonymous origin → pseudo-news → influencer → larger media → repeated citation?
14. Is apparent grassroots activity consistent with genuine community behavior, or is there evidence of coordinated inauthentic behavior?
15. What evidence would falsify the attribution hypothesis? An analysis that cannot be disproved is not a forensic conclusion.

11.2 A four-layer analytic workflow

Layer	Questions	Typical evidence
A. Content	Is the claim accurate, manipulated, selective, or unsupported?	Primary documents, data, eyewitness corroboration, domain expertise, fact-checking
B. Source	Is the claimed sender authentic?	Account history, signatures, contact verification, organizational records, technical metadata
C. Network	How did it spread and who coordinated?	Timestamps, repost graphs, identical text, URL infrastructure, account creation patterns, bot/Sybil indicators
D. Strategy	What objective and beneficiary best fit the evidence?	Target selection, recurring narratives, timing, resource patterns, known doctrine - with explicit alternative hypotheses

11.3 Indicators of possible source laundering

- Earliest version appears on an obscure outlet and later versions cite one another circularly.
- An alleged expert has no independently verifiable publication, employment, credential, or institutional history.
- Multiple websites share analytics IDs, hosting patterns, templates, contact details, or unusual errors despite presenting as independent.
- Accounts created in bursts suddenly focus on one geopolitical narrative or use highly synchronized posting.
- Large numbers of accounts use the same unusual phrasing, translation artifacts, images, or link-shortening pattern.
- A supposed local persona posts continuously across incompatible time zones or demonstrates cultural/linguistic inconsistencies.
- Documents circulate only as screenshots or low-resolution scans that prevent metadata and structural inspection.
- A "leak" is distributed by a persona whose claimed organizational access cannot be established.
- Corrections address the factual claim but the origin story changes repeatedly, suggesting attribution is being adapted after exposure.

11.4 Media-forensics cautions

Deepfake detection is only one part of provenance analysis. Authentic media can be miscaptioned, genuine video can be edited selectively, old footage can be relabeled, a real document can be leaked by a falsely attributed persona, and an AI-generated image can be clearly labeled satire rather than deception. Analysts should ask both "Is the media synthetic?" and "Is the claimed context and source authentic?"

11.5 Defensive principles

- Publish provenance, not just verdicts: explain where the material first appeared and how attribution was established.
- Distinguish confidence levels: "likely," "high confidence," "officially alleged," and "proven in court" are not interchangeable.
- Correct without unnecessarily amplifying: reproduce only the minimum false content needed to explain the correction.
- Pre-bunk recurring techniques: teach audiences how cloned domains, impersonated personas, and false leaks work before a crisis.

- Build trusted rapid-authentication channels for campaigns, agencies, companies, and newsrooms.
- Preserve evidence before takedown: timestamps, headers, domains, archives, and network relationships matter for later attribution.
- Avoid partisan asymmetry: apply the same provenance standard regardless of whether a claim favors one's political preferences.

12. Common Analytical Errors

Error	Why it is analytically dangerous
Equating “a claim I dislike” with propaganda	Propaganda is an analytical category involving purposeful influence; disagreement or bias alone is insufficient.
Assuming all anonymous information is an intelligence operation	Anonymous speech has many legitimate and illegitimate sources. Attribution requires evidence of sponsorship or coordination.
Confusing falsity with source manipulation	A false claim is not automatically black propaganda; black propaganda requires deliberate false attribution.
Assuming factual truth excludes propaganda	True material can be selectively framed for propaganda and can be black if source attribution is false.
Treating official attribution as judicial proof	Intelligence assessments, indictments, and sanctions have different evidentiary and procedural statuses from court findings after trial.
Measuring success by impressions alone	Exposure, engagement, belief change, behavior change, policy effect, and strategic outcome are different dependent variables.
Ignoring domestic adoption	A foreign-seeded narrative may later be amplified for independent domestic reasons; downstream users are not automatically controlled by the original sponsor.
Over-attributing to bots	Real humans frequently dominate diffusion once a narrative resonates; bot activity should be measured rather than assumed.
Forgetting base rates	Large platforms contain enormous amounts of organic spam, satire, trolling, activism, marketing, and misinformation. Suspicious behavior must be compared with normal behavior.
Confirmation bias by investigators	Analysts can selectively interpret ambiguous evidence to fit a preferred adversary attribution. Competing hypotheses and disconfirming evidence should be recorded.
Overconfidence in AI detectors	Synthetic-media detectors can fail across models, compression levels, and editing. Provenance, context, and source validation should complement forensic classifiers.
Ignoring second-order effects of exposure	Public attribution can deter an operator but can also amplify the narrative or cause audiences to overgeneralize that all dissent is foreign manipulation.

13. Core Concepts, Scholars, and Authoritative Sources

13.1 Twenty core concepts of black propaganda

Concept	Definition
1. Source deception	Deliberate falsification of who originated or sponsors a message.
2. False attribution	Assigning a communication to an adversary or third party that did not create it.
3. Identity impersonation	Manufacturing a person, organization, outlet, or institutional identity.
4. Attribution ambiguity	Creating uncertainty about origin even when no single false source is asserted.
5. Content-source decoupling	Analyzing factual truth separately from provenance authenticity.
6. Credibility borrowing	Using the impersonated source's reputation, access, or identity as a persuasion asset.
7. Credibility sabotage	Publishing damaging material in another source's name to reduce trust in the real source.
8. Plausible deniability	Maintaining distance between sponsor and operation until attribution is established.
9. Source laundering	Passing content through intermediaries that obscure original provenance.
10. Narrative laundering	Transforming a suspicious claim into apparently ordinary discourse through repetition and recontextualization.
11. Front organization	An apparently independent institution that conceals sponsorship or control.
12. Astroturfing	Manufacturing the appearance of grassroots public opinion or activism.
13. Cutout / intermediary	A person or organization that creates separation between sponsor and operational activity.
14. Black radio / pseudo-media	Media designed to appear as an adversary or indigenous independent outlet.
15. Forgery	Fabricated document or artifact designed to borrow institutional authenticity.
16. Hack-and-leak persona	A disguised identity used to publish or frame stolen material; authentic documents can still be part of source deception.
17. Coordinated inauthentic behavior	Networked activity that misleads users about who is acting or how independent the actors are.
18. Synthetic persona	AI-assisted or fabricated identity with generated biography, text, image, audio, or behavioral history.
19. Provenance forensics	Methods for reconstructing source, chronology, chain of custody, and diffusion.
20. Trust manipulation	The strategic alteration of whom an audience believes, distrusts, or treats as authentically representative.

13.2 Ten major scholars / theorists

Scholar	Contribution
Harold D. Lasswell	Pioneer of systematic propaganda analysis; studied symbols, mass communication, and wartime persuasion.
Jacques Ellul	Analyzed propaganda as a social and technological system embedded in modern mass society, not merely isolated lies.
Garth S. Jowett	Co-author of a leading comprehensive framework for propaganda and persuasion, emphasizing deliberate systematic influence.
Victoria O'Donnell	Co-author with Jowett; developed historical and analytical approaches to propaganda processes and audience effects.
Philip M. Taylor	Historian of propaganda and psychological warfare; emphasized communications as an instrument of conflict and statecraft.
Paul M. A. Linebarger	Early theorist and practitioner of psychological warfare; influential in conceptualizing propaganda classes and operational psychology.

Scholar	Contribution
Ladislav Bittman	Former Czechoslovak intelligence officer and scholar who documented Soviet-bloc disinformation and active measures.
Thomas Rid	Historian of active measures who traces twentieth-century covert political warfare into the digital era.
Claire Wardle	Key scholar/practitioner on information disorder, misinformation/disinformation/malinformation, and verification.
Nicholas J. Cull	Historian of public diplomacy, propaganda, international broadcasting, and the information dimensions of statecraft.

13.3 Twenty authoritative academic books, reports, and government sources

#	Source	Why it matters
1	Harold D. Lasswell, <i>Propaganda Technique in the World War</i> (1927).	Foundational study of organized wartime propaganda and symbols.
2	Jacques Ellul, <i>Propaganda: The Formation of Men's Attitudes</i> (1965 English ed.).	Classic sociological theory of propaganda systems and modern mass society.
3	Garth S. Jowett & Victoria O'Donnell, <i>Propaganda & Persuasion</i> , 7th ed. (SAGE, 2018).	Leading academic framework for definition, process, history, and analysis.
4	Philip M. Taylor, <i>Munitions of the Mind: A History of Propaganda</i> (Manchester University Press).	Broad history of propaganda and psychological warfare.
5	Paul M. A. Linebarger, <i>Psychological Warfare</i> (multiple editions).	Classic psychological-warfare theory and source-classification discussion.
6	Frank L. Goldstein & Benjamin F. Findley Jr., eds., <i>Psychological Operations: Principles and Case Studies</i> (Air University Press, 1996).	Official professional text; explicitly distinguishes white, grey, and black by source. https://www.airuniversity.af.edu/AUPress/Display/Article/4416268/psychological-operations-principles-and-case-studies/
7	Claire Wardle & Hossein Derakhshan, <i>Information Disorder</i> (Council of Europe, 2017).	Seminal mis/dis/mal-information taxonomy. https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html
8	Thomas Rid, <i>Active Measures: The Secret History of Disinformation and Political Warfare</i> (Farrar, Straus and Giroux, 2020).	Comprehensive historical treatment of covert political warfare and disinformation.
9	Richard H. Shultz & Roy Godson, <i>Dezinformatsia: Active Measures in Soviet Strategy</i> (1984).	Cold War analysis of Soviet disinformation and active measures.
10	Ladislav Bittman, <i>The KGB and Soviet Disinformation</i> (Pergamon-Brassey's, 1985).	Insider/scholarly account of Soviet-bloc disinformation practice.
11	Richard H. Shultz Jr., <i>The Secret War Against Hanoi</i> (HarperCollins, 1999).	Detailed history of U.S. covert action and black PSYOP in North Vietnam.
12	Thomas Boghardt, "Soviet Bloc Intelligence and Its AIDS Disinformation Campaign," <i>Studies in Intelligence</i> 53(4) (CIA, 2009).	Historical study of Soviet AIDS disinformation. https://www.cia.gov/resources/csi/studies-in-intelligence/volume-53-no-4/soviet-bloc-intelligence-and-its-aids-disinformation-campaign/
13	UK National Archives, <i>Political Warfare Executive records</i> (FO 898).	Primary archival record set for British wartime political warfare and black propaganda. https://www.nationalarchives.gov.uk/
14	National WWII Museum, "Operation Cornflakes."	Historical account of OSS forged-mail operation. https://www.nationalww2museum.org/war/articles/operation-cornflakes
15	U.S. Department of Justice, <i>Internet Research Agency indictment</i> (Feb. 16, 2018).	Primary legal allegation describing fake U.S. personas, organizations, and social-media influence. https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere
16	U.S. Department of Justice, "Doppelganger" domain seizure announcement and affidavits (Sept. 4, 2024).	Primary U.S. attribution/allegation concerning cloned news sites, fake personas, and Russian-directed influence. https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

#	Source	Why it matters
17	Google Threat Analysis Group, "DRAGONBRIDGE" / Spamouflage update (June 26, 2024).	Platform evidence on PRC-linked coordinated influence, AI use, and low authentic engagement. https://blog.google/threat-analysis-group/google-disrupted-dragonbridge-activity-q1-2024/
18	OpenAI, "Disrupting deceptive uses of AI by covert influence operations" (May 30, 2024).	Primary platform report on how influence actors used generative AI and their limited observed reach. https://openai.com/index/disrupting-deceptive-uses-of-ai-by-covert-influence-operations/
19	NATO, "Information threats" policy materials (2024-2025).	Official framework emphasizing manipulative, coordinated information activities and broader "information threats." https://www.nato.int/
20	Council of Europe / UNESCO journalism and verification resources, including Journalism, "Fake News" & Disinformation (2018).	Practical source verification, information-disorder, and journalistic defense frameworks. https://unesdoc.unesco.org/

13.4 Additional legal and policy primary materials

Material	URL
DOJ FARA FAQ (updated 2026)	https://www.justice.gov/nsd-fara/frequently-asked-questions
Federal Election Commission - Foreign nationals	https://www.fec.gov/help-candidates-and-committees/foreign-nationals/
NCSL - Artificial Intelligence in Elections and Campaigns (June 23, 2026)	https://www.ncsl.org/elections-and-campaigns/artificial-intelligence-ai-in-elections-and-campaigns
New York Times Co. v. Sullivan, 376 U.S. 254 (1964)	https://www.law.cornell.edu/supremecourt/text/376/254
United States v. Alvarez, 567 U.S. 709 (2012)	https://www.law.cornell.edu/supremecourt/text/11-210
18 U.S.C. § 1343 - Wire fraud	https://www.law.cornell.edu/uscode/text/18/1343
ICRC Customary IHL Rule 62 - Improper use of enemy flags/insignia/uniforms	https://ihl-databases.icrc.org/en/customary-ihl/v1/rule62
SEC / Investor.gov - Social Media and Investing: Stock Rumors	https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/alerts-bulletins/updated-1

14. Comparative Tables and the Future of AI-Enabled Black Propaganda

14.1 White vs. grey vs. black propaganda - consolidated comparison

Dimension	White	Grey	Black
Claimed source	Real source	No clear source / uncertain	False source
Real sponsor	Disclosed	May be hidden	Hidden and replaced by fabricated attribution
Content truth status	Often accurate/selective; can still mislead	Variable	Variable - true, selective, misleading, or false
Primary deception	Framing and persuasion rather than identity	Ambiguity / omission	Impersonation / source falsification
Credibility strategy	Sponsor's own reputation	Plausible neutrality / deniability	Borrowed or sabotaged credibility of another identity
Exposure risk	Low attribution risk	Moderate	High: exposure can collapse message credibility and damage sponsor
Typical media	Official statements, overt broadcasts, labeled ads	Anonymous leaflets, unattributed rumors, unclear organizations	Pseudo-enemy radio, forged documents, fake outlets/personas, front identities, cloned sites
Forensic priority	Check evidence and framing	Establish provenance	Prove the gap between apparent and real source

14.2 Disinformation vs. black propaganda - consolidated comparison

Question	Disinformation	Black propaganda
What is manipulated?	Information content / factual representation	Attribution, identity, provenance, and trust
Must content be false?	Yes or materially misleading by most standard definitions	No
Must the source be false?	No	Yes, in strict source-based usage
Can it be overt?	Yes	No, while it remains black
Can it use authentic documents?	Yes, if combined with deceptive framing; pure authentic disclosure may be malinformation instead	Yes - authentic documents can be released through a false persona or false provenance
Primary verification method	Fact verification and context	Identity and provenance verification plus content verification
Characteristic harm	False belief about events/facts	False belief about who is speaking, what group believes, or who is responsible
Strongest overlap	False narrative openly issued by a state = disinfo only	Fabricated message issued through a fake enemy/grassroots identity = both

14.3 Traditional black propaganda vs. AI/social-media-era black propaganda

Dimension	Traditional model	AI / social-media model
Identity production	Human-created aliases, forged stationery, clandestine organizations, radio voices	Large numbers of synthetic personas, generated biographies, AI profile images, cloned voices and video
Content production	Slow, specialist, language-intensive	Rapid multilingual rewriting, personalization, automated variation, synthetic media
Distribution	Leaflets, radio, print, mail, controlled front media	Platforms, messaging apps, influencers, recommendation systems, targeted communities, cross-platform reposting
Scale	Limited by printing, transmitters, personnel, logistics	Potentially very high output at low marginal cost
Credibility bottleneck	Access to believable medium and cultural fluency	Trusted accounts, community acceptance, influencer relay, platform reach remain bottlenecks
Feedback	Slow intelligence and audience reporting	Near-real-time engagement metrics and rapid adaptation

Dimension	Traditional model	AI / social-media model
Forgery	Physical document craftsmanship	Digital document alteration, synthetic imagery, voice, video, metadata manipulation
Source laundering	Front newspapers, foreign outlets, cutouts	Anonymous accounts → pseudo-news → influencers → communities → mainstream recitation
Detection	Paper/printing analysis, signals intelligence, human-source investigation	Graph analysis, infrastructure links, account behavior, provenance standards, AI/media forensics, cross-platform chronology
Failure mode	Broadcast discovered as enemy station or forgery exposed	High-volume spam with low authentic engagement; persona inconsistencies; rapid platform takedown
Strategic risk	Sponsor exposure and diplomatic backlash	Same, plus scalable forensic footprints and persistent archives
Key continuity	Trust, identity, narrative resonance, and social conflict remain decisive	Technology changes production economics more than the underlying psychology

14.4 Detection checklist - print-ready summary

Check	Question
1	Who is the original source - not merely the account or outlet from which I personally encountered the material?
2	Can the claimed source be independently verified through an official site, known contact channel, verified archive, or corroborated publication history?
3	Is the sender's identity authentic? Does the account's history, domain registration, biography, profile image, language, time zone, and prior behavior cohere?
4	What is the earliest known posting time? Are there earlier versions in another language, platform, image, document, or domain?
5	What is the diffusion path? Which accounts, outlets, or groups were early amplifiers, and which later sources merely copied them?
6	Are multiple accounts repeating unusually identical text, timing, links, images, hashtags, or narrative sequences?
7	Does the material depend heavily on emotional provocation - fear, humiliation, outrage, betrayal, disgust - before supplying verifiable evidence?
8	Does it appeal more strongly to identity, anger, or fear than to checkable facts?
9	Do independent information sources confirm the claim, and are those sources actually independent of one another?
10	Can images, video, audio, and documents be authenticated through metadata, reverse-search, geolocation, chronology, file analysis, provenance credentials, or comparison to originals?
11	Does the source possess the access it claims to possess? Are jargon, organizational procedures, seals, fonts, signatures, document numbers, and bureaucratic details authentic?
12	Who stands to gain strategically if the target believes the claim or merely becomes confused by it?
13	Is there evidence of source laundering - anonymous origin → pseudo-news → influencer → larger media → repeated citation?
14	Is apparent grassroots activity consistent with genuine community behavior, or is there evidence of coordinated inauthentic behavior?
15	What evidence would falsify the attribution hypothesis? An analysis that cannot be disproved is not a forensic conclusion.

14.5 How AI and generative media may transform black propaganda

Future shift	Assessment
Identity abundance	Synthetic identities will become cheaper to create and maintain across languages, images, voices, and posting histories. Defenders will need to verify social history and provenance, not just visual realism.
Hyper-localization	Models can rapidly translate and adapt narratives to local slang, grievances, legal contexts, and cultural references, increasing the plausibility of “local” personas.
Synthetic evidence	Audio, video, images, documents, transcripts, and screenshots can be generated in mutually reinforcing sets, making single-item debunking insufficient.
Real-time adaptation	Operators can use public response data to reformulate narratives quickly. The defensive counterpart is faster cross-platform monitoring and source authentication.
Persona persistence	Agentic systems could maintain long-running synthetic identities with more consistent interaction histories, though platform defenses may also become more automated.
Influencer laundering	The strategically valuable step may be less the generation of fake content than getting authentic trusted humans to repeat it without seeing the sponsor.
Provenance arms race	Cryptographic content credentials, signed official media, secure account authentication, and chain-of-custody systems will become more valuable - while adversaries will attack the trust placed in those systems.
The “liar’s dividend”	As synthetic media becomes common, genuine recordings can be dismissed as AI-generated. Black propaganda may therefore create uncertainty without producing a convincing forgery at all.
Detection asymmetry	Generation can be cheap and abundant while high-confidence attribution remains expensive, multidisciplinary, and time-consuming.
Narrative flooding	AI enables a high volume of mutually inconsistent narratives whose goal is confusion rather than belief in one version. Yet excessive volume can also trigger platform defenses and audience fatigue.
Automated verification	AI will also strengthen defense: entity resolution, cross-language similarity detection, image provenance, network anomaly detection, and rapid comparison against primary records.
Continuity of human vulnerability	The durable strategic variables remain social trust, identity, emotion, grievance, institutional legitimacy, and distribution. Generative quality cannot substitute for a believable social path to the audience.

14.6 Strategic assessment

The most consequential future change is likely to be the industrialization of attribution deception. Instead of one forged newspaper, one clandestine radio station, or one carefully constructed front organization, an actor may be able to sustain a portfolio of synthetic identities, pseudo-local outlets, forged media, automated interactions, and multilingual variants. But the defender also gains more observable data: account graphs, timestamps, infrastructure, model artifacts, repost patterns, signing/provenance technologies, and cross-platform evidence.

The competitive center of gravity will therefore shift toward authentication systems and social trust. Institutions that can rapidly demonstrate “this is genuinely ours,” preserve verifiable archives, maintain secure channels with journalists and platforms, and communicate corrections through trusted local intermediaries will be harder to impersonate. Conversely, institutions that already suffer low trust, fragmented communications, weak cybersecurity, and slow response may be disproportionately vulnerable.

Final conclusion Black propaganda is not merely “a lie.” It is an organized influence mechanism that manipulates provenance, identity, and trust. Its distinctive strategic move is to make the audience evaluate a message under the wrong source identity. The most reliable defense is therefore not ideological counter-propaganda but disciplined provenance analysis: verify the source, reconstruct the chain, authenticate the media, compare independent evidence, measure coordination, and state uncertainty honestly.

Reference Notes for In-Text Brackets

Ref.	Source
[1]	Springer Nature, "Propaganda" (2026), source-based typologies; etymological background.
[2]	Goldstein & Findley, eds., Psychological Operations: Principles and Case Studies, Air University Press (1996).
[3]	Wardle & Derakhshan, Information Disorder, Council of Europe (2017); UNESCO journalism handbook (2018).
[4]	UK National Archives, Political Warfare Executive records and institutional history.
[5]	National WWII Museum, Operation Cornflakes historical account.
[6]	Thomas Boghardt, "Soviet Bloc Intelligence and Its AIDS Disinformation Campaign," CIA Studies in Intelligence 53(4) (2009); Kramer/Selvage archival discussion of Operation Denver.
[7]	CIA Studies in Intelligence historical account of the Congress for Cultural Freedom and covert sponsorship.
[8]	CIA Reading Room documents concerning the Sacred Sword Patriots' League; Richard H. Shultz Jr. (1999).
[9]	U.S. Department of Justice, Internet Research Agency indictment, Feb. 16, 2018.
[10]	U.S. Department of Justice, GRU indictment concerning DCLeaks and Guccifer 2.0, July 13, 2018.
[11]	U.S. Department of Justice, disruption/seizure of domains used in the Russian "Doppelganger" influence operation, Sept. 4, 2024.
[12]	Google Threat Analysis Group, DRAGONBRIDGE / Spamuouflage reporting (2024).
[13]	OpenAI, "Disrupting deceptive uses of AI by covert influence operations," May 30, 2024, and later threat reports.
[14]	Meta public reporting on Coordinated Inauthentic Behavior and deceptive networks.
[15]	NATO policy materials on information threats and disinformation (2024-2025).
[16]	Vosoughi, Roy & Aral, "The spread of true and false news online," Science 359 (2018).
[17]	Brady et al., "Emotion shapes the diffusion of moralized content in social networks," PNAS 114 (2017).
[18]	Current Opinion in Psychology review (2024) on repetition and belief in misinformation / illusory truth.
[19]	U.S. Department of Justice, FARA Frequently Asked Questions, updated 2026.
[20]	Federal Election Commission, "Foreign nationals."
[21]	National Conference of State Legislatures, "Artificial Intelligence (AI) in Elections and Campaigns," updated June 23, 2026.
[22]	New York Times Co. v. Sullivan, 376 U.S. 254 (1964).
[23]	United States v. Alvarez, 567 U.S. 709 (2012).
[24]	18 U.S.C. § 1343, fraud by wire, radio, or television.
[25]	ICRC Customary IHL Rule 62, improper use of enemy flags, military emblems, insignia or uniforms.
[26]	SEC/Investor.gov, "Social Media and Investing - Stock Rumors" and 2026 social-media stock-scam alerts.
[27]	SEC v. Andrew Left and Citron Capital litigation release (July 26, 2024); used solely as an illustration of alleged deceptive market-related speech integrated with trading conduct, not as a black-propaganda case.

Editorial note on controversial or current influence operations

Where official U.S. or platform sources attribute an operation to a state or organization, this report describes the claim as an official attribution, allegation, or platform assessment unless the sponsorship is supported by broader historical documentation. Criminal indictments are allegations unless and until resolved by a final judgment. Intelligence assessments can be authoritative for policy purposes without being equivalent to evidentiary findings after adversarial litigation. Historical operations with incomplete archives are presented with the strongest available documentary basis and explicit uncertainty.

Authors and websites

The American Newspaper - <https://americannewspaper.org>

AmericanTV - <https://americantv.org>

Prepared as a research and media-forensics reference. The report is educational and analytical and is not legal advice.