

The Cauldron Never Empties: Synthetic Narratives that Create Strategic Opportunity

By
Greg Sharpe, Fellow

Published: October 19, 2026

The most dangerous Russian information operation may not begin with a lie. It may begin with something true. A legitimate news report. An authentic photograph. A real grievance. Russia's information operators need not manufacture the informational environment when Western societies produce credible material every hour. They can enter that stream, identify narratives with emotional or political weight, and introduce just enough distortion to change their meaning. The cauldron is already full. The task is to keep it hot, stir selectively, and add synthetic ingredients slowly enough so that audiences struggle to see where fact ends and manipulation begins.

The problem is that there the contamination is increasing. Manipulated narratives are posted beside authentic information, counterfeit sites resemble legitimate journalism, artificial personas discuss genuine disputes, and real reporting is reframed until audiences carry the distortion forward. The [U.S. Department of Justice's 2024 disruption of the Russian-directed Doppelganger operation](#) offers a documented example. Russian actors used 32 domains, websites mimicking legitimate media, AI-assisted advertisements, fabricated personas, and influencers to promote state narratives while concealing their origins.

Credibility itself can become exploitable terrain. Operators need not make audiences trust Russia; they can exploit something familiar long enough for a manipulated interpretation to take hold. A counterfeit article borrows a newspaper's authority. A false account gains plausibility from an authentic conversation. A manipulated video is posted beside genuine footage which exploits viewers' difficulty from distinguishing them.

The [European External Action Service's 2025 threat report](#) described hundreds of domains, coordinated networks, multiple languages, and localized content aimed at undermining democracy and support for Ukraine. It linked Russian information activity to drone incursions, sabotage, and attacks on critical infrastructure.

This creates a **bait-and-switch dynamic**, which is an analytical description, not a formal Russian doctrinal term. The bait is real: a military incident, economic grievance, election controversy, or historical argument. The switch changes its frame. An authentic report receives a fabricated caption, a real photograph is assigned to the wrong location, or a genuine speech is shortened until its meaning changes. The altered version moves faster than the original.

AI increases the volume. Before Moldova's 2025 parliamentary election, researchers documented Russian-linked activity using generated articles, spoofed Western media sites, fabricated allegations, artificial personas, and engagement networks. [The Associated Press reported](#) that some operations imitated serious journalism. Repeated exposure can leave people unsure whether anything deserves trust.

Synthetic artifacts force verification. Journalists check images; analysts trace provenance; governments coordinate attribution; fact checkers reconstruct timelines. Meanwhile, contaminated narratives keep moving. Screenshots survive debunking, clips circulate without corrections, and translations lose context. The advantage may be less about convincing everyone of one falsehood than forcing institutions and publics to argue over what happened.

Synthetic media also creates a “liar’s dividend.” Once audiences know audio, photographs, and video can be fabricated, authentic evidence faces an added burden of proof. A fake can impersonate reality, while genuine evidence can be dismissed as fake. Fabricated material may be accepted and authentic material rejected.

Influence need not dictate a decision directly. It can alter the information surrounding it until a preferred choice seems reasonable. Hesitation may appear prudent, even when adversarial activity helped create uncertainty. This is why [NATO Allied Command Transformation’s work on cognitive warfare](#) matters. It focuses on manipulating perception, trust, judgment, cohesion, and decision-making, not simply content. Small shifts in confidence or willingness to act can affect coordination and decision speed.

The [September 2026 Narrative Strategy Symposium](#) in Arlington reflected this broader concern, examining influence warfare, artificial intelligence, narrative strategy, and societal resilience. Narrative security cannot be separated easily from decision security. The question is whether institutions retain enough confidence in their information to act before uncertainty becomes strategically useful to an adversary.

Russia can exploit an existing narrative, introduce manipulated material, surround it with apparent corroboration, and amplify it across channels. Disagreement fragments audiences. Screenshots, search results, commentary, and translations preserve those fragments. Later audiences may encounter the derivative narrative before the original evidence. The false trail begins generating its own apparent history.

These activities create a strategic asymmetry. Western institutions face expectations of evidence, attribution, transparency, and credibility. Russia can produce ambiguity faster than democratic institutions can resolve it, then portray their caution as weakness or concealment. The response cannot simply be to debunk more content. Verification must be paired with rapid authentication, transparent attribution, and clear communication about what is known, what remains uncertain, and why. Institutions should make credible evidence accessible before manipulated versions dominate the conversation. Resilience means preserving the ability to make timely, evidence-based decisions under uncertainty, not eliminating uncertainty altogether.

There is also a danger to overcorrecting. If governments label inconvenient reporting or legitimate dissent as foreign interference without sufficient evidence, they risk damaging the very credibility they seek to protect. Effective responses must distinguish coordinated hostile manipulation from authentic journalism and domestic disagreement. Otherwise, defensive measures can reinforce suspicions that adversaries are trying to cultivate.

Deterrence depends on beliefs about capability, credibility, cohesion, and willingness to act. If Russian leaders see prolonged attribution disputes and hesitation driven by [information contamination](#), they may misread confusion as political weakness. The risk is not only persuasion, but misperception produced by uncertainty Russia helped create.

Russian information operations are not simply a contest between truth and falsehood. The battlefield is the boundary between them, where credibility can be borrowed to weaponize authentic evidence and repetition can manufacture apparent corroboration. Digital debris becomes tomorrow's source material, giving operators another chance to stir the cauldron.

The cauldron need not produce one dominant narrative. It only needs enough [Foreign Information Manipulation and Interference](#) in enough languages to consume attention, divide interpretation, and delay confidence. Russia does not have to make the world believe Moscow. It may be enough to keep the world arguing with itself while synthetic narratives harden into political positions and shape the next crisis before the last is understood.

Stirring the cauldron does not have to break the geopolitical system. It only must stay warm.

Mr. Greg Sharpe is a Fellow and the director of Communications and Marketing for the National Institute for Deterrence Studies and the Managing Design Editor for the Global Security Review. He has 25+ years in marketing and communications with a focus on digital communications, organizational and institutional change, and analysis. Greg has over 45 years of military, federal civilian, and defense contractor experience in the fields of database development, digital marketing & analysis, technology use case exploration, and assessment, and as a USAF Doctrine outreach and engagement analyst. Views expressed are his own.