T2COM Intelligence Post

3 FEBRUARY 2026

Russia Using Information Confrontation as a Weapons System

EXECUTIVE SUMMARY

The Russian Armed Forces integrate information confrontation at all levels of military planning to achieve strategic outcomes without the use of conventional force. Deception is a key component of information confrontation, enabling Russian commanders to conduct offensive and defensive operations. Observations from Russian operations in Crimea and, most recently, OPERATION OVERLOAD in Moldova highlight how information confrontation impacted tactical to strategic initiatives. Understanding information confrontation would allow U.S. Army commanders, staffs, and planners to enhance the visualization of the operational environment, counter Russian deception tactics, and improve training against Russian information confrontation operations.

RUSSIA DOCTRINALLY VIEWS INFORMATION AS A WEAPONS SYSTEM

Information operations are embedded at all levels of Russian military planning. While U.S. and NATO militaries maintain a separation between public affairs, cyber defense, and psychological operations, Russian doctrine fuses them into a unified operational concept known as information confrontation.[1] The Russian Armed Forces believe that information confrontation can achieve strategic outcomes without the use of conventional force. Russia uses information confrontation against adversaries to undermine decisionmaking, threaten societal cohesion, and degrade command, control, communication, computers, cyber, intelligence, surveillance, and reconnaissance (C5ISR) systems. Successful information confrontation disrupts an adversary's planning and coordination efforts and degrades its view of the electronic environment.

Information confrontation can be viewed as both a legacy and current innovation for the Russian military: a reimagining of Soviet military doctrine for the digital age. The Soviet-era concept of active measures *(aktivnye meropriyatiya)* has evolved into the contemporary model of reflexive control—manipulating an adversary's perception to induce self-defeating behavior.[2, 3] This evolution was reflected in the 2011 Russian Ministry of Defense document, "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space," which defines military information activity as "achieving superiority in the information space."[4]

The weaponized narrative is applied through a doctrinal view of the information environment as a battlespace. To accomplish this weaponization, Russian doctrine states commanders should aggressively shape and contest the information environment like maneuver forces would shape and contest physical objectives.

INFORMATION CONFRONTATION AND DECEPTION

Deception (maskirovka) is deeply integrated into Russian information confrontation doctrine and remains a primary tool of Russian operational art. Russian theorists emphasize deception in information confrontation not only as a means of concealment but also as a method for creating an alternative reality for targeted commanders and sensor systems.[5] Observations of recent Russian military, intelligence, and diplomatic operations highlight the practical implications of deception and disinformation on Russia's adversaries across all levels of operations: strategic masking of intent, operational manipulation of data, and tactical denial of the truth.[6]

The Russian Ministry of Defense identifies deception as both offensive and defensive. Information is used to protect the Russian commander's decision space while simultaneously disrupting the adversarial commander's ability to visualize the battlespace.[7] Russian deception operations achieve maximum effect by blending psychological, electronic, and cyber capabilities. The desired end-state is mutually supporting capabilities designed to fracture trust and distort perceptions.[8]

Russian forces complement the cognitive distortion achieved by information confrontation through tailored electronic warfare (EW). Russian doctrine distinguishes EW that supports information confrontation from their more traditional concept of EW supporting maneuver operations known as radio electronic battle.[9], [10] The use of EW supporting information confrontation requires deceptive techniques to ensure that the targeted unit does not suspect it is under electronic attack. At a set time, as part of a planned information operation, EW units will target key adversary systems to overwhelm or physically destroy them.[11]

INFORMATION CONFRONTATION IN PRACTICE: CRIMEA AND MOLDOVA

Russian commanders view information as a precision weapon with few drawbacks; they perceive it as cheap, deniable, targetable, and scalable. Observations from Russian activities in Crimea (2014) and Moldova (2024-25) highlight how information confrontation enables operations. By conceptualizing information as a precision weapon, Russian planners achieve nested effects, including destabilization, delegitimization, and deterrence from the tactical to the strategic levels without risking overt escalation.

The Russian use of information confrontation in the invasion and annexation of Crimea involved narrative control, deception, and technical means.[12] The contribution of information confrontation to the success of the operation is the result of a decade of Russian military thought and doctrinal refinement.[13] Russian planners used lessons from the 2008 Russian invasion of Georgia to integrate cyber, propaganda, and deception operations.[14] This resulted in an expanded use of information confrontation tools during Russia's annexation of Crimea.

Figure 1: Russian Forces Without Distinguishing Insignia in Crimea, 2014 (Source: WikiCommons)[15]

The primary Russian innovation between 2008 and 2014 was increased coordination between information confrontation planners, supported commanders, and organizations conducting information operations. Russian military leadership increased cooperation with the national press, intelligence agencies, and military units to maximize the information confrontation effect.[16, 17] By capitalizing on coercive messaging to the West and interfering with Ukraine's ability to see the battlefield, Russian operatives in Crimea, known as "little green men," were able to complete their assigned objectives largely unopposed.

Russia's OPERATION OVERLOAD against Moldova offers a more recent example of Moscow's adaptive information warfare. This operation was an AI-amplified propaganda campaign that impersonated Western news outlets and spread divisive narratives to influence the 2025 Moldovan parliamentary elections.[18, 19] Early efforts sought to delegitimize President Maia Sandu's reformist agenda by portraying the government as corrupt and controlled by the West.[20] As early as June 2024, Western governments publicly accused Moscow of attempting to sway Chişinău's elections via disinformation and illicit funding.[21] The Moldovan Security Service later exposed influence networks tied to exiled pro-Russia oligarch Ilan Shor, channeling Russian money through cryptocurrency and shell NGOs.[22] By late 2025, Moldovan authorities had conducted raids and arrests of individuals accused of laundering Russian funds to destabilize the government.[23]

OPERATION OVERLOAD combined financial interference, cyber-enabled propaganda, and on-the-ground agitation to undermine confidence in Moldovan democratic institutions. This hybrid approach also blended doctrinal information confrontation and other tools of state power to wield information and achieve reflexive control. Although OPERATION OVERLOAD did not change the outcome of Moldova's parliamentary elections, it did increase social and political tensions in the small Black Sea nation.[24]

IMPLICATIONS FOR THE U.S. ARMY

Viewing information confrontation through a Russian doctrinal framework allows commanders and supporting staffs to understand how Russia uses information as both a sword and a shield. By examining Russian application of information confrontation, Western commanders may be able to anticipate and counter Russian deception. This would provide U.S. Army commanders with a deeper understanding of the environment and more options in developing courses of action.

Operationally, cases like Moldova reveal the adaptability of Russia's doctrine to nonmilitary arenas, employing hybrid methods that merge cyber, finance, and narrative manipulation. For military planners, these patterns underscore that Russia's information warfare is not a discrete capability but a holistic strategy. Understanding how information confrontation combines state, military, and proxy actors may allow commanders, intelligence personnel, and information warfare planners to identify and counteract Russian efforts.

The U.S. Army may benefit from increased realism by conducting exercises in a contested information environment. Replicating the impact of Russian technical attacks can be achieved by degrading components of the training unit's C5ISR capability. Units can employ red teaming to identify the potential impacts of maskirovka on the battlefield. Finally, strengthening the incorporation of behavioral health teams and chaplains, as well as reinforcing the role of noncommissioned officers in maintaining good order and discipline through Soldier engagement, may reduce the negative effects of deception meant to demoralize Army formations.

References

1 Grisé, Michelle, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska. "Russian Conceptions of Information Confrontation." Santa Monica, CA: RAND Corporation, 2022. https://www.rand.org/pubs/research_reports/RRA198-8.html.

2 Ibid.

3 Fridman, Ofer. Russian *"Hybrid warfare": Resurgence and politicization*. New York, NY: Oxford University Press, 2019. Pp. 42-45.

4 Ministry of Defense of the Russian Federation. «Концептуальные взгляды на деятельность Вооружённых Сил Российской Федерации в информационном пространстве.» Москва: Министерство обороны РФ, 2011. https://safe.menlosecurity.com/doc/docview/viewer/docN621638115C31b271455882526c4046faebd3d67c88e123a8449fda2db8738e46d180b6a42b05

5 Saifetdinov, K. I. «Информационное противоборство в военной сфере.» *Военная мысль*, no. 7 (2014): 38–41. https://www.elibrary.az/docs/JURNAL/jrn2014_615.pdf.

6 Ibid.

7 Ibid.

8 Ibid.

9 Ibid. P.2-2, Para. 2-10.

10 Ibid.

11 Ibid. Pp. 2-1, 2-1.

12 Bembenek, Christina, "Truly Understanding the Adversary: Describing the Threat in the Information Space", *Military Intelligence Professional Bulletin*, U.S. Army Military Intelligence Center of Excellence, April – June 2021. https://tinyurl.com/bdyzdsxb

13 Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, Khrystyna Holynska, "Rivalry in the Information Space: Russian Conceptions of Information Confrontation" RAND Corporation, 2022. https://tinyurl.com/yc4j2268

14 Emilio J. Iasiello, "From Georgia to Crimea: Russia Adjusts its Information Operations to Fit the Conflict." *Parameters*, 2021. https://press.armywarcollege.edu/parameters/vol47/iss2/7/

15 By Anton Holoborodko (Антон Голобородько) - http://www.ex.ua/76677715, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=31559794

16 Emilio J. Iasiello, "From Georgia to Crimea: Russia Adjusts its Information Operations to Fit the Conflict." *Parameters*, 2021. https://press.armywarcollege.edu/parameters/vol47/iss2/7/.

17 Ibid.

18 Institute for Strategic Dialogue. "Operation Overload's Underwhelming Influence and Evolving Tactics." Washington, DC: Institute for Strategic Dialogue, 2025. https://www.isdglobal.org/digital_dispatches/operation-overloads-underwhelming-influence-and-evolving-tactics/

19 Ibid.

20 Atlantic Council. "Moldova Accuses Russia of Election Interference Ahead of Key Vote." Washington, DC: Atlantic Council, 2024. https://www.atlanticcouncil.org/blogs/ukrainealert/moldova-accuses-russia-of-election-interference-ahead-of-key-vote/.

21 Balmforth, Tom, and Jonathan Landay. "Us, Britain, Canada Accuse Russia of Plot to Sway Moldova Election | Reuters." US, Britain, Canada accuse Russia of plot to sway Moldova election, June 14, 2024. https://www.reuters.com/world/us-britain-canada-accuse-russia-plot-influence-moldova-election-2024-06-13/.

22 Insikt Group. "Russian Influence Assets Converge on Moldovan Elections." Recorded Future: Securing Our World With Intelligence, September 3, 2025. https://www.recordedfuture.com/research/russian-influence-assets-converge-on-moldovan-elections.

23 Mcgrath, Stephen. "Moldovan Officials Carry out Raids and Detain 1 over Alleged Russian Financing of a Party." AP News, September 23, 2025. https://apnews.com/article/moldova-election-russia-raids-europe-8f32d48131335f44be2bb5f5d55f934d.

24 Ibid.