Jamestown

Strategic Snapshot

01.11.2026 Russia–PRC Technology & Hybrid Operations

Russia–PRC Technology & Hybrid Operations

The Jamestown Foundation
January 11, 2026

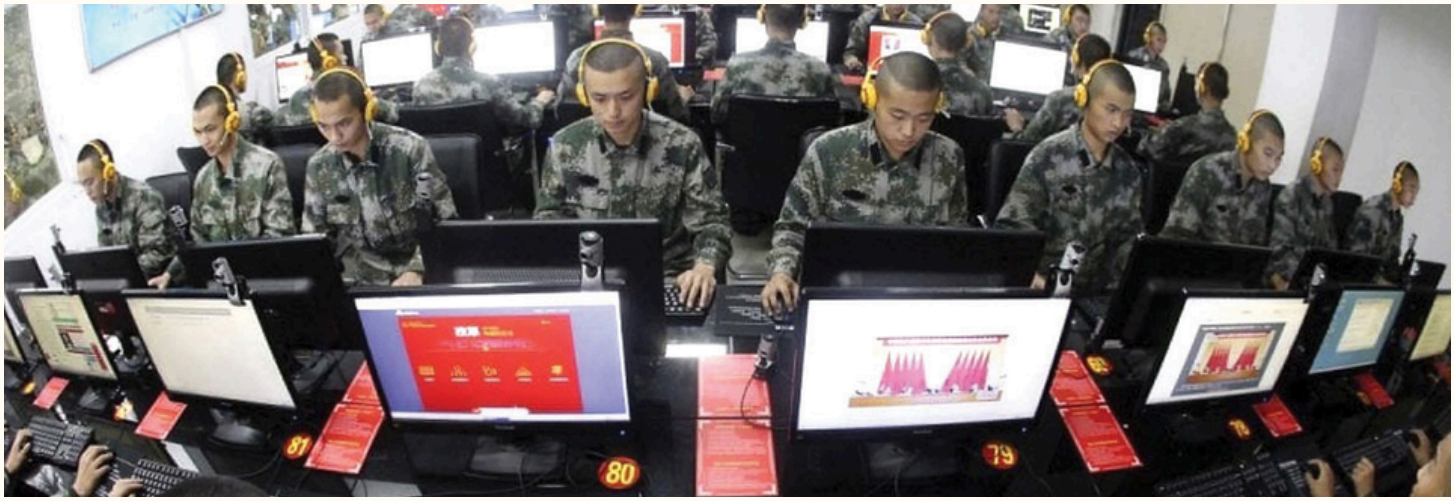
Introduction

Technological innovation is reshaping the modern battlefield. Russia and the People's Republic of China (PRC) are combining conventional warfare with electromagnetic disruption, cyber attacks, digital influence campaigns, and unmanned and autonomous systems to target U.S. partners and allies. The frontline states of the North Atlantic Treaty Organization (NATO) are under mounting pressure from these new technological threats. Russian violations of Polish, Estonian, Latvian, Lithuanian, and Romanian airspace, as well as GPS spoofing and sabotage of critical undersea infrastructure, particularly fiber-optic cables, in the Baltic and Arctic regions, illustrate the expanding scope of targeting technology and its use for subversive means. These activities reflect a broader shift toward multi-domain warfare, where ambiguity and deniability are key assets.

Drone warfare is now a central feature of this evolving technological domain. Ukraine has become a world-leading drone producer and pioneer of maritime and autonomous systems since Russia's full-scale invasion began in 2022. The PRC has also recently unveiled new unmanned systems capabilities for use in a Taiwan contingency, signaling its intent to operationalize lessons from Russia's war in Ukraine.

The PRC and Russia's military technological modernization builds on decades of Cold War-era research, illicit procurement networks, and recent battlefield experience in Ukraine. Military technology procurement, however, remains a challenge. The PRC and Russia are exploiting procurement loopholes and legacy networks to accelerate the acquisition of military technology. Beijing continues to use middlemen and shell companies to circumvent export controls, while Moscow faces constraints from sanctions, talent shortages, and budget limitations that hinder sustained innovation and production. The development of artificial intelligence (AI)-enabled command systems, autonomous platforms, and integrated air defenses depends on state investment.

Russia and the PRC are not merely modernizing their military technology and capabilities; they are reengineering the operational environment to exploit systemic vulnerabilities in Western defense architectures. Deterrence in this environment will depend less on mass and more on agility, resilience, and adaptability to counter new and evolving technological threats before they escalate.



Source: People's Liberation Army via U.S. Military Press

Military Artificial Intelligence

Executive Summary

- The People's Republic of China (PRC) is leveraging Artificial Intelligence (AI) to enhance its military capabilities and strategic advantages using Western technology. This includes Meta's open-source model Llama (Large Language Model Meta AI), which is a preferred model for building features tailored to military and security applications.
- The People's Liberation Army (PLA) is showing signs of adapting to the era of AI, emphasizing intelligentized warfare, prioritizing information dominance, algorithms, and systemic disruption over population, resources, or industrial capacity.
- Russia's full-scale invasion of Ukraine marked the first major conflict with widespread AI use. Ukraine, supported by U.S. AI firms, successfully countered Russian forces, prompting Russia to accelerate AI integration in command systems, drones, and air defense networks.

Russia–PRC Technology & Hybrid Operations

Selected Jamestown Analysis:

- Deep Seek Use in PRC Military and Public Security Systems, October 27, 2025, Sunny Cheung and Kai-shing Lau.
- Dissipative Warfare: The PLA's Potential New Strategy in the AI Era, September 19, 2025, K. Tristan Tang.
- Experts See Risk and Reward to Integrating AI in Nuclear Weapons, June 7, 2025, Alex Lewis Richter.
- Russia Capitalizes on Development of Artificial Intelligence in Its Military Strategy, March 3, 2025, Sergey Sukhankin.
- PRC Adapts Meta's Llama for Military and Security AI Applications, October 31, 2024, Sunny Cheung.

Source: Ukrainian Ministry of Defense

Drones & Autonomous Systems

Executive Summary

- Ukraine has become the largest producer of tactical and long-range drones in the world. The country's defense sector has grown by 350 percent since the start of Russia's full-scale invasion in 2022. Low-cost, rapid-production systems such as AI-driven drones, robotic ground vehicles, and long-range missiles such as the FP-5 give Ukraine asymmetric advantages. Ukraine's advanced maritime drones, such as the Magura and SeaBaby, have have demonstrated high effectiveness, sinking ships, striking aircraft, and even damaging infrastructure like the Kerch Bridge.
- Russia is increasing the production and use of Shahed-type kamikaze drones against Ukraine, constantly improving their effectiveness and ability to break through air defenses. Moscow is also developing and testing unmanned aerial vehicles (UAVs) featuring AI for auto-targeting and computer vision, which it may transfer to allies such as the PRC and Iran in exchange for resources and weapons.
- Chinese military experts are incorporating lessons from Russia's full-scale invasion of Ukraine on the use and importance of drones and autonomous systems, which is reshaping the PLA's strategic planning and operational doctrine. Chinese strategists emphasize the need to develop stealthier drones, robust anti-jamming capabilities (such as fiber-optic guidance), and autonomous ground logistics systems to enhance battlefield sustainability and reduce vulnerabilities in future combat scenarios.

Russia–PRC Technology & Hybrid Operations

Selected Jamestown Analysis:

- PLA Insights from Ukraine's Asymmetric USV Operations, October 31, 2025, *Sunny Cheung and Owen Au*.
- *Russia's War Transforms Ukraine into a World-Leading Military Producer*, October 5, 2025, *Taras Kuzio*.
- Maritime Drones Becoming Flagship of the Ukrainian Navy, October 1, 2025, *Yuri Lapaiev*.
- Ukraine Ramps Up Defense Production With Increased International Cooperation, September 17, 2025, *Yuri Lapaiev*.
- *Moscow Downplays Drone Incursion on Poland*, September 15, 2025, *Pavel K. Baev*.
- Russian Drones Pose Growing Danger, *June* 4, 2025, *Yuri Lapaiev*.
- Drone Attacks on Port Sudan Jeopardize Plan for Russian Red Sea Naval Base, May 28, 2025, *Andrew McGregor*.
- *Autonomous Battlefield: PLA Lessons from Russia's Invasion of Ukraine*, March 28, 2025, *Sunny Cheung and Joe McReynolds*.
- *Ukrainian Drone War Shakes Up Russian Society*, October 16, 2024, *Vadim Shtepa*.
- *Ukraine Leads World in Drone Innovation and Production*, October 8, 2024, *Taras Kuzio*.
- *PLA Unveils New Unmanned Weapons Aimed at Taiwan at the Zhuhai Airshow*, December 20, 2024, *Peace Ajirotutu*.
- *PRC Gray Zone Activities Against Taiwan: Civilian Drone Incursions*, December 20, 2024, *Yiyao Alex Fan*.
- *Russian Drone Crash Exposes Critical Weakness in Latvian Comprehensive Defense*, November 15, 2024, *Ovels Nikers*.
- *Innovative Ukrainian Naval Tactics Largely Nullify Russia's Black Sea Superiority*, August 13, 2024, *John C. K. Daly*.
- *Ukraine's Drone and Missile Offensive in Black Sea Knocks Russian Navy Flat Aback*, March 26, 2024, *Andrii Ryzhenko*.

Source: European Space Agency

Satellites & Space Technologies

Executive Summary

- Chinese military strategists view commercial space as an essential strategic force in future conflict, as the PRC begins to narrow the gap in its space capabilities relative to the United States. The first national-level long-term plan for space science development from the PRC sets the goal of becoming a global leader by 2050, by which point it aims to lead in revolutionary scientific breakthroughs and deep-space missions, and to become the global center for space science.
- Russia's state-owned space corporation, Roscosmos, controls eight percent of the Russian military-industrial market and provides the Russian military with technology such as rockets, spacecraft, and satellite systems. Roscosmos faces debilitating challenges, including financial difficulties, inefficiencies, and the loss of Western partnerships since Russia's full-scale invasion of Ukraine.
- Kyiv has recently prioritized developing a national satellite communication system as a key element of Command and Control and military technology development. Ukraine is searching for alternatives to Starlink since the sudden connectivity losses during the maritime drone attack on Sevastopol in 2022 and the Ukrainian Armed Forces' operation in Russia's Kursk oblast in 2024.

Russia–PRC Technology & Hybrid Operations

Selected Jamestown Analysis:

- PLA Military Aerospace Force: On the Frontier of Innovation and Competition, *July 11, 2025, John Castello.*
- *Ukraine Prioritizes Developing National Satellite Communications System, April 10, 2025, Yuri Lapaiev.*
- *Roscosmos's Director General Exemplifies Inefficiency in Russian Government, March 6, 2025, Mikael Pir-Budagyan.*
- PRC Unveils New Space Plan, *November 5, 2024, Jie Gao.*
- *Russian GPS Games in the Baltic Sea Region, May 15, 2024, Otto Tabuns.*
- *The Future of Roscosmos Unclear as Challenges Mount, February 23, 2024, Pavel Luzin.*

Source: National University of Defense Technology

Military Cyber Operations & Information Technology

Executive Summary

- The PRC's reorganized Cyberspace Force recently displayed command and control, reconnaissance and sensing, and cyber-electromagnetic countermeasures equipment at a parade commemorating the end of World War II. This included a new UAV data relay system, a data spectrum monitoring vehicle, a signal-jamming vehicle, an electromagnetic reconnaissance and jamming vehicle, a network communication node vehicle, and an information jamming vehicle. These upgrades suggest that the PLA has learned lessons from shortcomings in information and electronic warfare during the Russian invasion of Ukraine.
- Russian information security companies are expanding their operations in Russia's near abroad despite facing limitations caused by Western sanctions, as other states increasingly view internet freedom as a threat to their sovereignty. Russia's information security sector continues to struggle with a shortage of technology and personnel to prepare the country for continuing cyber conflict, relying solely on domestic solutions.
- Poland has become the primary target for Russian subterfuge, including low-level sabotage, insider espionage, informational warfare, and cyber-attacks.

Russia–PRC Technology & Hybrid Operations

Selected Jamestown Analysis:

- New Quality Combat Forces Underpin Military Modernization, *December 22, 2025, Arran Hope.*
- *New Military–Civil Fusion Body for PRC Robotics Ecosystem, December 18, 2025, Sunny Cheung.*
- *Kremlin Shifts Focus to Information Warfare, November 6, 2025, Yuri Lapaiev.*
- *Cyberspace Force Equipment at the 2025 Military Parade, October 1, 2025, Thomas He and Ying Yu Lin.*
- *Weaponizing the Electromagnetic Spectrum: The PRC's High-powered Microwave Warfare Ambitions, May 9, 2025, Tin Pak, Yu-cheng Chen.*
- *Poland on the Frontlines Against Russia's Shadow War, May 8, 2025, Anjou Kang-Stryker and Janusz Bugajski.*
- *The Cyberspace Force: A Bellwether for Conflict, April 25, 2025, John Castello.*
- *Russia's Information Security Industry Expands International Footprint, March 27, 2025. Luke Rodeheffer.*
- *Russian IT Sector Effectively Serves the Kremlin Despite Sanctions, February 27, 2025, Ksenia Kirillova.*
- *Russia Ramps Up Cybersecurity Systems, February 6, 2025, Luke Rodeheffer.*
- *PRC Use of Middlemen to Circumvent US Government Export Controls: The Case of Suzhou Rebes Electronic, July 12, 2024, Matthew Bruzzese.*
- *Russia's War Against Ukraine Driving Evolution of Cyber Warfare, July 3, 2024, Luke Rodeheffer.*
- *PRC Transfer of Military and Dual-Use Technology: the Case of the International Conference on Defence Technology, June 7, 2024, Matthew Bruzzese.*
- *Foreign Intelligence Hackers and Their Place in the PRC Intelligence Community, March 29, 2024, Matthew Brazil.*

Source: OSP.ru

Undersea Cables

Executive Summary

- The PRC is promoting cross-border power transmission projects, deploying its leading producers of submarine electric cables to deepen integration with other countries' critical infrastructure. Beijing sees submarine cables as critical infrastructure that can serve as conduits not just for electrical power but also for its own geopolitical power.
- Earlier in 2025, suspicious activities by the merchant vessels Shunxing-39 and Vasili Shukshin in the vicinity of Taiwan suggest a possible collaboration between Chinese and Russian merchant ships related to the reconnaissance and sabotage of undersea communications cables connecting Taiwan to the outside world.
- In the Baltic and Arctic regions, Russian hybrid attacks targeting critical undersea infrastructure, particularly fiber-optic cables, have surged. Incidents in 2023 and 2024 involving Chinese vessels damaging Baltic subsea cables raise concerns over possible Russian–PRC hybrid warfare collaboration.

Russia–PRC Technology & Hybrid Operations

Selected Jamestown Analysis:

- PRC Seeks Dominance in Submarine Power Cable Infrastructure, *July 2, 2025, Tsaiying Lu and Athena Tong.*
- *Strangers on a Seabed: Sino-Russian Collaboration on Undersea Cable Sabotage Operations*, *February 14, 2025, John Dotson.*
- *Hybrid Attacks Rise on Undersea Cables in Baltic and Arctic Regions*, *February 5, 2025, Gabriella Gricius.*
- *Creative Destruction: PRC Undersea Cable Technology*, *January 16, 2025, Sunny Cheun and Cheryl Yu.*

The Jamestown Foundation is an independent, nonpartisan organization supported by tax-deductible contributions from corporations, foundations and individuals. To donate to Jamestown, please call (202)483-8888 or donate through our website: **www.jamestown.org**

A: 1310 L Street, NW, Suite 810,
Washington DC 20005
T: (202) 483-8888
F: 202 483-8377
W: jamestown.org