CNA

CNA Research Highlights

October 2025

About This Newsletter

This publication contains highlights of CNA's work during the fourth quarter (July through September) of FY 2025. The highlights include work from CNA's federally funded research and development center (FFRDC), the Center for Naval Analyses, as well as from CNA's Institute for Public Research (IPR).

If you would like more information about a particular study, please email inquiries@cna.org.

Table of Contents

China, Russia, and Global Security

PRC Concepts for UAV Swarms in Future Warfare

Timothy Ditter and Eleanor Harvey

DOP-2024-U-040462-1Rev

This report examines People's Republic of China (PRC) writings on the growing use of uncrewed aerial vehicles (UAVs)—commonly called "drones"—in warfare. The PRC has been developing and testing uncrewed platforms since the 1960s but has largely lagged behind the world's leading military powers technologically in uncrewed systems, particularly in autonomous and semiautonomous drone swarm research. An examination and analysis of PRC writings from 2019 through 2024 indicates an intent to accelerate and advance the People's Liberation Army's (PLA) development, testing, and use of uncrewed systems, especially for drone swarm technology, in part due to the perceived threat from advancements in US drone capabilities. PRC writings suggest the widespread use of drones in recent conflicts is drawing further PRC attention to drone warfare. PRC writings from the past four years demonstrate that the PLA is exploring the use of uncrewed systems and testing drone swarm technology for use in a possible invasion of Taiwan. In addition, the PRC is examining militaries' use of drones and drone swarms to develop its own counter–drone swarm methods and technologies.

Russian Concepts of Future Warfare Based on Lessons from the Ukraine War

Michael Petersen, Paul Schwartz, and Gabriela Rosa-Hernandez

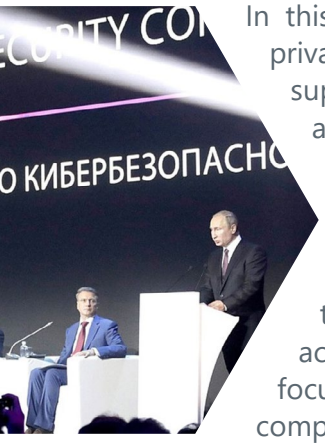
DRM-2025-U-041457-1Rev

This paper examines the evolution of Russian thinking regarding military strategy and conventional operations after three years of conflict in Ukraine. It assesses Russian elite military thought on combined arms operations, naval surface warfare, and air dominance operations, and how the country's strategy and operational concepts should evolve to address changes in the character of armed conflict in future wars. Despite significant tactical and technological changes, Russian strategic and operational thinking remains largely unchanged from approaches adopted prior to the war. Thus, in spite of the ground forces' failure to conduct effective combined arms maneuver, military elites remain focused on suppressing the restoration of the conditions needed to wage future wars of maneuver. Similarly, in spite of the navy's failure to maintain control of the Black Sea, Russian naval thinkers are looking for ways to offset the asymmetric strike capabilities that led to this outcome. Likewise, Russian air power theorists are looking to increase the force size and rely on advanced technology to restore the aerospace forces' ability to achieve air superiority and improve long-range precision strikes in future wars. Thus, as the Russian military reconstitutes its forces, it is likely to do so with its existing strategic and operational concepts in mind and without substantial innovation. However, it would be unwise to discount the Russian military, which remains extremely capable and dangerous despite its many setbacks in Ukraine.

Hacking and Firewalls Under Siege: Russia's Cyber Industry During the War on Ukraine

Justin Sherman

DOP-2025-U-042210-Final



In this paper, we examine how Russian private sector cybersecurity firms are supporting the Russian government as well as how they have adapted to the new economic, security, and geopolitical environment since Russia's full-scale invasion of Ukraine in 2022. We describe the diversity of state and nonstate actors in Russia's cyber web—focusing on the role that private sector companies are playing—and describe how relationships between state elements and cyber companies have changed over time. We provide case studies of three companies: Kaspersky, Security Code, and Positive Technologies. We analyze their relationships with the Russian government and how their functions tie into the Kremlin's objectives. We conclude with three questions that analysts, practitioners, and policy-makers should further explore to better understand the role of private cyber firms in Russia and to develop better responses to future Kremlin threats.

The Shooting Party: Russia's Evolving Threat Perceptions Since 2022

Gabriela Rosa-Hernandez

DOP-2025-U-043056-Final

In this paper, we examine how Russian military thinkers interpret and operationalize the threat perceptions defined by the country's political leadership. Despite nearly four years of war in Ukraine, Russian security concerns regarding US military capabilities remain largely unchanged. Russian military thinkers continue to perceive US ballistic missile defense and Prompt Global Strike programs as the main threats to Russia's security, believing these programs to be designed to degrade Russia's retaliatory strike capabilities. The war in Ukraine has exposed gaps in Russia's military capabilities, heightening Russian anxiety about the North Atlantic Treaty Organization's (NATO's) military contingents in the Baltic and Black Seas, particularly regarding potential US deployments to Finland and Sweden. Viewing the substantial US and NATO military assistance to Ukraine as part of a broader strategy to weaken Russia, Russian military thinkers are particularly alarmed by Ukrainian offensive operations within Russian borders or those that target mainland Russia. Russian military thinkers believe that the United States and NATO are preparing for a long-term confrontation with Russia, which reinforces their views on the importance of maintaining and enhancing Russia's strategic deterrence capabilities.

Dynamics of Russian Civil-Military Relations During the War with Ukraine: Legal Reforms, Elite Dynamics, and Societal Perceptions

Kirill Shamiev

DOP-2025-U-042031-Final

This report examines the evolution of Russian civil-military relations between 2022 and 2025, focusing on how civilian authorities, society, and the military interact and influence each other during wartime. It analyzes legal and regulatory changes affecting civil-military relations, particularly the Kremlin's response to the Russian military's operational and structural deficiencies. The report also explores elite-level developments by analyzing coalition building among key stakeholders in the Ministry of Defense. Furthermore, it incorporates public opinion data to assess societal perceptions of the war and the armed forces, highlighting how these are shaped by battlefield developments and state propaganda. The final section outlines how Russian civil-military relations may develop in the future.

Russia-India Relations: Multipolarity in Practice?

Dmitry P. Gorenburg, Jeffrey Edmonds, Julian Waller, Jeffrey Kucik, and Decker Eveleth

DRM-2025-U-041438-2Rev

The Russia-India relationship has remained stable in the past five years despite a rapidly changing geopolitical situation. At the request of US European Command's Russia Strategic Initiative, we examined cooperation between Russia and India across the political, military, and economic dimensions of their relationship. By examining a set of detailed indicators, we found that the relationship has remained steady, although some aspects—including overall trade—have considerably improved since Russia's invasion of Ukraine and others—including arms sales and other aspects of military cooperation—have declined. The political relationship has remained stable, buoyed in part by the personal rapport between Russian President Vladimir Putin and Indian Prime Minister Narendra Modi.

Intersections: Technology, National Security, and US-China Strategic Competition, Issue 15, July 2025

Chris Cairns, April Herlevi, and John Mahoney

DNL-2024-U-039879-Final5

Written by CNA's experts on China and Indo-Pacific security affairs, *Intersections* is a news digest describing the interplay between the People's Republic of China's (PRC's) technology acquisition and defense industrial base development efforts, US and partner nation responses, and critical and emerging technology risks and challenges with military implications.

Maritime Industry

CNA: A Trusted Partner in Maritime and Defense Revitalization

Randall Gentry and Don Boroughs

DMM-2025-U-042470-2Rev

After decades of declining US shipbuilding and US-flagged maritime trade, leaders in Washington are prioritizing a renaissance of American sea power. The goal is to restore American maritime dominance and ensure our Navy, Marine Corps, Coast Guard, and Merchant Marine have the industrial support and human capital needed to meet global challenges. Achieving this ambitious goal will require not only funding and policy support, but also world-class data analytics, labor analysis, and strategic planning. CNA offers critical resources in these areas.

Artificial Intelligence and Technology

CNA Expertise in Air Traffic Control Modernization

Tayo Ladeinde

IMM-2025-U-042912-Final

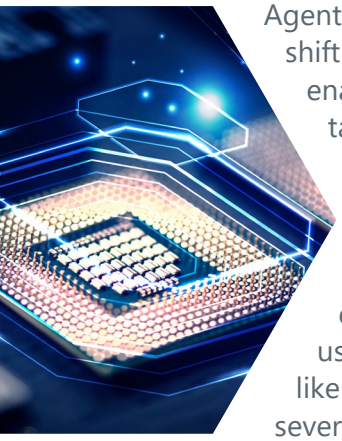
CNA's aviation expertise supports the Federal Aviation Administration, National Aeronautics and Space Administration, Department of Homeland Security, Department of Defense (DOD), and National Institute of Standards and Technology through objective, mission-driven analysis and solutions. We advance air traffic control modernization and the safe integration of emerging technologies into National Airspace System (NAS)—artificial intelligence (AI), machine learning (ML), autonomous systems, uncrewed aircraft systems, and cybersecurity—

via systems engineering, rigorous modeling, and verification and validation. Leveraging partnerships and operations research, CNA delivers pragmatic architectures and evidence-based outcomes that translate policy into operational effect for NAS system stakeholders and accelerate modernization with clarity, rigor, and impact.

Exploring Agentic AI

John Crissman and Kate Thresher

IMM-2025-U-042088-Final



Agentic AI represents a transformative shift from traditional AI models by enabling systems to carry out complex tasks over time and adapt based on context and memory. Unlike single-turn prompt response models, agentic systems form persistent feedback loops to perceive, decide, act, and self-correct toward user-defined goals, behaving more like collaborators. CNA has developed several agentic AI applications, including a data analysis agent, synthetic survey data agentic crew, and wargaming adviser agent. These agents enhance productivity, accessibility, and decision-making in various domains, and robust risk mitigation strategies ensure their safe and effective deployment.

Harnessing Artificial Intelligence and Machine Learning in the Public Sector

John Crissman, Roberto Herrera Del Valle, and Rebekah Yang

IIM-2025-U-042661-Final

CNA is dedicated to helping the public sector leverage the benefits of AI and ML safely, responsibly, and efficiently. Our portfolio of projects includes both research and strategic planning for AI/ML integration as well as prototyping and supporting the use of AI/ML solutions.

Homeland Security

Civil Defense: From the Cold War to Contemporary Threats

Dawn H. Thomas

IOP-2024-U-039690-Final

Civil defense has played a critical role in national security for much of American history. From its origins in World War I Europe, through its establishment in the United States during World War II, and its use during the heightened tensions of the Cold War, civil defense has been used to meet the threats faced by the United States. This white paper explores the historical role of civil defense, its evolution over time, and the relevance of past strategies in addressing today's emerging threats and challenges.

Facing 21st-Century Threats: What Every Consequence Manager Should Know

Dawn H. Thomas, Megan McBride, David Knoll, David Wallsh, Maryanne Kivlehan-Wise, Dmitry P. Gorenberg, and Michael P. Connell

IOP-2025-U-042415-Final

This paper addresses the evolving threat landscape confronting the United States due to advancements in technology and military capabilities. It emphasizes the need for consequence managers to prepare for unprecedented missions by understanding which threat actors have the intent and ability to harm the US, identifying their most likely and consequential targets, and recognizing the vectors they might use to attack.

Integrating UAS to Enhance Public Safety Operations

Steven C. Habicht

IMM-2025-U-042992-Final

As the adoption of UAS continues to increase, this technology offers the opportunity for advancements in public safety operations; however, these opportunities are not without risk. CNA has a deep understanding of the complexities and challenges involved in implementing a new technology in local policing. We serve as the training and technical assistance provider for more than 250 law enforcement agencies, and many of the challenges they are facing are relevant to UAS use.

Military Concepts and Plans

CAN: Cards Against NATO

Nolan J. Noble, Dmitry P. Gorenburg, Jeremy Sepinsky, Jeffrey E. Chilton, Patrick Feng, Michael Petersen, Paul Schwartz, Andrew Olson, Christoper J. Steinitz, Simca Cramer, and Margaret Holmes

DGM-2025-U-042141-Final

Consider this game to be your comedic crash course in geopolitical shenanigans: How might Russia create headaches for NATO, and how might NATO attempt to alleviate them? Think of this game as the appetizer to the main course of real-world discussions—just with a lot more laughs and fewer diplomatic incidents.

Civilian Harm Mitigation and Response in a Large-Scale Contingency Operation Wargame

Lawrence L. Lewis, Andrew Olson, Catherine Lea, Sarah Agyapong, Sabrina Verleysen, Tess Martin, and Christopher J. Steinitz

DIM-2025-U-041492-Final

This document summarizes a February 2025 CNA-facilitated tabletop wargame examining large-scale contingency operations, precision lethality, and civilian harm mitigation and response (CHMR) within the US Indo-Pacific Command (INDOPACOM) area of responsibility. Twenty-five participants from across DOD, INDOPACOM components, and partner organizations explored operational integration of CHMR through six vignettes spanning a range of future warfighting challenges. The analysis identified specific opportunities for INDOPACOM to strengthen future warfighting readiness, including empowering the joint task force commander, improving commanders' guidance, establishing dedicated civilian environment and harm assessment teams, strengthening partner interoperability, and embedding CHMR in cycles of learning for future exercises, simulations, and operations.

Military Personnel and Readiness

DOD Function Code Update and Coding Framework Review

Jessica S. Wolfanger, Tom Woo, Michelle A. Dolfini-Reed, Rikesh Nana, and Darlene E. Stafford

DRM-2025-U-042263-1Rev

DOD function codes identify the type of work performed by all activities in the defense infrastructure and operating forces. Every active, reserve, and civilian manpower authorization (or billet) is assigned a DOD function code in authoritative manpower databases to describe the work performed. The current set of function codes, however, has not been reviewed or updated in five years. CNA reviewed the function codes to determine their currency and relevancy and updated and revised the codes based on subject matter expert discussions and a review of the relevant literature.

Emergency Management and Response

The Virginia Blue Book Project

Joel S. Silverman

IMM-2025-U-042982-Final

To meet current challenges, the Virginia Department of Emergency Management (VDEM) has undertaken a major consequence management planning effort—a modern day Blue Book Project. The goals of the Blue Book Project are to develop a coordinated concept of operations to support local, state, federal, and private sector operational priorities; support Virginia residents; and ensure continuity of government in the event of a coordinated cyberattack on critical infrastructure systems that results in a national emergency. VDEM has received funding from a Federal Emergency Management Agency Regional Catastrophic Preparedness Grant and has contracted with CNA to develop and support this effort.

After-Action Report on the NRV Regional Water Authority's Response to a Boil Water Advisory During Hurricane Helene

Eric Trabert

IMM-2025-U-042995-Final

The NRV Regional Water Authority contracted with CNA to conduct an independent after-action report to identify notable challenges during the flooding incident and provide recommendations to improve response operations and outcomes in future emergencies.

Supply Chain Analysis Capabilities and Experience

Lars Hanson

IMM-2025-U-042480-Final

Over the past six years, CNA has pioneered the analysis of regional food, fuel, and water networks and the analysis of the supply chains of other lifeline commodities to support emergency management planning and operations. Our work in these areas has been featured in presentations at the Big City Emergency Managers and the National Emergency Management Association conferences. In this paper, we present selected highlights of our recent supply chain analysis work.

The CNA Supply Chain Operational Engagement (CNA SCOPE™) Method

Lars Hanson

IMM-2025-U-042479-Final

In an era of increasing urbanization, automation, on-demand delivery, unpredictable weather, and capable nation-state adversaries, large urban areas are more vulnerable than ever to supply chain disruptions for lifeline commodities that can turn a disaster into a catastrophe. Recognizing that 1) public sector relief channels cannot match the scale of need for lifeline commodities in large, concentrated populations, 2) no single entity has a complete picture of commodity flow, and 3) actions taken by the public sector can both alleviate and exacerbate bottlenecks, CNA has developed a methodology to characterize lifeline commodity networks to inform both public and private sector decision-makers.

Public Health

An Overview of Public Health Assessment Projects in the Commonwealth of Virginia

Eric Trabert

IMM-2025-U-043009-Final

Over the past decade, CNA's Center for Public Health Preparedness and Resilience has conducted several projects focusing on public health service delivery within the Commonwealth of Virginia. These projects have examined a variety of issues ranging from dialysis center preparedness to the adoption of warm zone care best practices during active violence incidents. CNA's team of public health analysts has collaborated with state, regional, and local entities to collect and analyze data and develop practical, outcome-focused solutions to priority public health threats in Virginia.

Dedicated to the Safety and Security of the Nation

About CNA

The CNA Corporation (CNA) is a not-for-profit analytical organization dedicated to the safety and security of the nation. With nearly 700 scientists, analysts, and professional staff across the world, CNA's mission is to provide data-driven, innovative solutions to our nation's toughest problems. It operates the Center for Naval Analyses—the Department of the Navy's federally funded research and development center (FFRDC)—as well as the Institute for Public Research. The Center for Naval Analyses provides objective analytics to inform decision-making by military leaders and ultimately improve the lethality and effectiveness of the joint force. The Institute for Public Research leverages data analytics and innovative methods to support federal, state, and local government officials as they work to advance national and homeland security.

3003 Washington Blvd., Arlington, VA 22201 | Phone: 703-824-2000

CNL-2026-U-045446-Final

cna.org