NEW AMERICA

May 2025

The Future of Deception in War: Lessons from Ukraine

Mick Ryan & Peter Warren Singer

Future Security

Last edited on May 27, 2025 at 1:38 p.m. EDT

Acknowledgments

The authors would like to thank the Ukrainian Armed Forces for their support during multiple research visits to Ukraine and the editorial and publications team at New America and Useful Fiction for their assistance. This publication was funded in part by the Russia Strategic Initiative, U.S. European Command.

Editorial disclosure: The views expressed in this report are solely those of the authors and do not necessarily reflect the views of New America, its staff, fellows, funders, or board of directors. They also do not necessarily represent the views of the Department of Defense or the U.S. Government.

About the Authors

Major General (retired) Mick Ryan is the inaugural Senior Fellow for Military Studies at the Lowy Institute and an adjunct fellow at the Center for Strategic and International Studies.

Peter Warren Singer is strategist and senior fellow at New America.

About New America

We are dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Future Security

Future Security is a partnership between New America and Arizona State University. It reconceptualizes U.S. security policy towards a holistic engagement with current and future challenges including domestic terrorism, armed drones, climate change, pandemics, rising authoritarianism, and new and emerging technologies.

Contents

Contents Cont'd

Executive Summary

Deception—the act of deliberately misleading your foe so that they will take actions that contribute to your own goals—has a long history and enduring value in war. Yet new technologies and ongoing conflicts are reshaping how military deception is planned and conducted.

This report explores the opportunities for and contemporary challenges of conducting the planning, execution, and adaptation of military deception, which have become apparent during the war in Ukraine. As all wars are learning labs of a sort, these lessons matter not just for that conflict, but will have significant impacts on future conflicts as well.

Current U.S. and North Atlantic Treaty Organization (NATO) doctrine provides useful planning principles that inform military deception activities. However, new and disruptive technologies provide both challenges and opportunities for those who practice the art and science of military deception. This report finds that seven key technologies exert such an influence:

- Uncrewed systems;
- Artificial intelligence;
- Additive manufacturing;
- New advanced materials;
- Quantum computing; and
- Commercial sensing and networks.

These technologies are combining with six trends in modern war to drive change in military deception:

- Democratized battlespace awareness and the signature battle;
- New era mass and mobilization;
- Cheaper and more precise deep strike capacity;
- Strategic influence and cognitive dominance activities;

- Ubiquitous air, sea, and land autonomy and human-machine integration; and

- Faster and better integrated adaptation battle.

The convergence of the new technologies and battlefield trends is seeing longer, conventional warfare. Both maneuver and attrition feature in this construct. Concurrently, the massed use of precision munitions—both cheap and exquisite—that are cued from military and commercial sensors has proliferated. This has compounded the challenge for military deception. The military organizations of democracies must act now to improve their planning, conduct, measurement, and adaptation of military deception in this evolved environment, and not to become future victims of it. These include updates and adjustments of command and leadership training, strategy, battlespace operations, personnel systems, military organizational structures, equipment and technology, and doctrine.

We should not deceive ourselves into thinking that we are ready for the deception campaigns of the future.

Introduction

In December 2024, Ukrainian forces planned an attack on Russian positions near the village of Lyptsi in the Kharkiv region that would have been both recognizable and utterly mystifying to prior generations.[1]

Before the attack, drones dropped speakers behind Russian lines that played digital recordings of Ukrainian voices to make it seem like soldiers were present where they were not. Then the force attacked a location the Russians were not expecting and in a form they had never faced before. Dozens of uncrewed ground combat vehicles (UGV) raced out to clear landmines and fire upon the Russian position with machine guns. Overhead, the robotic vehicles were supported by first-person view (FPV) drones, which provided both overwatch and their own attack capability. No humans directly crossed the battle line, and yet the enemy trench section was taken.

In involving a completely robotic attacking force, the Battle of Lyptsi is an important step in the transformation of the character of war from a purely human endeavor into something quite different in the twenty-first century. It also points to how militaries must grapple with how new technologies and trends, especially those emerging from contemporary conflicts like Ukraine, are both reinforcing the age-old lessons of war and updating them.

Drones are used often in modern warfare for reconnaissance.

Source: Melnikov Dmitriy via Shutterstock

Taking your enemy unawares has an enduring value in war, so much that surprise and deceptionare among the foundational lessons for young officers. As the U.S. Army's *Tactics* field manual describes:

> "As a principle of war, surprise is a combat multiplier that amplifies the effects of the other principles of war. Its effective use allows friendly units to strike at a time and place or in a manner that the enemy is unprepared for, which induces shock and causes hesitation. Every echelon works to achieve surprise in an operation and only by multiple echelons working together is surprise achieved. The easiest way to achieve surprise is to use deception. Units throughout history have used deception to their advantage. It is an effective way to cause the enemy to dissipate their efforts and resources. Deception enhances the conditions that allow friendly units to concentrate forces at decisive times and locations. Executing tactical deception comes with costs. These costs include time, material, and risk. However, history shows that executing deception at any scale and echelon is almost always worth the costs."[2]

The reasons for this come down to who we are as humans. Our minds, and institutions, can only deal with so much information at any one time. Individuals in military organizations are thus incentivized to be orderly and generally conformist. As Martin van Creveld wrote, "The history of command

in war consists essentially of an endless quest for certainty—certainty about the state and intentions of the enemy's forces; certainty about the manifold factors that together constitute the environment in which the war is fought."[3]

Yet leaders must operate in an environment that is inherently complex and often chaotic. The complicating factors range from Clausewitz's proverbial "fog of war" to an enemy seeking to foil your every move. So leaders are also encouraged to draw conclusions and act, even on imperfect information. Deception seeks to exploit this paradox. It is ultimately founded on taking advantage of and then reshaping human behavior, decision-making, influence, trust, and the value placed on different kinds of information.

In Western culture, stories about deception extend back to the first epic poems of warfare, such as Virgil's *Aeneid*, in which a large wooden horse delivered to the Trojans as a victory trophy allows Greek soldiers hidden inside to sack the city.[4] Long after these myths were told around the campfires of antiquity, a "Trojan horse" remains a metaphor for many kinds of deceptive behaviors in civil life and military affairs.

Eastern tradition is similarly replete with examples of deception, from antiquity through to the modern day. Sun Tzu in his writings paid particular attention to deception, before and during wars. Notably, he did not see it as an end in itself. Rather, deception was designed to surprise the enemy, and to allow friendly forces to concentrate where they were least expected. But Sun Tzu also warned that friendly forces should "not pursue feigned retreats."[5] He therefore was also concerning himself with countering enemy deception activities. These historical antecedents provide the foundation for approaches to deception operations by the modern People's Liberation Army (PLA).[6] Deception is an important aspect of its information confrontation system, which underpins their contemporary doctrine of systems destruction warfare.[7]

And yet, deception is often undervalued in security studies. Of the literally tens of thousands of open-source reports on lessons from Ukraine, only a handful have explored deception.[8] This information gap is nothing new. In a 2003 report for the RAND Corporation, Scott Gerwher and Russell Glenn wrote that "although the literature on deception in animal biology has only recently emerged from naturalism and become an experimental science, it is richer and more scientifically rigorous than the corresponding literature on military deception. This should not be taken as a criticism of the quality of work on military deception, but rather a comment on its nature: There is relatively little scientific literature on military deception."[9]

As Gerwher and Glenn's report notes, there is a difference between how countries such as China and Russia emphasize the centrality of deception in all forms and levels of military endeavor, and how Western nations integrate deception into military planning. In essence, this has resulted in a "deception

gap" that Western military institutions need to address. Adding to the challenge, much of the literature that provides detailed examinations into deception is focused on pre-twenty-first-century examples. While these are useful in understanding the basics for planning military deception, the literature lacks a broad range of studies relating to twenty-first-century military deception. Providing insights about this gap, and initiatives that might assist in bridging it, is a key driver in the production of this report.

Consequently, the authors of this report have attempted to provide a more rigorous and contemporary focus on military deception while also illuminating potential future pathways for related operational and scientific studies. The project is multidisciplinary in its methodology and sourcing. It incorporates findings from multiple field visits; interviews and discussions in Ukraine and Israel with political and military leaders; documents, including doctrine and field manuals from the United States, NATO allies, and Russia; academic and professional research literature on deception; history studies; and finally, open-source intelligence, including social media posts.

This report builds a picture of what successful military deception might look like in coming decades, addressing the following questions:

- What is the role of deception in warfare?
- How is military deception codified in doctrine, and what are the key principles?
- What are the "maxims" of deception, to perform it well?
- What technological developments affect military deception?
- What are the key trends in military affairs changing military deception?
- What are the key implications of these trends for the U.S. military and NATO?

Chapter I: Deception in War and Key Principles

There are many definitions for deception. The Cambridge Dictionary defines it as "the act of hiding the truth, especially to get an advantage."[10] Nearly all definitions in the literature that explore deception are similar. Donald Daniel and Katherine Herbig describe military deception as "the deliberate misrepresentation of reality done to gain competitive advantage."[11] According to Charles Cruickshank, deception is "the art of misleading the enemy into doing something, or not doing something, so that his strategic or tactical position will be weakened."[12] And in *Strategic Denial and Deception*, Roy Godson and James Wirtz describe it as "a nation's effort to cause an adversary to believe something that is not true."[13]

An effective way to deceive humans is to have them engage in self-deception. As Conrad Crane wrote, "It is easier to deceive us than most of our enemies."[14] Norman Dixon explores this phenomenon in *On the Psychology of Military Incompetence*, describing how interwar Royal Navy battleship advocates disregarded all evidence about the potential future impact of aircraft in the maritime environment. This august group of senior officers needed no encouragement to deceive themselves—and the British government—in their efforts to save battleships.[15] It is a fruitful area of exploration for the conduct of military deception if such behavior can be nurtured in our adversaries.

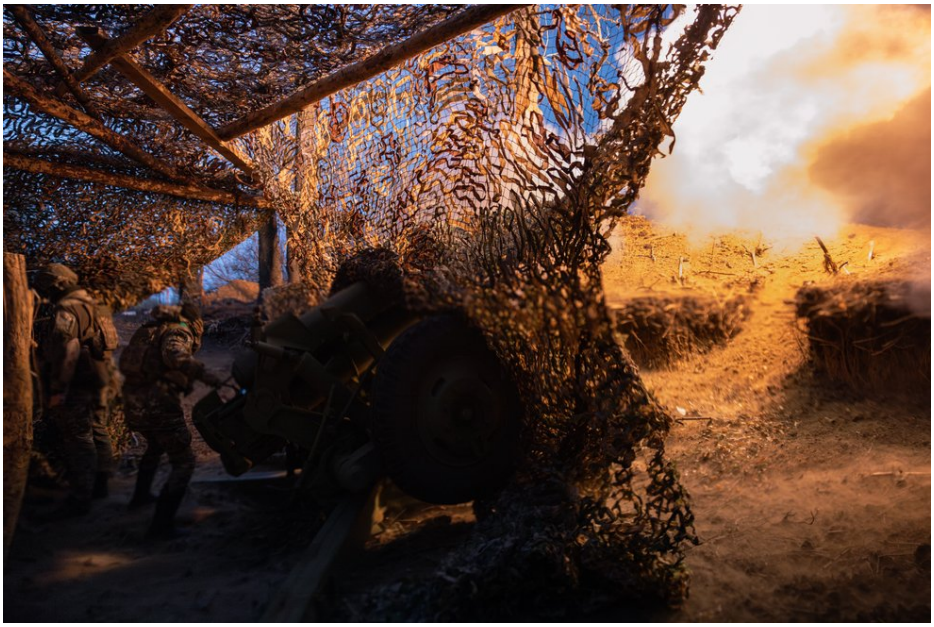
Military doctrinal publications have also defined deception. U.S. Joint Doctrine describes the purpose of deception as to "deter hostile actions, increase the success of friendly defensive actions, or to improve the success of any potential friendly offensive action."[16] The U.S. Marine Corps doctrinal publication on this topic described deception as "the art of convincing the enemy or adversary we will do something other than what we are actually planning to do."[17] Finally, NATO doctrine on military deception describes it as "deliberate measures to mislead targeted decision makers into behaving in a manner advantageous to the commander's objectives."[18]

Russian and Chinese doctrine also emphasizes deception, with Russian deception activities famously encapsulated in the concept of *maskirovka,* the Russian term for "disguise" or "camouflage," which has a larger meaning. As Morgan Maier writes: "Like other complex cultural ideas, Russia's conceptualization of deception defies simple definitions. While the conceptualization of deception in Russia shares similarities to Western thought, it also possesses its own unique characteristics. For the last 50 years, the West has considered maskirovka synonymous with deception. Maskirovka's central theme is the presentation of a believable falsehood to conceal the truth. Maskirovka seeks to create a false reality for the target audience."[19]

The roots of deception in Chinese doctrine reach back to the ideas and writings of Sun Tzu. The enduring centrality of deception in Chinese military thought is embedded in contemporary doctrine. This has been explored in recent reports by the RAND Corporation, the Center for Strategic and International Studies, and the Center for Naval Analyses.[20] These reports explore specific People's Liberation Army (PLA) strategies to manipulate the thinking and actions of enemy forces in different domains. Recent Chinese joint doctrine promotes feints, false signals, and misinformation, ensuring adversaries remain uncertain about PLA intentions. Additionally, PLA Air Force and Navy doctrine stresses the use of decoys, camouflage, and fake communications to mislead enemy commanders.[21] And unlike in Western practice, in Chinese deception, doctrine describes how it is the responsibility of commanders to personally create deception plans, rather than have deception staff officers create them.[22]

The essence of military deception is changing the perception of an enemy commander, by misleading them or reinforcing an idea that is unproductive (or disastrous) for the force they lead. It should either increase ambiguity (A-type deception) or reduce ambiguity by building up attractiveness of the wrong alternative (M-type deception).[23] Deception is thus also an information operation because its aim is to deceive the human mind, the machines that humans rely on, or both.[24]

Codifying Deception



Ukrainian artillery fires while hidden under camouflage netting.

Source: Diego Fedele via Getty Images

Principles for the application of military deception have been derived from the study of military history. Among the scholars who have described principles of deception in the modern era are Barton Whaley in *Toward a General Theory of Deception*, Daniel and Herbig in *Strategic Military Deception*, Jon Latimer in *Deception in War*, Christopher Rein as the editor of *Weaving the Tangled Web*, and Michael Dewar in *The Art of Deception in Warfare*.[25]

Yet the doctrinal publications of many nations reflect Whaley's proposition in his 1969 study on deception and surprise in war: "Deception has been so infrequently or, rather, intermittently and idiosyncratically practiced that it has never gained a firm hold on formal doctrine."[26]

For instance, French doctrine lists the purposes of deception (conceal, divert, and confuse)[27] without providing principles for its employment. The use of deception similarly features throughout the British Army's *Land Operations Doctrine*, although it is not specifically called out for attention, nor are the principles associated with its application by British forces.[28] Likewise, the British joint doctrine on multi-domain operations, issued in 2020, refers to the importance of deception without further expanding on its application in joint operations.[29]

Fortunately, U.S. doctrine stands out for having clear principles for the conduct of military deception. The U.S. joint doctrine on deception[30] and the U.S. Army doctrine[31] list six common principles of military deception:

1. **Focus.** Military deception should target the thought process of the adversary decision maker to cause a desired action. The enemy's intelligence, surveillance, and reconnaissance (ISR) system is normally not the target; rather, it is a means by which deception can deliver information to the decision maker.

2. **Objective.** Deception plans focus actions and resources that motivate an enemy to decide to take (or not to take) specific desired actions. The plan cannot focus solely on motivating the target to believe certain things; it must lead to the target making a specific decision.

3. **Centralized planning and control.** A centralized approach is necessary to avoid confusion, ensuring that various elements portray the same story and do not conflict with other operational objectives or evolving conditions in an operational environment. Execution of the deception may, however, be decentralized if all participating organizations adhere to a single plan.

4. **Security.** Military deception operations require strict security. Successful planners apply strict need-to-know criteria to each aspect of the deception plan. Maintaining the security of the deception means limiting the number of informed planners and participants to those needed.

5. **Timeliness.** A critical aspect of deception planning and execution is appropriate synchronization with the commander's intent and maintaining synchronization during execution. A key challenge is to get the deception target to act in accordance with the deception objective within the timelines required. Friendly deception activities must be completed in a way that accounts for the time consumed by the enemy's intelligence collection and analysis process, the enemy's decision-making process, and the enemy's activity that is to be exploited by friendly forces.

6. **Integration.** Military deception must be integrated at all levels throughout the planning process. Integration also necessitates developing a concept for deception that supports the overall mission. The integration of deception activities begins with planning, continues through execution, and concludes with the termination of the deception.

Coming from an organization trying to bring together multiple national approaches, NATO doctrine on deception is conceptually similar to U.S. doctrine. But it lacks the coordination mechanism inherent in the U.S. military's "centralized control" principle, and it is also more target-centric, dealing almost exclusively with the target and desired outcome. The NATO principles are:[32]

- **Create a behavioral response.** Deception must focus on creating a desired behavior. This behavioral outcome must meet the commander's intent.

- **Reinforce existing beliefs.** Understand what the adversary is predisposed to believe (including how they expect friendly forces to act) and what they are predisposed to disbelieve. It is easier to reinforce a belief than to change it.

- **Target the decision maker.** The targeted decision maker must be able to detect deceptive events, process them, and subsequently act upon them. The decision maker may be at the tactical, operational, or strategic level.

- **Be credible, consistent, verifiable, and executable.** Deception must be:

    - credible in their minds: Is it believable?

    - consistent with the narrative of the operation and the strategic communications framework: Does it make sense in context with what is happening?

    - verifiable by their collection assets in the time required: Can it be satisfactorily confirmed?

    - verifiable by friendly forces collection assets: Can friendly forces collect information to confirm that the enemy is deceived?

    - executable in terms of the actions required over the time period available to do so: Can we actually do this in a timely manner?

- **Use multiple approaches.** Creating effects through joint action will ensure an integrated approach. The greater the number of channels used, the greater the likelihood of the deception being perceived as credible.

- **Conceal the real and reveal the false.** Draw attention away from real dispositions and intentions, while simultaneously attracting attention to false intentions. Alternatives require the adversary to evaluate them.

Military doctrine on deception also recognizes the close relationship between information operations and deception operations. NATO doctrine on deception describes how "Info Ops is the staff function that coordinates information activities to create effects on will, understanding, and capability. To maintain credibility of the overall messaging, the information activities within OPSEC [operational security] and deception plans must be coordinated with Info Ops."[33]

The 2012 U.S. Joint Doctrine on deception also notes that "MILDEC [military deception] and other information operations (IO) capabilities must be planned and integrated to support the commander's campaign and/or operation."[34] The 2022 U.S. Marine Corps doctrinal publication *Information* describes how "deception is an information activity because we endeavor to deceive the human mind, the machine the human relies on, or both."[35]

The 10 Maxims of Deception

While there is a doctrinal foundation upon which military institutions can base their deception activities, there is also a set of maxims that might inform the implementation of military deception doctrine. These maxims were included in the 2019 version of the U.S. Army's doctrine on deception but originated from a Central Intelligence Agency (CIA) research project in 1981, which was declassified in 2015.[36]

These "maxims of deception" help to frame what successful deception operations might look like, and provide a starting point for countering adversary deception activities.[37] The 10 CIA maxims are:[38]

Maxim 1: Magruder's Principle—the Exploitation of Preconceptions

Named for Confederate general John B. Magruder's trickery during the 1862 Peninsula Campaign, it is generally easier to induce an opponent to maintain a pre-existing belief than to present notional evidence to change that belief. Thus, it may be more fruitful to examine how an opponent's existing beliefs can be turned to advantage than to attempt to alter these views.

Maxim 2: Limitations to Human Information Processing

There are several limitations to human information processing that are exploitable in the design of deception schemes—among these, the law of small numbers and susceptibility to conditioning.

Maxim 3: Multiple Forms of Surprise

Surprise can be achieved in many forms. In military engagements, these forms include location, strength, intention, style, and timing. Should it not prove attractive or feasible to achieve surprise in all dimensions, it may still be possible to achieve surprise in at least one of these.

Maxim 4: Jones's Lemma

Named for Professor R.V. Jones, a key figure in Winston Churchill's "boffins" during World War II, deception becomes more difficult as the number of channels of information available to the victim increases. However, within limits, the greater the number of controlled channels, the greater the likelihood of the deception being believed.

Maxim 5: A Choice Among Types of Deception

Where possible, the objective of the deception planner should be to reduce the ambiguity in the mind of the victim to force them to seize upon a notional worldview as being correct—not making him less certain of the truth, but more certain of a particular falsehood.

Maxim 6: Axelrod's Contribution—the Husbanding of Assets

Named for the work of the political scientist Robert Axelrod, there are circumstances where deception assets should be husbanded despite the costs of maintenance and risk of waste, awaiting a more fruitful use. Such decisions are often susceptible to rational analysis.

Maxim 7: Sequencing Rule

Deception activities should be sequenced to maximize the persistence of the incorrect hypothesis(es) for as long as possible. In other words, "red-handed" activities should be deferred to the last possible instant.

Maxim 8: The Importance of Feedback

A scheme to ensure accurate feedback increases the chance of success in deception.

Maxim 9: "The Monkey Paw"

Named for the 1902 short horror story by W.W. Jacobs, deception efforts may play on desire and greed to produce subtle and unwanted side effects. Planners should be sensitive to such possibilities and, where prudent, take steps to minimize these counterproductive aspects.

Maxim 10: Care in the Design of Planned Placement of Deceptive Material

Great care must be exercised in the design of schemes to leak notional plans. Apparent windfalls are subject to close scrutiny and often disbelieved. Genuine leaks often occur under circumstances thought improbable.

Maxims of Deception in Ukraine

There are multiple examples from the war in Ukraine where these maxims have been applied. For instance, Magruder's principle (maxim 1) was employed by Ukraine in the lead-up to the 2024 Kursk offensive. Ukraine sought to reinforce in the minds of the Russians, and Ukraine's allies, that Ukraine was not able to conduct offensive activities at scale. The second maxim, limitations on human processing, is used almost nightly by the Russians as they deploy dozens of decoy drones to overwhelm Ukraine's air defense network and confuse decision makers about actual targets. Multiple forms of surprise, which is maxim 3, are employed in the planning and execution of Ukrainian long-range strikes inside Russia in order to improve the chances of penetrating Russia's air defenses and hitting desired targets. The enduring utility of these maxims is being demonstrated in real time in modern war.

The deception principles and maxims represent the "state of the art" in thinking about planning, executing, and measuring the conduct of military deception activities. The relationship between military deception operations and information operations, described in the more recent doctrinal publications, is also an important consideration in developing a framework for future military deception. That said, reviewing the principles of military deception will be necessary given the impact of new technologies and changes in the character of war explored in the following chapters.

With the fundamental knowledge of deception operations now examined, it is time to turn to an examination of those factors that are driving the adaptation of military deception. First, new and disruptive technologies are impacting the art of deception. Second, a range of trends in wider military affairs will force military institutions to adapt beyond traditional approaches to deception.

Chapter II: Technological Trends and Their Impact on Military Deception

For as long as there have been military organizations, new technologies have shaped and influenced military forces and their operating theories. Since the first industrial revolution, new and disruptive technologies—when combined with new ideas and organizations—have underpinned military revolutions and revolutions in military affairs.[39]

While much may be unpredictable about the future, it is easy to project that future operating environments will be reshaped by the rapid technological trends ongoing all around us in both advanced software and hardware. Adaptive and meshed networks, decentralized command and control, and a vastly expanded ability to gather data all have fundamental implications for the generation and delivery of military capability. Rapid advances in technology allow for an evolved capacity to influence the tempo of military operations, as well as the massed delivery of precision effects, or what Michael Horowitz recently described as precise mass.[40] This is potentially a much more lethal environment for all human combatants, and one where deception has a range of new possibilities and threats due to new and disruptive technologies.

The following technologies are likely to have the greatest impact on the planning, conduct, and evolution of twenty-first-century military deception.

Uncrewed Systems

Military robotics have a wide variety of deception applications, including simulating the presence of real physical or electronic units to misdirect the enemy, undertaking missions with lower detection thresholds, or being deployed in large and disaggregated ways to deceive an adversary about friendly intentions.

Military robots have been used since the First World War and the first remotely operated weapons. However, their use has expanded exponentially during the wars spawned by 9/11. There has been a Cambrian explosion in the development and deployment of uncrewed systems since the start of the Russian full-scale invasion of Ukraine in 2022. Every Ukrainian brigade now has drone companies or even drone battalions, as do special operations regiments. Ukraine has gone from manufacturing just several thousand drones in 2022 to being able to build around 2 million over the course of 2025.[41] Based on its experiences, Ukraine has become the first nation to form an independent drone service, the Unmanned Systems Force, which is an equal counterpart to the Ukrainian Army, Navy, and Air Force.[42]

Robotic systems have particular utility in performing tasks that are dull, dirty, or dangerous, such as contaminated areas; urban, deep sea, and subterranean environments; densely protected military sites; and also more mundane applications such as vehicle maintenance and repair, as well as basic logistics and movement tasks.[43]

Yet their greatest contribution in a wide variety of future military applications will be in human-machine teams (HMT). Human-robot combinations are already proving useful in training establishments to improve outcomes and test best practices in developing human-robot tasking relationships.

The scale of these HMT may be immense. A future joint military task force may comprise several hundred human personnel and several thousand (or even tens of thousands of) robotic systems of various sizes and functions. Many functions currently undertaken by humans might be better performed by robots in human-robot teams.

In turn, this has the potential to reduce the size of many types of military units by hundreds of personnel.[44] The ongoing introduction of military robotics will free up personnel for redeployment into areas where the art of war demands leadership and creativity—enabling intelligence functions, training and education, planning, and most importantly, command and leadership, including deception operations.[45]

The war in Ukraine has also supercharged adaptation with many types of drones, including widespread use of maritime and land drones, development of fiber optic–controlled drones, and the practice of large drones piggybacking smaller ones. The U.S. Army has described in detail such an approach in a 2020 presentation called *Robotic Warfare Battlefield Geometry*.[46]

A significant development in the Russo–Ukraine War has been that while uncrewed systems in intelligence, surveillance, and reconnaissance (ISR) and strike roles have received a large amount of investment, counter-autonomy systems have now moved ahead in a variety of ways. Recent initiatives in Ukraine include drone interceptors[47] and robotic machine guns to shoot down battlefield uncrewed systems, long-range Shahed drones alongside sensor networks, and integrated, autonomous reporting systems to support command and control as well as adaptation cycles. These Ukrainian efforts have been complemented by a range of American, European, and other efforts to develop cheaper ways to bring down enemy drones.[48]

Artificial Intelligence

There are few technologies likely to have as significant an impact on deception as artificial intelligence (AI). Some have speculated that AI may increase the

advantages to those who seek to hide information or physical objects. Using data from their own operations, they can model their own forces comprehensively and then use this knowledge to build algorithms that increase the "fog of war." Those engaged in trying to fight through the fog and friction or war and divine an adversary's location or intentions will be forced to "rely upon noisy, incomplete, and possibly mendacious data to construct their own tracking algorithms."[49]

Future military deception activities will occur at the intersection of behavior and data. Until recently, deception operations targeted the conduct of human military commanders and decision makers. Henceforth, though, state and non-state actors will attempt to target the actions of humans in military systems and the performance of algorithms that support human decision-making.[50] And, with new sensors and networks delivering more data, the ability to search and recognize useful data will move beyond the comprehension of humans. Therefore, AI will be essential to counter deception by the enemy but will also be targeted by the enemy to prevent AI from undertaking this function.

There are multiple functions where AI may extend cognition and enhance military deception. For example, AI has a wide application in large-scale information analysis. It has been widely used in Ukraine for this purpose.[51] It will continue to drive a large variety of autonomous systems on the ground, in the air, and on (or under) the sea. Not only is this relevant in the planning and conduct of military strategy and subordinate operations, but it is also relevant to deception and counter-deception activities.

Generative AI also offers many opportunities and risks. It permits the rapid generation of imagery, text, video, and even music (or equipment sounds) that might be used in military deception. These tools can be used against friendly forces and friendly populations, particularly in spreading disinformation for strategic deception. As a 2024 report from Freedom House found, "Over the past year, the new technology was utilized in at least 16 countries to sow doubt, smear opponents, or influence public debate."[52]

Additionally, new generations of chatbots, such as the DeepSeek-R1 model released in January 2025, offer cheaper and more accessible AI. They might be used for an array of different military applications by potential adversaries, including military deception. A March 2025 report in the *Asia Times* indicates that China's People's Liberation Army (PLA) is already exploring DeepSeek-R1 applications.[53]

The application of AI in military deception comes with risks. There is increasing evidence that AI deceives humans. "Alignment faking"—situations where people appear to share the views or values of others but are in fact only pretending to do so—has recently been observed in AI. A research paper

published in December 2024 found that large language models might also engage in this behavior. As the paper notes, "What if a model, via its prior training, has principles or preferences that conflict with what's later rewarded in reinforcement learning? In such a situation, a sophisticated enough model might 'play along,' pretending to be aligned with the new principles—only later revealing that its original preferences remain. This is a serious question for AI safety."[54]

As a report in *MIT Technology Review* noted, "AI models will mindlessly find workarounds to obstacles to achieve the goals that have been given to them. Sometimes these workarounds will go against users' expectations and feel deceitful."[55] This means that using AI in military operations holds the potential for deceptive conduct by the same decision support tools employed by humans to plan and implement military deception.

Commercial Sensing and Networks

Commercial sensing and communication networks have an important influence on military deception. A range of new terrestrial, space, aerial, and maritime sensors, employed by non-military government and commercial entities, provide near-real-time data that can inform military operations. Networks carry and fuse sensor data used by analysts and commanders. Networks also provide the entry point for those who might wish to interfere with the perceptions of military staff and commanders by inserting false data or cutting off that data altogether as part of a deception plan.

The array of different sensors deployed by non-military entities has continued to expand in the past decade. Partially this has been due to the expansion in the use of drones for applications such as public safety, agriculture, disaster monitoring, traffic observing, and many other everyday functions. Often the data from the sensors mounted on drones is publicly available. But there is a range of other sensors, including acoustic and seismic sensors as well as ocean current and air quality monitoring systems, which might be used in an integrated way to build improved situational awareness for military and other national security endeavors. Finally, advances in passive sensing, which can receive and analyze transmissions such as television or radio signals, add to this complex mix of commercial sensing capabilities.

Space-based technologies are germane to the field of military deception because space-based sensors are now what detect many different kinds of signatures associated with military operations. These technologies underpin connectivity in sensor networks and the rapid communication that can assist in counter-deception activities. They provide a range of detection capabilities that until recently were the preserve of only the most sophisticated and well-resourced military institutions. Detection, and the ability to "see through"

deception operations, is consequently available to nearly every military and non-state actor that might pose a threat to friendly forces.

The magnitude of cost reduction in space access over the past decade, as well as advances in cheaper mini satellites, has driven what has been described as Space 2.0. This shift is accelerating the pace of satellite launches with companies such as SpaceX launching hundreds of satellites to provide global internet connectivity. Its StarLink system, launching 60 satellites at a time on its Falcon 9 rockets, is intended to eventually incorporate a constellation of over 12,000 satellites orbiting at 550 kilometers above the Earth.[56] This system has proved integral to communications and the use of digital command and control systems by Ukraine since 2022. The war in Ukraine has provided such a powerful demonstration of Starlink's applications that China is developing its own version of the system called SpaceSail.[57]

This is both proliferating and revolutionizing space sensing and the ability of more people to access the data from space-based sensors. The kind of data collected, across all spectrums, is presenting unheralded opportunities to industries such as agriculture; energy; mining; sea, air, and land transportation; and entertainment. It also means that both friends and adversaries have the ability to see most of the surface of the Earth if they are willing to pay commercial entities for high-quality imagery and data.

Space denial is also a relevant topic in the context of military deception. The destruction or compromise of satellites and supporting infrastructure may be used by adversaries to deceive friendly forces and generate surprise.

During the Cold War, both the United States and the USSR pursued technologies to destroy or compromise the satellite capabilities of their adversaries. So too, in the twenty-first century, the United States, Russia, China, and India have all tested various forms of direct ascent anti-satellite missile capabilities like anti-satellite rockets.

However, these are expensive capabilities to develop and maintain. Consequently, several nations are developing another method of interfering with, or destroying, satellites: co-orbital weapons.[58] Recently, the U.S. Space Force unveiled that it had monitored Chinese "space dogfights" in 2024, which appeared to be a rehearsal for countering American dominance in space-based sensing in a future conflict.[59]

A simpler approach to space denial was conducted by Russia in the early hours of its 2022 full-scale invasion of Ukraine. The Russians executed a cyberattack that disrupted broadband satellite internet access by disabling the modems that communicate with Viasat's KA-SAT satellite network. This was an important service that provided internet access to tens of thousands of people in Ukraine as well as Europe.[60]

Additive Manufacturing

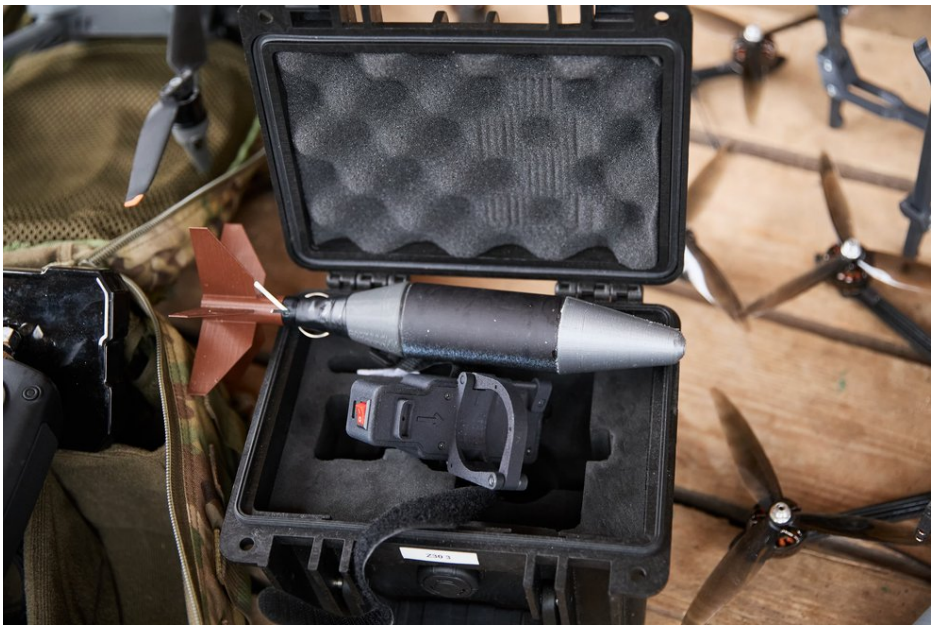
The potential to apply 3D printing to deception operations has been barely examined by most military institutions. However, it offers the potential to reward the imaginative commanders by allowing a more distributed logistics and repair system in the battlespace, and deny an adversary the ability to target large logistic concentrations. But it also offers the potential to rapidly create new camouflage capabilities tailored to the surrounding environment, and to produce dummy equipment or large numbers of dummy emitters to overwhelm adversary sensor networks.

Additive manufacturing, which is also known as 3D printing, is a process for creating a three-dimensional object layer-by-layer, utilizing a design that is generated on a computer. The first patent for 3D printing was filed in May 1980 by Hideo Kodama of the Nagoya Municipal Industrial Research Institute in Japan. However, his process was never commercialized. It wasn't until 1986 when the 3D Systems Corporation developed the first commercial 3D printing system, the SLA-1, which used a method that printed objects layer by layer using lasers.

Additive manufacturing now has significant aerospace, automobile, medicine, and education applications, as well as even home use. In Ukraine, 3D printing has been used for literally thousands of applications, for roles that range from casings for Starlink satellite receivers to drone bomb launching systems.[61] New versions of 3D printing technology are expected to continue advancing in capability and affordability in the coming decades. This will allow the use of new materials, faster production speeds, and lower manufacturing costs.

These advancements offer the ability to produce masses of small, cheap autonomous systems at dispersed locations throughout a military area of operations—or even outside the battlespace—in a way that has a low signature. Future iterations of these printers might also be able to rapidly produce camouflage netting tailored to a specific environment in which a military force is deployed or even produce large numbers of cheap emitters and jammers as part of a deception or spoofing approach.

Therefore, sensors in the future will need to detect not just military systems but potentially low-profile manufacturing capabilities that can rapidly produce or replace lost systems. As with many disruptive twenty-first-century technologies, military and civil institutions have only just begun to understand the impact of 3D printing. Its potential for improved military logistics and reducing the cost of mass-produced complex machines will see it deployed more broadly by military institutions over the coming decades. This has been the case in the Ukraine War.[62] The potential for additive manufacturing as part of a future military deception regime is significant—we just need to imagine more use cases.



An aerial drone bomb 3D printed by Ukrainian Army specialists.

Source: Hurricanehank via Shutterstock

New Advanced Materials

While they have not been deployed in Ukraine as of this writing, two additional technology areas merit mention: new advanced materials and quantum technology.

Developments in manufacturing, civil logistics, construction, automotive, and energy sectors over the past two decades have driven the demand for new types of materials. Generally, materials might be described as new if they are not in wide use, and advanced if their properties are superior to those which they are replacing.[63]

This is relevant to the conduct of military deception because some of the new and promising materials may allow military institutions to develop equipment that radiates less heat or electromagnetic emissions, or that operates on more efficient power sources, reducing exhaust emissions and logistic support needs.

These materials are being developed with the aid of artificial intelligence and machine learning, which has been explored earlier in this report.[64] These processes have reduced waste and produced materials with programmable properties that allow response to external stimuli, as well as lightweight and hybrid materials that provide a range of properties such as thermal shielding or better performance in semi-conductors and energy storage.

While the list of new and evolving materials is extensive, there are several worthy of noting in this study, due to their obvious application to signature reduction and management. The first is metal foam. This is a lightweight, low-density, and large-surface-area material that has potential in noise reduction and insulation. Another new material that offers similar properties is aerogel. It has excellent thermal insulation properties, and in addition, it may assist in energy conservation—a useful property in deployed environments. Other material technologies likely to have application in military deception include thermoelectric energy harvesting, self-healing materials, and graphene and carbon nanotubes.

A final new material worth singling out is metamaterials. These are synthetic composite materials that possess properties not exhibited in naturally occurring materials. There is a wide variety of new and advanced materials that may become crucial in the conduct of military deception. They can be designed to have specific properties, as the materials interact with different wavelengths. As a 2018 report from the Australian Defence Science and Technology Organization notes, "Employing metamaterials to alter how objects interact with the electromagnetic spectrum opens up the possibility of cloaking applications."[65] While often associated with science fiction, metamaterials might allow the coating of objects so that light flows smoothly around the object, effectively rendering it invisible. This application was examined in a 2023 article for the Army Mad Scientist Laboratory.[66] Other possible applications are cheaper synthetic radar sensors and smaller antenna sizes—both with obvious uses in countering military deception.

Quantum Technology

Quantum technology is relevant in the study of military deception because it offers the potential for adversaries to break the encryption systems that protect friendly secrets, including feints and deception activities. At the same time, this technology might be applied by friendly military forces to protect their operational information, including plans, locations, and other elements of friendly information. It is also likely to be suited to solving problems that possess multi-dimensional parameters, which could include breakthroughs in materials science (assisting with signature management), new approaches to machine learning for AI (analytically breaking through deception regimes), and improvements in military logistics (which might assist distributed operations).[67]

All of the potential applications of this technology use several fundamental properties of quantum phenomena. The concept of "superposition" refers to the ability of a particle to exist across all possible states at the same time. Another concept, "entanglement," involves linkage between two or more particles such

that their properties are interrelated. Concepts such as "tunneling," "quantization," and "decoherence" add to the strange properties of quantum mechanics and give them their unique power and potential.[68]

In 2017, China announced a project to construct the first "unhackable" computer network using quantum technologies. This built upon the 2016 launch of a "quantum satellite" by the Chinese in cooperation with European researchers. Other nations have spent decades investing in quantum technology to achieve more cost-effective and secure movement of data.[69] They have done so because quantum technologies have a range of theoretical applications in the future, including secure communications, sensing, and computation.[70]

In October 2024, Chinese scientists reported using a locally designed and built quantum computer to crack military encryption, and they believed it was the first time this had been achieved.[71] Quantum timing and navigation are another potential application with both civilian and military uses. The employment of quantum phenomena may underpin the development of quantum "clocks," which could provide hyper-accurate timing. This would have application in areas such as algorithmic trading in the commercial world to highly precise target location systems in the military world. Such a technology might improve underwater navigation by submarines, improve the precision of weapon systems, and also serve as a useful redundant navigation system should GPS be denied by enemy jamming or spoofing.

The tech industry considers that a million physical qubits (quantum bits, or basic units of quantum information)[72] will be needed on a chip to ensure there is sufficient power to both correct errors and yield a useful quantum computing capability. However a recently announced Amazon computer chip with only 100,000 qubits might offer a useful quantum computing capability, a significant reduction from the previously envisaged requirement of 1 million qubits.[73] Microsoft, taking a slightly different approach, has announced a chip featuring topological core architecture.[74] As Microsoft describes this technology, "The *topoconductor*, or topological superconductor, is a special category of material that can create an entirely new state of matter—not a solid, liquid, or gas but a topological state. This is harnessed to produce a more stable qubit that is fast, small, and can be digitally controlled, without the trade-offs required by current alternatives."[75]

There are a range of other theoretical applications of this technology relevant to deception. One use of quantum technology might be to improve situational awareness through the integration of a vast array of sensors, and the improved accuracy of sensors. As the 2024 annual report to Congress on PLA developments notes, "PRC [People's Republic of China] defense industry and universities are developing quantum imaging, navigation, and radar applications to enhance intelligence, surveillance, and reconnaissance (ISR)

capabilities, including position, navigation, and timing (PNT). PLA leaders view quantum sensing capabilities as tools to improve submarine detection."[76] When such capabilities do become available, and begin to proliferate through government, commercial, scientific, and military institutions, they will revolutionize computing and potentially the conduct of military deception operations.[77]

Technological Advances and Battlefield Lessons

Both warfare and the employment of deception in it continues to be shaped by technological developments and battlefield lessons. This evolution holds the potential to become more striking in the future, as advanced technologies including and going beyond the above both advance and proliferate.

Importantly, these technologies will interact with each other—as well as trends in strategic competition, international relations, demography, and other factors—to force change in how military institutions prepare for and conduct twenty-first-century military activities. These trends in military affairs, and their impact on military deception, are the focus of the next chapter.

Chapter III: Trends in Modern War Driving Adaptation in Military Deception

War is primordial, and its nature remains the same. Yet because of changes in the strategic environment and the impact of new technologies, the character of war—how it manifests itself in the real world—is evolving. This report proposes that there are six significant trends in contemporary military affairs that are not just driving changes in the character of war, but will specifically play a role in an evolved approach for military deception.

Trend 1: Democratized Battlespace Awareness and the Signature Battle

This trend sits at the confluence of three technological influences explored earlier: artificial intelligence (AI), commercial sensing, and uncrewed systems. The significant enhancements in battlespace awareness provided to military commanders by this convergence are perhaps the most important influence on the conduct of military deception.

Every item of military hardware possesses multiple signatures. These might be visual, aural, or in the electromagnetic spectrum. Military units, at different levels, also possess signatures. This can include patterns of operations and exercise schedules as well as indicators for impending military activity. For example, large formations of ground vehicles generate dust, noise, heat, and exhaust signatures that can be detected by a range of different sensors. Individual ships, and naval task forces, generate visual, electromagnetic, sound, and wake signatures. Aircraft and missiles—even those with stealth properties—also have unique signatures that can be detected. Future military organizations must be able to minimize their tactical and strategic signatures, use recorded signatures to deceive, and be able to detect and exploit adversary signatures—across all the domains in which humans compete and fight.

Finally, while each individual person can be seen, heard, smelled, etc., some individuals, such as senior commanders, have more prominent signatures. This might include concentrated communications networks around them or even signature styles of tactical decision-making, as well as individual and organizational patterns that might be identified in operational or strategic decision-making.

The aggregation of all of these kinds of signatures is an ongoing and adaptive signature battle. The technological sophistication of potential adversaries, their mass, and their presence in every domain of war mean that the battle of military signatures will be one of the defining aspects of warfare in the twenty-

first century. Those institutions that can collect information on the various signatures of military organizations and turn this information into timely, actionable products will possess a decisive advantage.[78]

A major shift from the above trends is how signature detection using large numbers of uncrewed systems and commercial sensors has also become more important in military operations, and this was examined in the previous chapter. For example, many commentators and analysts now use the U.S. National Aeronautics and Space Administration (NASA) Fire Information and Resource Management System (FIRMS), freely available online, to assess the level of artillery fire missions in Ukraine.[79] And because Russians have often resorted to insecure communications during their invasion, civilian operators as well as military intelligence agencies have been able to intercept, analyze, and share sensitive military discussions.[80]

Data from civilian technologies can provide a signature that might be exploited by unfriendly actors. The Strava information leak, in which fitness data led to the mapping of several U.S. facilities overseas, is just one example of consumer device signatures having an impact on military activities—and the challenge for military forces to minimize their signatures.

These open-source sensors often use older versions of contemporary military technology. And as the NASA FIRMS demonstrates, these provide only rough approximations of events that might be related to military activity. But intelligence activities—and busting through deception measures—are about assembling multiple layers of information to build a complete picture or hypothesis of what those layers mean. The ability of open-source sensors, often used by civilian intelligence agencies such as Bellingcat, to detect military activity means that military institutions must be even more careful and clever with their signatures in the twenty-first century if they hope to achieve any deception of their foes.

Open-source analytical capacity provides an important way to see more of an enemy operating system and break through their deception systems. It can be the provision of commercial AI and data services to assist in classified analysis, or the blending of commercial analysis (such as the daily reports and analysis for Ukraine, the Middle East, and Taiwan undertaken by the Institute for the Study of War). Perhaps the most promising capacity in the ecosystem of capabilities that make up democratized intelligence is artificial intelligence.

The war in Ukraine has become the first international conflict in which the opposing sides have actively developed and used AI for military purposes. During the war, Ukraine has benefited from allies and partners providing AI technologies. A key element of the war has been the massive amounts of data generated by a plethora of sources. The huge and growing volume of data is larger than humans can analyze quickly and accurately. AI has therefore

become an increasingly useful capability for data analysis to aid Ukrainian and Russian decision-making in this war.

Between 2014 and 2022, Ukraine's tech-savvy workforce developed and introduced multiple new situational awareness and battlefield management systems to the Ukrainian military. Many were unofficial and unsanctioned, but the volunteer groups had direct communication with front-line operational forces, allowing them to focus their development efforts on high-priority military needs.

One of the initiatives, the situational awareness system Delta, was eventually adopted and formally integrated into the Ukrainian military and also achieved NATO certification. Delta has recently been enhanced with AI/machine learning-enabled capabilities.[81] The use of Delta, and the tactical equivalent called *Kropyva*, has now been normalized at every level of military activities in the Ukrainian Armed Forces.

The support for AI development in Ukraine has transformed since 2022. Many government agencies and institutions have shifted from initially neglecting AI to actively creating specialized departments and units dedicated to developing AI capabilities. This transformation has been driven largely by the pressing demands of the ongoing war against Russia, in which AI technologies have repeatedly demonstrated the potential to provide an advantage on the battlefield.

In a recent report from the Center for Strategic and International Studies, Kateryna Bondar explores the expansion of military AI into six major applications:

1. **Autonomy.** The most significant advancements have been in autonomous systems, where Ukraine is making strides in areas such as GPS-denied navigation and swarm operations.

2. **Open-source intelligence and fighting disinformation.** AI helps to analyze large volumes of digital content from media and social networks and to identify Russian narratives, propaganda, and information campaigns spreading disinformation.

3. **Situational awareness and command and control.** AI enhances situational awareness with numerous software platforms used by the military to analyze battlefield and intelligence data and to facilitate real-time, efficient decision-making.

4. **Demining.** AI-powered analytic software and AI-enabled unmanned ground vehicles improve the efficiency and safety of mine clearance.

5. **Training and simulation.** AI-driven training simulations help soldiers adapt to complex battlefield conditions by playing close-to-real combat scenarios with AI adjustments to address warfighters' skill gaps.

6. **Damage assessment.** AI is crucial in damage assessment, utilizing satellite data and drone imagery to analyze damage, losses, and devastation, and to estimate future recovery efforts.[82]

The Russians are equally looking to exploit AI for military benefit. The Russian Ministry of Defense seeks to employ AI to provide data analysis and decision-making capacity to military forces in a "human in the loop" approach to improve the effectiveness of military operations. As Sam Bendett notes in a May 2024 report on Russian AI: "Russian military discourse emphasizes that in the long term, there will be an eventual point where technologies subsume and then replace human involvement in military operations—yet in the near term, Russian military thinking affirms that humans must remain firmly in the loop."[83]

There are five principal implications of this new era's democratization of battlespace awareness and the accompanying signature battle for military deception operations.

First, adversaries may be able to harness advanced sensor networks as well as open-source information that can much more rapidly subvert deception operations. Both Ukraine and Russia have used military and commercial sensor information throughout the war, providing a real-time demonstration of this capability to an array of state and non-state actors globally. Because of this, it is likely that it will be harder to generate surprise against enemy forces. Military organizations will therefore also need to improve their capacity to understand the wide range of open-source sensors and information that is available and develop methods to ingest this, and blend it with military intelligence to include their ability to detect threats and degrade enemy capacity to detect friendly forces.

Second, there has been an increasing use of the term "battlespace transparency" in discourse about the war in Ukraine and future war. This term is being used by lay commentators as well as in professional military forums.[84] While this trend of converging military and commercial sensing and analysis has significantly enhanced tactical visibility of the battlespace, the term "battlefield transparency" is probably an overstatement of what is taking place and sensible skepticism should be applied. There is unlikely to ever be an "unblinking eye" on all human activities and intentions despite the increasingly ubiquitous and pervasive nature of sensors—military and civilian—that mean many military signatures can be detected in near real time. As Ukraine has demonstrated, if the battlefield were transparent, surprise by definition would be impossible. That has not been the case in the past three years.

Third, deception operations are clearly possible despite the enhanced (but not transparent) visibility of the battlespace and the availability of rapid, massed precision-attack capabilities. New types of adaptive camouflage, vehicle shaping, cyber warfare, and interference will need to be developed to counter the new and integrated sensor technologies. At the same time, for effective military deception operations in the technical realm, space-based systems will need to be spoofed, jammed, or otherwise made unable to undertake the sensing and communications that can compromise deception and the generation of surprise (and force preservation) in military operations.

Fourth, such measures can enhance the practice of signature management. Insurgents and terrorist groups in the past two decades have especially learned to mask their various signatures to generate a level of stealth in how they operated, where and when they attacked, as well as their sources of support.[85]

Signatures must not only be detected but also measured and recorded. This can assist in detecting other similar adversary signatures using AI, or in friendly-projecting these signatures to confuse enemy sensors and analytical efforts. At the same time, signature management does not only support tactical deception. Another area requiring attention is strategic capabilities at home bases, military headquarters, and other infrastructure.

Using signatures that cannot be hidden to deceive can also be effective. In the 1973 Yom Kippur War, the Egyptian military successfully convinced the Israelis that their military preparations for war were actually just large-scale routine exercises. The Egyptians created an alternative truth to deceive the Israelis and retain the element of surprise. In 2024, Ukraine did the same by deploying a large number of troops to the Sumy region, ostensibly to defend against a Russian incursion in Sumy Oblast. In reality, this was the assault force that was allocated to strike into Kursk. Accordingly, in a battle of signatures—and application of algorithmic decision support—friendly systems must be trained to smash through deception measures that are provided by well-planned feints like these.

Fifth, despite the importance of technology, the centrality of good training and leadership development processes is even more crucial. The key to military success is generating more uncertainty in the minds of enemy commanders and staff than exists in ours. Humans, and humans supported by improved staff and better AI decision support, are a non-discretionary element of this. The training for commanders to employ and adapt new masking techniques to minimize their potential of detection will be increasingly important in pre-war and wartime activities. As discussed earlier in this report, deception planning in the People's Liberation Army (PLA) is a primary responsibility of commanders, not staff. Consideration of how this might be implemented in U.S. and NATO military institutions is required.

Trend 2: New Era Mobilization and Mass

New approaches to mass collection and analysis of personal information, misinformation and disinformation, manufacturing using 3D printing, and the ubiquity of massed, uncrewed systems across the land, sea, air, and space domains are resulting in a new era of mass warfare. This involves the concurrent use of large-scale conventional forces and massed autonomous systems, and the wide-scale use of influence operations, including sophisticated algorithms.[86]

The rise of unmanned systems has been chronicled elsewhere and is covered in more detail in Chapter II. While debate continues over whether robotic systems will replace or complement humans on the battlefield, military forces are racing to enhance the mass of combat power they can generate through the use of autonomous systems and clever algorithms. In the past three years, this has seen both Ukraine and Russia significantly expand the scope of precision attack across the battlespace and increase its pace.

Future military organizations will need to generate forces with an optimal balance of expensive platforms and cheaper, smaller autonomous systems that will be quicker, more adaptable to different missions, and more widely

available. This balanced force—which generates mass through crewed systems, autonomous capabilities, and influence activities—must be employed using new twenty-first-century warfighting concepts and strategies by people whose training and education feature the integrated application of human and machine capabilities.

Mass influence operations are an important element of the new operational environment. Algorithms, machine learning, and massive datasets can, and do, assist military and government organizations to undertake wide-scale—yet precisely targeted—influence operations in a way that was impossible even a decade ago. This form of mass will continue to develop as institutions learn the lessons of Chinese coercive activities in the Indo-Pacific and the activities of the belligerents in the Russo–Ukraine War, as well as the application of global information operations by terrorist organizations such as Hamas.[87]

As the war in Ukraine demonstrates, the convergence of this trend with the enhanced visibility of new-era meshed civil–military sensor networks means that massing forces can also lead to disaster. This is not a new trend, however. Since the lethality of large military forces began to significantly improve in the wake of the first industrial revolution, military doctrine has emphasized dispersion (and deception) as a response to the more lethal battlespace environment.

The harsh reality for military commanders now is that they face a twenty-first-century massing versus dispersion predicament. The new meshed civil–military sensor frameworks have resulted in an environment where nearly all signatures of military equipment, personnel, and collective forces can be detected more accurately and more rapidly. When linked to the outcomes of the precision revolution of the past three decades, this closes the detection to destruction gap (or kill chain) in military operations to very small amounts of time.

The consequence is that massing military forces for ground combat operations, large-scale aerial attacks, or naval operations has become tactically and even strategically higher-risk than in previous eras. Even if newly developed hard and soft kill measures can better protect forces when they mass for decisive events, they are almost assured of detection, which makes achieving surprise very difficult.

This lesson is driven home by the case of the failed Ukrainian 2023 counteroffensive. It was clear to the Russians, well before H-Hour, the locations where the Ukrainian main effort would fall. As one report notes:

> "At the strategic level, leaks of top-secret information from Ukraine's international partners gave the Russians a precise picture of the Ukrainian assault force's structure, anticipated capabilities,

> limitations, and options for axes of advance. Furthermore, the public messaging from the Ukrainian government, and public discourse from partners, gave Russia a clear understanding of the timing of a likely assault and informed AFRF [Armed Forces of the Russian Federation] planning. Russian penetration of Ukrainian communications systems enabled capture of a range of materials. The result was that when the offensive started, Ukrainian efforts to compartmentalise planning often left friendly forces with less understanding of the wider plan than Russian commanders. The lesson is clear: Future operations must be accompanied by appropriate deception and more effective operational security."[88]

Consequently, the Russians were able to ensure the optimum deployment of their ground forces and fires to blunt the initial Ukrainian attacks while permitting their forces more freedom of action elsewhere. This represents a signature battle and is a critical aspect of this operational problem. In essence, modern military forces must be equally capable of operating in dispersed and massed forms, but they must be able to minimize detection of when they do mass in a way that provides an improved chance of surprise and landing a decisive blow against an adversary.

This has multiple implications for the conduct of military deception operations:

First, the mass use of drones and other sensors, as seen throughout the conflict in Ukraine, has saturated the battlespace. This means that concentrations of military forces are difficult to hide, as are their support systems, such as logistics, transport networks, and communications networks. One of the Russian responses to this environment is the use of smaller tactical teams to conduct infiltration tactics at unit boundaries and during unit rotations by the Ukrainian ground forces. It is not fool-proof but is successful enough given the current disparities in manpower.[89]

Second, the use of technologies such as additive manufacturing (at home and in the field) may permit the rapid construction of dummies and decoys for use to saturate enemy sensors. This might include clear, plentiful emitters that replicate and saturate the enemy's capacity to undertake electronic warfare activities. While such technology has not been widely used in Ukraine, it offers one potential pathway for deployed deception operations in areas where there is no ready access to local industry to construct decoys.

Third, technologies to spoof enemy sensors and databases about friendly locations and intentions are crucial. This includes the mass production of noise to overwhelm enemy counter-deception measures, like the use of chaff to confuse enemy air defense systems in the Second World War as well as in the modern recent Gulf Wars and Ukraine. It will also probably demand the wide-

scale deployment of decoy drones to overwhelm enemy sensor systems during strike operations. Both Ukraine and Russia have employed this technique to improve the chances of penetrating sophisticated air defense systems.[90] To complement these decoys, the mass application of cyber capabilities and AI might be useful to detect and interfere with sensors and the networks that transmit data about friendly-force locations.

Fourth, the ability to disperse, concentrate, and re-disperse is critical to deception. Not only does this confuse an adversary about the direction from which a physical main effort might emanate, but it also makes the identification and destruction of high-value military targets a more difficult (and time-consuming) undertaking. The Russians, after the hard lessons of the introduction of high mobility artillery rocket systems (HIMARS) in 2022 and the targeting of their Black Sea Fleet, have adapted to implement more dispersed concepts of operations on the ground and at sea over the past three years. The concept of distributed operations, which has been explored by several Western military institutions, is crucial to dispersion and is explored in the final chapter of this report.

Trend 3: Cheaper, More Precise Deep Strike

Long-range strike has been a key development for the Ukrainian Armed Forces, as well as military and non-state actors in the Middle East, over the past several years. Beginning the war with almost no capacity to hit Russian strategic targets, the Ukrainians have demonstrated an evolved approach to long-range strike that embraces a high-end/low-end mix of weapons and combines foreign and indigenous solutions. This strike capability has been constructed from a combination of ground-based rocket launchers, armed drones, cruise missiles, and uncrewed maritime strike vessels. This long-range strike complex is not just a military capability—it is a political necessity.

The development of a lower-cost strategic strike complex in Ukraine and elsewhere has been underpinned by the technological influences of uncrewed weapons' availability and cost, as well as meshed military and civilian sensor networks.[91] A good example of a new long-range strike capability is the Ukrainian 14th Unmanned Aerial Vehicle (UAV) Regiment, which is part of the Unmanned Systems Force. It conducts strikes, employing integrated planning from a range of military and national intelligence organizations, at ranges out to 2000 kilometers. Potential adversaries will have increasing access to a wider range of long-range systems over the coming decade.

This lower bar for strategic strike capacity is forcing a new conversation among the most senior military and political leaders about what is the appropriate balance of long-range strike and close combat capabilities. Many nations have begun to increase their investment in longer-range strike systems. While long-

range strike capabilities are important components of the arsenals of military institutions, they are not a silver bullet.

The planning, conduct, assessment, and adaptation of long-range strike across domains must be carefully balanced with investment in close combat and other capabilities. There are several reasons for this. First, it forces adversaries to make difficult choices about the array of military capabilities to develop and deploy, generating uncertainty. Balancing between the deep and close fights also provides redundancy in conventional deterrence systems. An enemy might be able to penetrate a long-range strike complex but may still have to close with a fight in combat. Not every nation wants to do this. And as Israel discovered on October 7, 2023, placing too much emphasis on remote, long-range recon-strike complexes and insufficient emphasis on close combat capacity can lead to devastating failure.

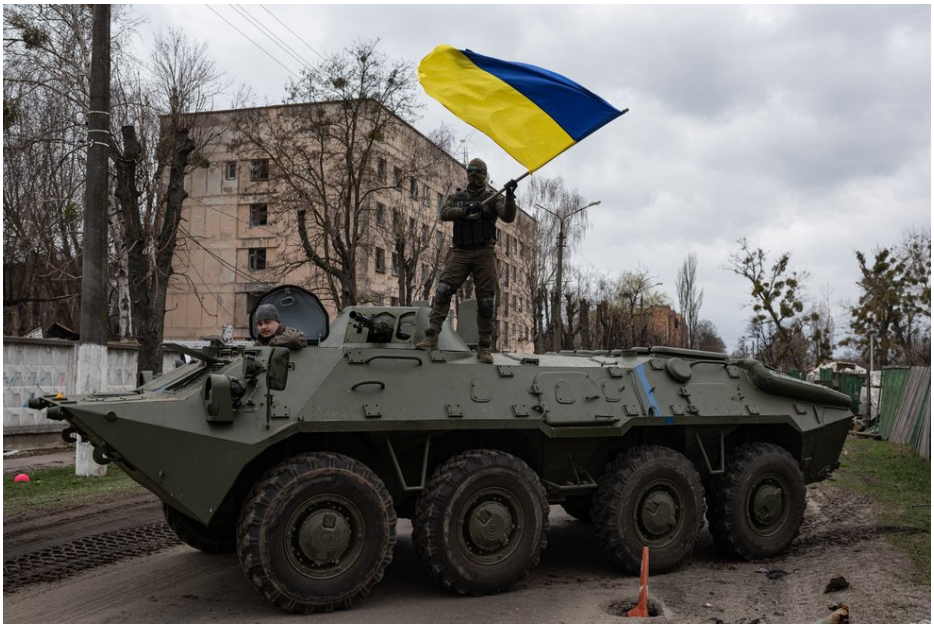
The wide availability of long-range strike capabilities among state and non-state actors has the following implications for military deception:

First, Ukraine has reinforced that deception is a necessary part of strike planning and execution. Route planning for weapons, as well as for preparatory intelligence collection, must deceive the enemy about likely targets, which will then influence their deployment of anti-drone and missile sensors and attack systems. Decoys during the execution of strike operations are critical, and this has been a feature of nearly all Ukrainian and Russian strike operations in the past couple of years.

Second, deception is key to protecting strike infrastructure. While the obvious challenge is to ensure an enemy cannot strike and destroy storage depots for munitions and delivery platforms, key planning staff locations must also be protected and potentially included in deception plans. This might involve operations to degrade the capacity of enemy sensors to collect imagery and other information for target mensuration. The Russians, for example, commonly use smoke and mist generators to degrade satellite collection of imagery over critical infrastructure in Russia. They, and the Ukrainians, also frequently move air defense units to improve their survivability and complicate strike planning for their adversaries.[92]

Finally, delivery of new weapon systems during wartime should also be accompanied by preconceived deception and operational security plans so that the adversary cannot prepare counters before the systems are used. This was the case for the arrival of ATACMs (army tactical missile systems) in Ukraine in 2023, which led to several important strikes on Russian force concentrations that did not realize they were at threat of such strikes.[93]

Trend 4: Strategic Influence and Cognitive Dominance Activities



A Ukrainian soldier waves the Ukraine flag during Russia's invasion attempt in 2022.

Source: Alexey Furman via Getty Images

War has always possessed a complex balance of physical, intellectual, and moral forces.[94] Influencing the thinking and actions of enemy commanders, and political leaders, is as old as war. Winning war in ancient times and in the modern era is about *winning the war* and *winning the story of the war.* Actions that are undertaken as part of influence activities before and during war include disinformation, and—importantly for our purposes here—military deception.

Disruptive twenty-first-century technologies have not only enhanced the lethality of military forces at greater distance, but they also now provide the technological means to target and influence various populations (enemy and friendly) in a way that has not been possible before. The ability of modern states, corporations, and non-state actors to devise and test strategic messages —targeting different groups with different narratives—through the internet and social media, adjust those messages, and access hundreds of millions of users almost instantly is unprecedented. Leaders, their advisors, military service members, and civilian populations can all be targeted in manners both directed and at scale.

Social media has revolutionized global communication, social interaction, marketing, and professional discourse. It has demonstrated a capacity for penetration and influencing perceptions of humans that is historically unprecedented, particularly when compared to other means of communication.

Social media is also dissimilar from other forms of media because of two principal reasons. First, social media is viral; users are both targets and also potential fellow combatants who can be enlisted into sharing content across their own social networks. As the 2018 book *LikeWar* proposes, "You are now what you share."[95]

Second, social media users with smartphones are media consumers who are highly mobile and increasingly omnipresent in most settings.[96] As of January 2025, just over 63 percent of people worldwide are classified as social media users, and social networks are either the most or second-most visited types of sites for every age group between 16 and 64.[97] Although there are limitations placed on content in many countries—China has a state-of-the-art censorship regime—even authoritarian nations like Russia and China have their own versions of social media, which are often used as tools of influence by the state and corporations. These regimes have become experts in leveraging social media to spread disinformation and undertake external influence campaigns. [98]

As the war in Ukraine has demonstrated, the "influence playing field" is not entirely dominated by authoritarian regimes. In the lead-up to the invasion of Ukraine on February 24, 2022, U.S. intelligence agencies were able to use sensitive sources and reporting to not just discover but also attempt to preempt Russian operations.[99] These releases of information discredited Russian narratives about the war, crowded the information space to degrade the impact of Russian influence campaigns, and directly assisted the Ukrainian development of military strategy to defend their nation.[100] Once the war began, President Volodymyr Zelenskyy masterfully leveraged social media to ensure his nation received military, economic, intelligence, political, and humanitarian aid from the West.

Influence activities undertaken by the Russians, as well as other state and non-state actors, have also had a significant impact on the war. Social media, and its attendant influencers and podcasters, had an impact on the congressional debate over American support for the war in 2024. Several podcasters in the United States were indicted for supporting Russian propaganda activities in September 2024 to influence American opinion on the war and voting in the 2024 presidential elections.[101]

The effect is also shaping the reporting and perception of war. The rise of citizen social media war commentators began to emerge more than a decade

ago, as was noted in a 2013 paper titled "The New War Correspondents."[102] But there has been an explosion in this approach during the Russo–Ukraine War. Hundreds, if not thousands, of online commentators—some well-credentialed and experienced, some not experienced at all—have gained a high level of influence among populations in Russia, Ukraine, and many Western nations. Analysts have developed sophisticated mapping products to track progress in the war and have shared countless numbers of images and videos, which all exert some level of influence on those who view them.

This has been a role traditionally reserved for a small number of specialist journalists, otherwise known as war correspondents. The older generation of war correspondents has adapted quickly, combining their traditional reporting approaches with the exploitation (and verification) of social media geolocation and other data to report on the war.[103] But because of the demands on rapid reporting, over-reliance on social media information (which is more difficult to verify and very open to lies and deception) is a risk for policymakers and senior military leaders. As one report on the use of social media in Ukraine notes, "We're still working out just what 'truth is the first casualty' means in the social media age. It's no longer the case that the truth just isn't out there, or that it's only available pre-glossed with propaganda. It's that there's too much information."[104]

The influence of generative AI is also reaching the war in Ukraine and the conduct of deception operations. Deepfake technologies can be employed to generate fake news and fake videos of credible spokespersons, with the aim of degrading trust in politicians and government-provided information about the war. At the same time, as a recent *Lawfare* article notes, deepfakes can cause a "liar's dividend," where those confronted with evidence of corruption and abuses of power can sow uncertainty and avoid accountability by saying, "It's fake."[105]

While China and Russia have demonstrated an advanced capability to undertake strategic influence operations, the recent war in Ukraine demonstrates that it is possible for democracies to also generate strategic influence. This can be done by military and government institutions, from professional and amateur war correspondents. War and competition in the twenty-first century will see an increasingly sophisticated approach to influence operations—at every level—and an increasing quantity of them.

A final element of this trend is the increasing attention being paid by military institutions to cognitive warfare, a concept with growing relevance in the modern security environment. Enemy states seek to continuously undermine the integrity of political processes in democratic societies, as well as related military-strategic aims, through the application of integrated strategies that coordinate political, military, economic, and information activities.[106]

It is important to draw a distinction here between traditional information operations and cognitive warfare.[107] As Christoph Deppe has written, "Whereas information warfare centers on controlling the dissemination of information, cognitive warfare strategically aims to shape and manage the reactions of individuals and groups to that information."[108]

It is an approach that China has been studying for some time. The most recent report from the U.S. Department of Defense about Chinese military capability notes that: "The PLA concept of cognitive domain operations (CDO) combines psychological warfare with cyber operations to shape adversary behavior and decision-making. Since at least the mid-2010s, the PLA has been incorporating the concept of cognitive warfare or CDO into PLA frameworks for conducting influence operations. While the concept of cognitive warfare appears to be a PLA-specific, overall PRC [People's Republic of China] influence operations reflect a whole-of-government approach to shaping the information environment."[109]

The efforts described in Chinese literature as cognitive dominance operations have the purpose of achieving "mind dominance." Given that the primary objective of military deception is to influence how enemy decision makers think, the concept of cognitive warfare is likely to play an increasingly important function in planning and achieving military deception aims. Building a capability for implementing this approach to war has seen China invest in a range of human sciences, as the 2024 Pentagon report notes: "The PLA is exploring a range of 'neurocognitive warfare' capabilities that exploit adversaries using neuroscience and psychology."[110] But it also uses new technologies such as AI, social media, and deepfakes as well.

Russia has also invested in cognitive operations. As Dima Adamsky describes in *The Russian Way of Deterrence*, Russia's operations in the information sphere have traditionally been divided into cognitive-psychological (CP) and digital-technological (DT) activities, but there is an increasing convergence of the two forms of operation. The aim of these activities is to achieve "informational deterrence," and in a term used by Adamsky, the achievement of "cumulative coercion."[111]

One of the most chilling possibilities with this approach to warfare is that potential adversaries might be able to entirely circumvent military operations by using cognitive warfare to coerce entire societies into believing that either war is not possible to win or that their nation has no interest in challenging the strategic objectives of an adversary state.

While mass, precision-strike, and meshed civil–military sensor networks are crucial elements of contemporary warfare, the ability to influence and shape decision-making at all levels is also critical. This has been accepted by many Western military organizations, and some of the leading work done outside

China and Russia is undertaken at the NATO Allied Command Transformation organization. It has developed a cognitive warfare concept, explaining "cognitive" as referring to "the mental action or process of understanding, encompassing all aspects of intellectual function, including the subconscious and emotional aspects that drive a majority of human decision-making."[112]

But in Western military organizations, cognitive warfare still presents multiple challenges. While it may provide military and national security decision makers with a method to navigate the complexities of modern warfare, it may also require new methods of recruiting, training, and developing individuals and evolve how strategic and operational planning is conducted. Importantly, the assessment of strategic risk and opportunity in these kinds of operations in Western military organizations remains underdeveloped.

Military deception is an important component of contemporary strategic influence and cognitive dominance operations. The application of military deception seeks to influence the thinking and decision-making of enemy leaders. Consequently, the interaction of strategic influence, cognitive dominance activities, and military deception has the following implications:

First, cognitive warfare is likely to increasingly influence the planning and conduct of military deception and will eventually become the principal influence in these activities. Further work to develop the concept of cognitive warfare is required, as is research and doctrine development on the role of cognitive warfare in the conduct of military deception.

Second, the pervasiveness of social media users in many of the environments in which humans will fight means military commanders and planners must incorporate the threats and opportunities of social media into planning processes. Assumptions must be made in formal planning and decision-making about the level of visibility that social media might provide over military operations, and the levels of deception that might be required to prevent or minimize it. The war in Ukraine has probably been a peak in social media commentary about any single war.

Citizen commentators and influencers are now a prolific, constant presence in national and global discourse and the battle of ideas. The opinions of social media commentators, regardless of their expertise, can shift opinions in portions of the less-informed citizenry of democratic and authoritarian nations alike. These commentators can be deceived, however. In addition to the rise of citizen war correspondents using social media, there has been an emergence of curators. As "The New War Correspondents" notes, "People have taken the role of both aggregating and disseminating information to a large number of people in the city who follow them and who even send reports to them."[113] Further study of this phenomenon and its application for military deception operations might start with these curators and super-aggregators.

Third, the application of deepfakes by potential adversaries could impact the credibility of national leaders, and their communication with their citizens, in situations of competition and conflict. The Russians, early in this war, attempted to use a deepfake of President Zelenskyy surrendering to influence opinion in Ukraine and among its supporters.[114] In 2023, Russian President Putin even addressed a deepfake version of himself at an event in Russia.[115] The use of advanced AI to create these will necessitate counter-deepfake technologies in military and other national security institutions to ensure that flooding the internet with deepfakes doesn't impact the "cut through" of actual national strategic messaging and subsequently dissuade populations from supporting national competition or war efforts.

Finally, given the propensity of potential adversaries to engage in deception, the conduct of counter-deception operations must assume a more central place in military operations. The capacity to recognize adversary deception mechanisms must be enhanced if the ability of authoritarian regimes to bluff and deceive democracies is to be degraded.

Trend 5: Ubiquitous Air, Sea, and Land Autonomy and Human-Machine Integration

An important principle in the design of future military organizations is to augment human physical and cognitive capabilities to generate greater mass, more lethal deterrent capabilities, more rapid decision-making, and more effective integration in the battlespace. At the same time, the marriage of human and robotic/algorithmic capacity might also result in more efficient training and education; improved strategy development; better development, execution, and measurement of influence campaigns; and better experimentation and testing of future force models, battlefield options, and other institutional challenges.[116]

Robotic systems, big data, high-performance computing, and algorithms are already being developed and deployed by military organizations in increasing numbers. Recently, the application of autonomous systems within existing human organizations and tactical approaches has been seen in Ukraine and Israel. From its drone operations, Ukraine has amassed a huge trove of video data, which is now being applied to train AI targeting algorithms to improve the success rates of drone strikes on the battlefield.[117] Ukraine has also been employing AI for imagery analysis in strategic intelligence organizations, although, as the Chief of Ukraine's military intelligence General Kyrylo Budanov has made clear, it still requires improvement.[118] Israel, on the other hand, appears to have advanced even further. Before its war in Gaza, it developed AI models, called *Habsora* (the Gospel), which were able to rapidly generate hundreds of additional targets compared to human targeting processes.[119]

It is also apparent that both Ukraine and Russia are using humans teamed with algorithms in their domestic and international influence campaigns. These are activities that, because of their scale and sophistication in targeting, require both human inventiveness and machine power for generating mass influence. [120]

It is important to note that these new and disruptive autonomous systems (robots) and algorithms (AI) will not just be tools used by humans. In many cases, these technologies might act as full partners of human beings in the conduct of military missions. This will necessitate a change to many of the extant training and education philosophies in military organizations.

First, the marriage of human ingenuity and creativity with robots and algorithms in places like Ukraine, Russia, and Israel in the past three years portends significant improvements in the speed and quality of decision-making in future operations; this includes deception and counter-deception activities. The advantages of this approach will accrue to both friendly and enemy forces.

Second, the marriage of human and algorithmic cognitive abilities might be leveraged to develop more sophisticated (and possibly creative) approaches to military deception operations as well as the conduct of counter-deception activities against adversaries.

Trend 6: Faster and Better-Integrated Adaptation

Frank Hoffman proposes in *Mars Adapting: Military Change During War* that "the ultimate test of military preparation and effectiveness does not end once a war begins. On the contrary, history strongly reflects the enduring phenomena of learning and implementing change during war as well...The requirement that

a force must adapt while it is in combat is built into the inherent nature of war."[121]

Adaptation is a device to build advantage in many areas continuously while constantly negating enemy advantage. The possession of a systemic, strategic, and well-led approach to adaptation is something that can give a nation, or alliance, greater power in both peace and war. At the same time, it is something that can be used against friendly forces to devastating effect if they don't understand it or don't make efforts to degrade our enemy's ability to learn and adapt.

Since the beginning of the large-scale Russian invasion in February 2022, the most important individual and institutional behavior for Ukraine and Russia has been their ability to learn and adapt. This is an interactive fight because each side is learning based on the reactions of their adversary and then finding and implementing solutions to improve their effectiveness against that enemy. This process, which can be described as the Adaptation Battle, occurs at the tactical, operational, and strategic levels.

Adaptation has taken place in both the Ukrainian and Russian military institutions during the war. This adaptation has changed the structure, tactics, and training of both organizations, and they are both different military institutions now if compared to the Ukrainian and Russian military institutions that existed before the Russian invasion of 2022.

It has also taken place at multiple levels in both military institutions. Adaptation is not a singular or holistic process that takes place at one level of an institution. In any military institution, there will be multiple instances of adaptation occurring at any one time, and these will generally be occurring in different geographic areas (depending on threat) as well as at different levels within the hierarchical construct of a military force.

The effectiveness of adaptation that occurs in war, however, relies at least partially on the quality of pre-war foundations. While adaptation that occurs in combat is a natural reaction for military personnel who wish to "survive the next battle," wider-scale adaptation can be more effective if there are pre-existing processes and cultures for learning and sharing lessons within and between institutions. The possession of an institutional learning culture and an agreed method for learning and sharing lessons can ensure that once battlefield lessons begin to flow during wartime, there are ready pathways for ensuring that these lessons can be employed to improve training, education, tactics, strategy, equipment, and alliances to improve the overall military effectiveness of an institution.

There is a relationship between adaptation and deception in at least two areas.

First, the speed of planning, decision-making, action, and assessment in many forms of military operations is increasing. Ukrainian battlefield commanders now describe an adaptation cycle on the battlefield, seeing drone ops evolve every two to three weeks and Russian ground tactics evolving every two to three months.[122] This is an outcome of the effects of hypersonic weapons, the potential for AI to speed up decision-making at multiple levels of command, and the increasingly rapid media cycles that influence political decisions. This also means an adversary will seek to speed up its learning and adaptation to overcome friendly forces' efforts to generate a tempo of operations that overwhelms their decision-making capacity. Deception can play a role in slowing down the ability of the enemy to learn about friendly intentions, posture, locations, and capabilities, and therefore have an impact on their adaptive cycles.

Second, deception might be deliberately injected into enemy adaptation cycles. As Scott Gerwehr and Russell W. Glenn note in their 2003 report *Unweaving the Web*, "Covert/clandestine or other actions taken to introduce errors into the innovation process may significantly hamper adaptation." Multiple actions might be part of this effort, including disinformation that is communicated to the enemy that purports to reveal a technical or tactical vulnerability. Or enemy deception measures may be allowed to go unchallenged to permit replication of the bad to hinder adaptation and provide friendly planners with a targetable vulnerability in the enemy system.[123]

For example, Ukraine injected fake stories about the reasons for the deployment of forces to Sumy in early 2024, and about its inability to generate an offensive operation in 2024. This meant that the Russians focused on adapting to Ukrainian defensive initiatives in the eastern front and not in the northeast in Kursk.

Before undertaking deception activities to interfere with enemy adaptation processes, an assessment would be required to gauge just how good we are at learning and adaptating at the tactical and strategic levels. While Gerwehr and Russell propose one model in *Unweaving the Web*, other models might be more appropriate in the circumstances faced by NATO forces in Europe.

In a recent discussion, a Ukrainian senior officer who just completed four years in command of a tank brigade offered that his Russian enemy has become very good at deception. It is a rapidly evolving field, and what worked a year ago does not work now. He noted that while some commanders on both sides are poor at military deception, it is a crucial idea in how the Ukrainian Armed Forces operate. He paraphrased Sun Tzu in describing how Ukrainians think about deception: "If you are weak, make the enemy think you are strong." For Ukraine, this has cognitive and technical elements.[124]

The rapid pace of learning and adaptation in modern operations has the following implications for the conduct of deception operations:

First, the rapid pace of adaptation in modern tactical operations will have an impact on measuring the success or failure of deception operations. The Ukrainians, Russians, Israelis, and Hezbollah have all demonstrated this faster learning and adaptation trait in the past three years, and it should be assumed that this is the new pace of learning for any adversary we face. Consideration should be given to rapid-assessment methodologies that enhance measurement of the impact of deception, and these might then be leveraged for measuring the success and failure of medium- and long-term deception activities.

Second, another implication of the quickening pace of tactical operations is that there will be minimal time for separate or sequential planning activities for supporting plans such as deception. Therefore, deception planning must be integrated fully within normal tactical planning processes.

Third, the shortening of the detection to destruction timeframe, as evidenced from the Russo–Ukraine War, increases the imperative for deception and concealment operations. It will demand the seeding of the battlespace with more dummy targets—including physical decoys and fake networks—than an adversary can deal with.

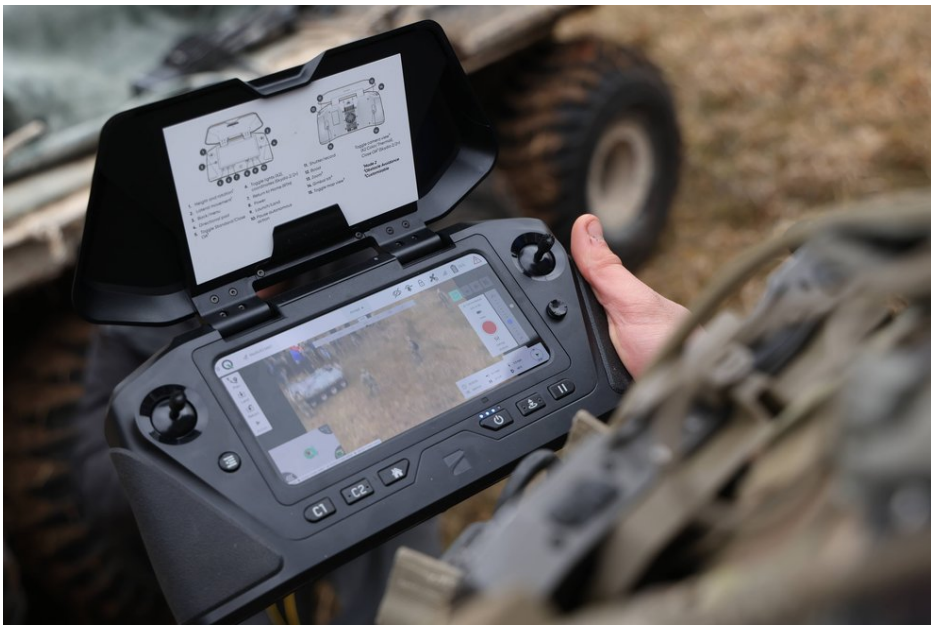
Fourth, for strategic deception operations, these may take months or years to come to fruition. Building a culture of strategic patience in both political and strategic military leaders will be critical to the success of such deception activities.

Finally, contemporary military deception activities will demonstrate their own learning and adaptation cycles. Both Ukraine and Russia have learned this lesson during the past three years, with one example being that placing decoys alone no longer works. They must be accompanied by fake heart sources, periodic transmissions, and track marks to and from the decoy. This constitutes a deeper level of investment in deception and must be integrated into broader institutional learning and adaptation systems.

Adaptation is important for the cognitive aspects of war. It underpins learning about enemy misinformation and the impact it is having on friendly populations and political systems. Adaptation is crucial not just to winning the war, but also to winning the "story" about the war. It is also vital for military deception operations. As the next chapter describes, military organizations have a range of areas where they will need to adapt in order to be successful at military deception operations in the coming decades.

Chapter IV: Building Enhanced Military Deception Systems

As was highlighted in the introduction to this report, the difference in emphasis for military deception between nations such as Russia and China and Western military institutions has led to a modern "deception gap" that needs to be addressed. Recent technological developments, including ubiquitous uncrewed systems, commercial sensing technologies, and artificial intelligence (AI) have exacerbated this gap. This section of the report therefore provides a summary of implications and potential remedies to close this gap in military deception with adversaries during the conduct of twenty-first-century operations. The implications and solutions cover the following thematic areas: (1) command and leadership, (2) strategy, (3) battlespace operations, (4) personnel, (5) military organizational structures, (6) equipment and technology, and (7) doctrine.



A drone operator with the U.S. Army 3rd Brigade performs a military training exercise near Hohenfels, Germany.

Source: Sean Gallup via Getty Images

Command and Leadership

During a recent research visit to Ukraine, a brigade commander who had commanded a tank brigade since the beginning of the war explained that

"deception is a central part of Ukrainian planning and can't be added on after planning for operations is complete."[125] Evolving an institution's approach to military deception demands advocacy and leadership from the highest levels. If a fundamental level of reform in thinking about military deception is desired, an explicit strategy with clear purpose, vision, priorities, and resources may be required. Changes must be explained (frequently) and experiments conducted to validate both the reasons for change and the directions to be taken in enhancing the institutional capacity for military deception.

Such a strategy might also be the opportunity to provide a clear statement of an institutional vision that inspires an organization's members to stretch their expectations, aspirations, and performance to achieve its mission. It provides the people in a military organization with purpose and gives their work a unified guide to action.[126] Such a strategy for improving military deception might also address the recommendations and initiatives that are proposed in the pages that follow.

Deception and surprise are thus an important element of command. As such, there must be a high level of advocacy for, and emphasis on, achieving surprise through deception by senior military leaders. Importantly, there must be a spokesperson for change. This was a key finding of General Don Starry in his examination of institutional change in the U.S. Army in the wake of the Vietnam War. This principle holds true for most military institutions that contemplate change. Whoever the spokesperson is, they must build a consensus that will give the new ideas about deception, and the need to adopt them, a wider audience of converts and advocates.[127] This also appears to be a crucial function of Ukraine's new Chief of the Unmanned Systems Force, Colonel Vadym Sukharevskyi. One of his key functions is the advocacy for the use of drones, but more importantly, for the cultural and organizational changes required in all elements of the Ukrainian Armed Forces that are driving enhanced strategic and tactical effectiveness through use of a wide variety of uncrewed systems.[128]

At the same time however, deception operations hold the potential to challenge civil–military relations in democracies that value transparency and accountability in all arms of government. To that end, the most senior military leaders may need to hold discussions with political leaders on the rationale for deception operations and to ascertain the legal and ethical limitations that might be placed on the conduct of military deception operations.

Senior military leaders need to be educated in the various aspects of signature management, measurement, and projection as a part of military strategy as well as operations. They should further be incentivized to include deception operations and outcomes in all command-intent statements when dealing with an adversary (doctrinal evolution is related to this). Senior leaders will need to

be educated in the art of perception management for use in deception operations.

As military deception is focused primarily on changing the perceptions of adversary leaders, adapting the conduct of deception must focus on the education and development of friendly senior military personnel, as well as other national security leaders. Talented future leaders must be given the opportunity to not only lead but to practice the art of influence—it is an important way to shape the perceptions of others. Making senior leaders use social media frequently is one very easy way that NATO might be able to hone this art of influence in its personnel. But literacy in the psychological underpinnings of perception management might also be incorporated into respective professional military education systems, or in external educational opportunities.

All likely adversaries are likely to practice deception. Indeed, Russia has a long history of such activities. This leads to a finding that friendly forces must not only embrace a culture of deception but also pierce enemy deception regimes through the practice of counter-deception. In his book *The Art of Deception in Warfare*, Michael Dewar notes, "To counter the deceiver, one must also study him in depth...counter deception involves microscopic analysis in order to discover the minutest inconsistency, but it also involves a macroscopic appreciation of the enemy's fears, aims, prejudices, and habits."[129]

Counter deception is also included in the 2012 U.S. joint doctrine on military deception, which defines it as follows: "Counter deception contributes to situational understanding and IO [information operations] by protecting friendly command and control systems and decision makers from adversary deception. Friendly decision makers must be aware of adversary deception activities so they can formulate informed and coordinated responses."[130]

In their 2003 study, Russell Glenn and Scott Gerwehr proposed a modern concept for counter-deception. They note that "counter-deception is a skillset of its own that requires conscious allocation of resources and training." They identify five categories of counter-deception worthy of additional study and potentially for incorporation into NATO training and education curricula. These categories are: data type, data collection, data analysis, unmasking deception with deception, and rendering deception moot.[131]

A final point to note is that self-deception is a critical weakness that must be minimized in military leadership. Michael Dewar notes, "A study of deception in history reveals that success was usually achieved because the ruse conformed with a preconceived idea in the mind of the target and, since they were more or less what the target was expecting."[132]

Russian actions at the start of the full-scale invasion in 2022 are an example of self-deception. If the Russians had searched for it, they would have found Ukrainian forces beginning to disperse their units and logistic supplies in the lead-up to the February 2022 invasion. But they did not look for it because Putin and commanders were convinced that the Ukrainians would not fight and that Russia's forces could seize control of the country in 10 days.

Self-deception is unlikely to ever be totally removed from any human organization, however. To that end, investment might be required in additional research by academic institutions into psychology and other human cognitive sciences to inform training, education, and developmental opportunities for developing commanders and leaders who are less prone to self-deception before and during military operations.

Strategy

While military deception has an important role to play in tactical actions and the conduct of military campaigns, it also has utility at the strategic level of military affairs and in a broader range of national security affairs. Education, doctrine, and training should not focus exclusively on the tactical aspects of deception. This will require the cultivation of knowledge and expertise at the highest level in strategic deception activities, and potentially the establishment of a small permanent staff to coordinate such activities.

Strategic deception activities will make an invaluable contribution to solving some of the significant strategic and operational challenges facing military organizations due to the trends outlined in the previous section of this report. In particular, deception may contribute to solutions to the following contemporary military challenges in search of a solution. These are strategic problems because they involve all elements of contemporary military institutions and require new thinking about strategic force design, warfighting concepts, equipment and munitions, training, and education.

Strategic Problem 1: Mass versus Dispersion

The meshed civil–military sensor frameworks, and attendant signature battle, described in this report have produced an environment where all the signatures of military equipment, personnel, and collective forces can be detected more accurately and rapidly. When linked to an array of precision munitions, this closes the detection-to-destruction gap in military operations to just minutes. Massing military forces for ground combat operations, large-scale aerial attacks, or naval operations, therefore, becomes a high tactical and operational risk. As the Russians have found during the war in Ukraine, when

they have massed forces in training or accommodation locations, or concentrated their logistics depots close to the frontline, the Ukrainians have been able to find and attack them.[133] This has also driven both sides to conduct attacks with small teams to improve their ability to move to their lines of departure undetected.

Even if an array of hard and soft kill measures can protect massed forces, they are almost assured of detection, which makes achieving surprise difficult. Modern military forces must be equally capable of operating in dispersed and massed forms, but they must be able to minimize their detection when they do mass in a way that offers an improved chance of surprise and landing a decisive blow against an adversary. Strategic and operational deception activities may provide at least part of the solution to this quandary.

Strategic Problem 2: Closing Operational and Strategic Distances

Modern combat forces require new-era techniques that are quicker, lower signature, and more survivable at crossing operational and tactical spaces between them and their objectives. The failings of current Western military doctrine were exemplified by Ukraine's struggle in 2023 to penetrate Russian minefields and defensive belts in southern Ukraine. Meshed sensor networks, electronic warfare, and multi-layered and multi-domain drone frameworks make this a difficult problem.

In eastern Ukraine, where almost all movement on and above the ground is visible within many kilometers of the front line, assembling forces for any significant activity and moving those forces has become very high risk. We should expect that the ability of aircraft to assemble strike packages in friendly airspace, and the ability of naval task groups to move to their operating areas, will also become increasingly threatened.

Therefore, new warfighting concepts are needed to ensure that friendly forces can surviveably mass and move to a start point for operations and tactical activities in friendly parts of a theater. Deception may play a crucial role in solving this challenge, but this will require investment in strategic force design and force options testing activities.

Strategic Problem 3: Lowering the Cost of Defending Against Missiles and Drones

One of the implications of the new trend in more accessible long-range strike is that it requires a strategic approach to protecting key military and national assets much further beyond the front line. Enormous investment has been made in development of remotely controlled, autonomous, and

semiautonomous uncrewed systems. Ukraine has essentially developed a long-range strike complex, capable of striking deep into Russia, from a standing start three years ago. A large proportion of the Ukrainian strike capability consists of indigenously designed and built long- and medium-range drones.

Until recently, there has been a large gap between the capabilities of uncrewed systems and those that counter them, as well as a major disparity in the costs of drones versus the systems to counter them. New systems developed by the Ukrainians, including their Drone Fall program using interceptor drones, the expanded use of tactical radars to improve detection, and improved electronic warfare have all started turning this situation around, but Russian adaptation to these countermeasures poses a constant challenge.[134] As such, deception operations at multiple levels might provide part of the solution to this strategic problem in the following areas:

- deceiving an adversary about the capability and range of counter-drone systems
- deceiving an adversary about the locations and depth of these systems
- deceiving an adversary about the locations of strategic capabilities, such as low-density munitions
- dispersion and deception activities for key military production facilities

Finally, strategic deception activities hold the potential to endanger the contract of trust that an elected government has with the people. In his book *Active Measures: The Secret History of Disinformation and Political Warfare*, Thomas Rid argues that "it is impossible to excel at disinformation and democracy at the same time."[135] While it may not be such an absolute, strategic deception activities by democracies will face cultural challenges, and must be endorsed by political leadership as well as having a basis in law and be subject to legal oversight.

Battlespace Operations

Deception operations should be planned and conducted not as separate but as integral aspects of military activities. Two forms of maneuver that embrace deception as a core enabler are distributed operations and flooding the zone. These will be examined separately but should not be seen as distinct approaches; they are most likely to be mutually reinforcing methods of operations.

Distributed operations deceive an enemy about capacity to concentrate and force structure because distributed elements can be grouped, disaggregated, and then regrouped according to the mission and threat profile of the enemy.

Distributed operations have been studied by several military organizations, perhaps most resolutely by the U.S. Marine Corps.[136] One reason these operations offer a useful approach in operational and tactical activities is that they support enhanced force-preservation and survivability against technologies that have increased the lethality of the contemporary battlefield; they deceive the enemy about a friendly main effort and its critical vulnerabilities.

Increased lethality has been a trend for at least the last 200 years of human conflict. Charting force dispersion and theoretical killing power over two millennia, Trevor Dupuy notes that the lethality of warfare remained constant for nearly two thousand years. But the dawn of the first industrial revolution at the end of the 1700s saw a significant change in this pattern. Starting in the 1800s, the trend in lethality commenced a sharp upward curve.[137]

However, this was countered over the past century through dispersion of military forces. This lowered average daily casualty rates in war. Technological progress in killing was countered by an intellectual response.

In addition to lowering lethality, dispersion of forces through distributed operations allows for more opportunities to deceive an adversary. This is because a more dispersed force provides fewer insights into friendly main and supporting efforts due to a lack of concentrated forces. Distributed operations also distribute logistics and fire support assets, again denying an enemy detailed insights into main efforts, and deceiving them about friendly intentions for a longer period of time than might otherwise be the case with more traditional operational approaches.

Service and joint operational approaches will require extensive review to ascertain whether different modes of distributed operations, as well as signature minimization and projection, have utility—and a good return on investment—in preserving a deployed force in a lethal environment, and its potential for deceiving an adversary.

As well as considering distributed operations, normal military operations must consider the minimization of all forms of signatures. Where possible, exercise designs for military training activities—single-service and joint—should encourage the recording of signatures of all platforms and units, so that the projection of false signatures in the real world and in cyberspace can be used to overwhelm or at least confuse adversary analysts and AI analytics about friendly locations, capabilities, and intentions.

"Flood the zone" is a term that originates in team sports and, in American football, refers to an offensive team deploying a larger number of players than normal to one side of the field to force a defending team to over-commit their number of players on that side of the field. It is a term that has also been used in political commentary to describe political parties launching multiple policies and making numerous announcements in a short space of time to draw attention away from the most controversial policies.[138]

It is also a method increasingly used in Ukraine and Russia, by both sides, to penetrate the air, missile, and drone defenses of each nation. Both sides use large numbers of decoy drones in their strike operations, in successive waves, to draw defenders into firing scarce air defense missiles, while other drones are able to proceed to their targets. The Russians often use large numbers of Shahed drones in initial waves to draw out Ukrainian air defenses, and then use successive waves of cruise and ballistic missiles to hit targets. The number of drones used in these complex attack operations has increased over the past year. And while Ukraine has improved its ability to shoot down drones, it is not 100 percent successful. Missiles and drones get through.

Russian infiltration attacks on the ground use similar principles. Large numbers of small groups are used to conduct constant attacks to wear down defenders and force them to use up ammunition. It is a brutal yet effective way that Russian commanders on the eastern front have used their advantage in manpower to slowly advance—but at great human cost.

The key to flooding the zone in military operations will be flooding the battlespace with a wide array of targets—in the physical, cyber, information, and electromagnetic domains—to occupy sensors and engagement systems of the enemy, while attacking forces penetrate the tactical or operational zones they are seeking to move through. This may demand a range of autonomous systems to be employed as decoys as well.

Neither distributed operations nor flooding the zone are simple operational methods, and their combination will be more difficult still. Extensive experimentation and concept development will be required to employ such methods not only to deceive an adversary force but also to provide a higher chance of mission success for joint forces.

Military operations need to prioritize the conduct of planning and activities that serve to detect enemy deception, as well as to degrade the enemy's capacity to counter friendly deception operations. This may include, for example, evolution of the extant operating procedures for countering enemy sensors across all spectra. The conduct of this style of operation might consider prioritizing focus on enemy sensors, analytics and analysis processes, and shifting the perceptions of human decision makers.

Finally, some investment might be required in the capability to measure the success or failure of friendly deception endeavors. Measuring success and failure of deception activities can inform friendly commanders about tactical and operational risk (if deception fails, risk may rise).

Personnel

The quality of military personnel will have an important influence on the ability of military organizations to undertake effective military deception activities. To that end, three areas of personnel development may require reform: individual training, professional military education, and collective training.

Individual Training Design

Camouflage and concealment remain core competencies of military personnel and units. This is regardless of service, function, or proximity to combat operations. As our survey of new technologies and the signature battle found, almost everything is detectable and targetable in modern competition and warfare. And if it is not, we should assume it is anyway—we don't always understand the full scope of an enemy detection capability.

Training institutions must incorporate the development of expertise in camouflage and concealment as a foundational skillset, just as they do with weapons training and team building. This should include knowledge on all kinds of signatures that are generated by individuals, platforms, and units, and how these might be reduced or blended "into the noise" of military activities.

All personnel should understand the basic ideas associated with reducing signatures, conducting deception, and generating surprise. For example, these competencies should be included in formal training courses for officers and non-commissioned officers as well as in basic recruit and officer training. How potential adversaries conduct deception operations, and the markers for recognizing deception activities, should be included in military training curricula.

Professional Military Education (PME)

The various stages of military officer education offer the chance to inform and incentivize the use of deception in all forms of the military art. In particular, the education at command and staff colleges and war colleges should further reinforce the need for deception in an era where the most likely adversary will be a larger and even more powerful military force.

Professional military education (PME) systems potentially need to focus more on training in signatures, deception, and surprise; hone the capacity of officers to prioritize thinking about these aspects of war; and to fully incorporate them into formal and informal planning processes. Assessment in PME institutions might also shift more toward incentivizing lateral thinking about deceiving an adversary, and toward developing military leaders to invest in their capacity to influence the perceptions and behavior of enemy commanders.

Deception must be integrated into training and education systems. Presently, it is just one of many training outcomes in Western training institutions. It must be given more precedence because of the increasing need to surprise potential adversaries, deceive adversaries about locations and intentions to enhance force preservation, and recognize and counter enemy deception operations.

Collective Training Design

Collective training must be a mandatory part of exercise design for service and joint exercise design at every level. Achievement of surprise, through deception and other means, must be a required element of exercise assessment and a central aspect of all after-action reviews. Collective training activities must also be exploited as an opportunity to collect signatures of units, joint task forces, and other aggregated military capabilities. Not only does this signature measurement activity assist in efforts to minimize signatures and deceive adversaries, but these collected signatures might then be projected in cyber and information operations to deceive and confuse adversaries about friendly locations and intentions.

The concepts of signature management, deception, and surprise need to be part of design, conduct, and assessment criteria in military exercises. It should pertain to both single-service and joint environments, as well as in coalition or alliance exercises if possible. Pre-exercise activities and briefings should include the potential for enemy deception activities to ensure staff and commanders are trained in the art of recognizing deception conducted by an adversary in sufficient time to adapt to those enemy actions. Additionally, these exercises can provide useful testbeds for new techniques to mask signatures and deceive an adversary.

Military Organizational Structures

During the Second World War, the Soviets concentrated deception planning in their Stavka and General staff. They did this for two reasons. First, it provided for more thorough planning, including deception planning, between the various fronts. And second, the Soviets saw tactical, operational, and strategic deception as integrated and indistinguishable.[139]

At the same time as the Allied deception staff was conducting its operations, tactical deception organizations were also established by the British and Americans. These were able to bring a range of creative ideas to military commanders to enhance their chances of generating surprise on the battlefield. While a contemporary version of such organizations would need to focus on both the physical and cyber environments, small teams might be viable in contemporary joint task force organizations.

In 1990, a small team was established in the U.S. Central Command to develop a deception plan to focus Iraqi defenses on the Corps that would advance from the south. The aim of the plan was to deceive the Iraqis about a second Corps that would swing around into Kuwait from the west. This resulted in an integrated plan that included dummy formations and measures of success, and it even co-opted the media in their reporting of the lead-up to the U.S. offensive operations.[140]

In more contemporary practice, deception is a function of both Russian and Ukrainian planning at the general staff and senior tactical commands. Given the sensitivity of the topic, further details are not publicly available.

In U.S. combatant commands, the coordination of deception, while tightly controlled to maintain operational security like in the Ukrainian and Russian models, is generally overseen by the J39 deception staff in the operations branch. Responsible for military deception, electronic warfare (EW), psychological operations (PSYOP), operations security (OPSEC), and cyber operations, its key functions include developing and overseeing theater-wide deception strategies to mislead adversaries about U.S. and allied intentions and capabilities, coordinating with the intelligence organization to shape deception efforts based on adversary intelligence collection priorities, and coordinating with those undertaking longer-term planning to integrate deception into all operational and contingency planning.

The standardization of this approach might be considered for a wider number of military institutions. While this is unlikely to require the large-scale reallocation of military personnel to become deception specialists, a small number of experts in the art and science of deception might be useful at headquarters for joint task forces. Such small, expert teams—either integral to organizations or that can be "fly away" teams—might provide advice and planning for the conduct of tactical, operational, and strategic deception activities.

But organizational constructs beyond headquarters and staff will also be influenced by the new environment of enhanced battlespace visibility, democratized access to digital command and control systems, and ubiquitous all-domain drones. The combination of these developments now means that those conducting defensive operations have powerful advantages in modern warfare.[141] For survivability purposes, the structures of ground, air, and naval units will need to evolve based on the lessons of the last three years in Ukraine. And these new structures must incorporate designs for better deception and operational security constructs.

For integration of military deception into broader strategic deception efforts, a dedicated function executed by a strategic deception staff (which oversees deception and counter-deception activities) may be required. An example of this is the Allied deception staff, known as the London Controlling Section, established during the Second World War to deceive the Germans about the D-Day landings, which proved incredibly successful, all the way to convincing Hitler to hold off the release of Panzer division reserves even after the Normandy landing.[142]

Equipment and Technology Development

Decoys have made a big comeback in the war in Ukraine.[143] While the Second World War saw the use of decoys extensively, particularly in the lead-up to the invasion of Normandy in 1944, the period since then has not seen decoy equipment and networks used extensively—until now.[144]

Ukraine began deploying decoys early in the war. The provision of high mobility artillery rocket systems (HIMARS) systems by America led to Ukraine also deploying multiple decoy systems to protect real launchers and deceive Russian intelligence, surveillance, and reconnaissance (ISR) and strike capabilities into hitting fake launchers.[145] Since then, a wide array of decoys has been employed, including artillery systems, air defense radars and missile launchers, and armored vehicles.[146] Additionally, strikes by both Russia and Ukraine often use decoy drones in an attempt to overwhelm air defense systems and draw air defense weapons to shoot down decoys instead of warhead-bearing drones and missiles.

Nicolea Bonsegna has written about how decoys have a psychological impact: "Decoys have the potential to sow confusion, create uncertainty, and distort enemy decision-making processes. In Ukraine, Ukrainian forces have been using decoys to complicate Russian efforts to assess the real strength and positioning of Ukrainian forces...[and create] an atmosphere of uncertainty that forces Russian forces to misallocate resources, leading to operational inefficiencies."[147]

Cheap and easily emplaced decoys should not only be employed on military operations but become a new priority in defense research and acquisitions, being made part of standard provisioning when new equipment is procured. Decoys must be issued alongside the real equipment, particularly for high-value equipment such as radars, air defense systems, artillery, and armored vehicles. This is not presently viewed as a valued area of the modern defense economy outside Ukraine, and that should change.

Additionally, decoys extend beyond physical replicas of equipment or locations. Communications networks, drones, and other signatures of military operations also need to be employed to provide an overwhelming number of potential targets for enemy sensors and kill chains, and to protect actual military capabilities.

Systems for the procurement of military equipment and services to military organizations will probably need to focus more on lowering the signatures of weapon systems, military platforms across all domains, and support equipment. This is not to suggest that every platform will be a stealth platform. However, the range of signatures—from visual to aural to exhaust—must all be concurrently lowered to significantly increase the challenge of signature detection by enemy sensors and platforms.

At the same time, the elements of contemporary meshed sensor and communications networks described in this report should constantly be reviewed for their security, as well as for their capacity to be used in the conduct of friendly deception activities and counter of enemy deception.

The power of AI offers functions that replicate many human cognitive functions. And it can be used to extend cognition in those who are tired, or who are unable to cope with massive amounts of data generated by meshed sensor networks. The theory of AI extenders, developed by Jose Hernandez-Orallo and Karina Vold, proposes that cognitive functions in humans, including enhanced memory, attention, and search, can be 'extended' with AI.[148] For contemporary military institutions, AI offers the ability to develop bespoke algorithms that can support human analytic activities to counter enemy deception activities. Military institutions will need to consider investing in AI systems that can assist human activities associated with deception and counter-deception, as well as support friendly simulation and wargaming related to military deception.

The development of bespoke algorithms that support the countering of enemy deception activities may be required. The massive quantity of data that is currently generated by digital age sensors is generally beyond the comprehension and analytical capacity of human intelligence organizations. Some system to sort and recognize, in near real-time, is needed. Only AI can provide this capacity for breaking through the deliberately generated "fog of war" that Russian doctrine emphasizes. Such algorithms, and their accompanying datasets, might also be useful to support simulation and wargaming to hone friendly command and planning capabilities in deception activities.

Finally, new materials offer properties that might reduce friendly signatures and enhance the performance of friendly sensors in detecting adversary signatures. Complementing these new materials, 3D printing has field applications for the rapid production of tailored camouflage nets as well as dummy emitters and other forms of physical deception.

A wide array of commercial additive printing capabilities has been examined by military institutions in the past decade. In particular, they have applications in the production of spare parts. However, as 3D printers increase in capability and reduce in price, military institutions will be able to use massed, deployable 3D printers that can produce objects for the conduct of deception activities. For example, they may rapidly print tactical camouflage nets and covers that are tailored to the environment. Another example of deployed 3D printing for deception might be the rapid production of emitters for different electromagnetic emissions, or even the production of masses of small unmanned aerial vehicles (UAVs) to overwhelm enemy sensors.

The enhancement of military deception activities requires investment in technology. New or smart materials are one example of these technologies, but new types of sensors, masking technologies such as camouflage systems, and drone swarms are also important technologies that underpin deception and counter-deception operations. As with all military institutions, this investment

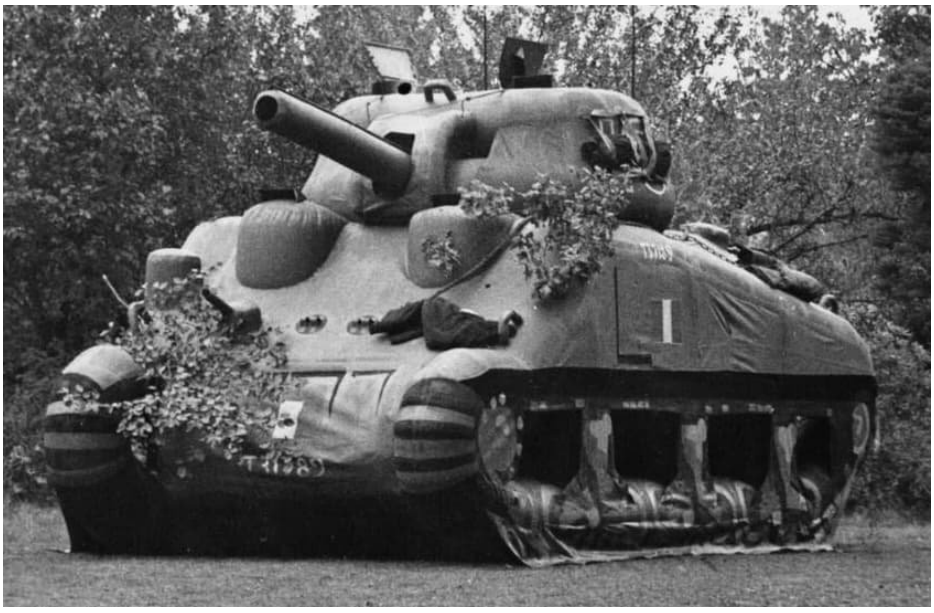
must be balanced against other technology investments, as well as investments in people and operations.

Doctrine

Doctrine provides the essential foundation for all military training and the conduct of operations. It should not be a fixed template, but an essential starting point for thinking about solutions to unit and individual challenges. Therefore, the production of dedicated doctrine for deception operations is often necessary. This can encompass tactical operations as well as strategic activities.

Importantly, deception needs to be a highlighted and an important aspect of doctrine on other elements of military activities, including operations, planning, logistics, and communications. As Michael Anderson notes, with regards to deception and doctrine, an improved focus on military deception begins with "the elevation of deception from a niche doctrinal approach to inclusion in the foundational principles and elements of doctrine."[149]

Doctrine on military deception, and counter-deception, will need to describe how deception operations go beyond just the orchestration of military deception into other military activities. It may also include the integration of civilian personnel into the conduct of deception activities. As an example, during the Second World War, the U.S. Army employed a range of artists, engineers, and architects in its secret 23rd Headquarters Special Troops organization to conduct tactical deception operations.[150]



An inflatable dummy tank used by the U.S. 23rd Headquarters Special Troops "ghost army" in World War II.

Source: U.S. Army via Wikimedia Commons

Deception must be employed at every level of national security activities, not just in military operations. This will pose some issues in democracies where transparency and auditability are essential parts of effective governance. New policies and potentially new laws might be required to enable this.

Finally, to inform doctrine for military deception activities, a review of existing principles and maxims was undertaken as part of the production of this report. The Maxims of Deception appear to have survived their transition into the twenty-first century. While some aspects of execution will evolve, similar to the principles for military deception, the maxims described earlier in this report remain suitable and are a useful guide to thinking about the conduct, execution, and measurement of military deception.

The principles for planning and conducting military deception must be consolidated and better incorporate new trends and technologies. To that end, the following new principles for military deception are proposed:

→ THE NEW PRINCIPLES FOR MILITARY DECEPTION

1. **Influence the decision maker.** Military deception should target the thought process of the adversary decision maker to achieve a desired action, decision, or outcome. The adversary sensing and analysis system is not the target of military deception. It is, however, a means by which deception can deliver information to the targeted decision maker. By the same token, friendly counter-deception activities should influence the actions of friendly commanders.

2. **Create a response that achieves desired outcomes.** Deception plans employ actions and resources to change the behavior of enemy decision-making in order for there to be an outcome desired by the friendly commander. Military deception must lead to the target making a specific decision or set of decisions.

3. **Integrate planning and control.** An integrated approach to planning military deception and counter-deception within the wider military planning process is necessary to avoid confusion and to ensure various elements portray the same story and do not conflict with other operational objectives. This integration should orchestrate an array of different means of deception, because the greater the number of channels used, the greater the likelihood that deception will work. This integration of military deception starts with planning, continues through execution, and also includes learning and adaptation activities.

4. **Ensure approaches are credible, verifiable, executable, and measurable.** Military deception must be credible in the minds of the targeted decision maker as well as those who provide advice. There must be consistency in the narrative being used to create the desired response. The enemy should also be able to conduct verification activities to confirm what our deception plan seeks to make them believe. The deception plan must be feasible to achieve with

given resources. And finally, friendly forces should be able to measure the impact of deception measures to see if they are successful or not.

5. **Make security a priority.** Military deception operations require appropriate security measures. Planning staff must employ the strictest need-to-know criteria for every element of military deception planning and execution. Counter-deception activities will require similar measures.

6. **Consider timeliness**. A critical aspect of deception planning and execution is appropriate synchronization with the commander's intent and maintaining synchronization during execution. A key challenge is getting the deception target to act in accordance with the deception objective within the timelines required. Friendly deception activities must be completed in a way that accounts for the time consumed by the enemy's intelligence collection and analysis process, the enemy's decision-making process, and the enemy's activity that is to be exploited by friendly forces.

Conclusion

This report has explored existing ideas about military deception, principally through the lens of doctrinal principles of Western military doctrines. It has also investigated the military trends that act as disruptors to force change in the planning, execution, and measurement of military deception operations.

The contents of this report provide foundational knowledge for developing multiple lines of endeavor that could improve the conduct, and outcomes, of future military deception activities. A range of changes and new programs, across the breadth of military endeavors, has been examined in the final chapter of the report. These areas for improvement incorporate personnel training, education, and development; doctrinal and tactical evolution; equipment design and procurement; and strategic and policy issues.

The pace of learning and adaptation that is being witnessed now in Ukraine, from both sides, continues to accelerate. Learning cycles for drone operations and technology are now just a couple of weeks. Ukraine and Russia are locked in an adaptation battle on the ground where tactics change every two to three months. And, more broadly, Russia has developed a learning and adaptation "bloc" with Iran, China, and North Korea, where it shares lessons from the war in a wide variety of subjects. As the most recent *Annual Threat Assessment* from the U.S. intelligence community describes, "Cooperation among China, Russia, Iran, and North Korea has been growing more rapidly in recent years, reinforcing threats from each of them individually while also posing new challenges to U.S. strength and power globally...Russia has been a catalyst for the evolving ties."[151]

This learning and adaptation cooperation among authoritarian governments is almost certain to include insights about tactical and strategic deception. Indeed, as the report proposes, it is very likely that the combination of cultural predisposition to deception activities and new technologies has opened up a "deception gap" between authoritarian and democratic military institutions. Thus, this is yet another driver to ensure that the best thinking, best technology, and best leadership are applied to evolving the conduct of military deception in American and allied military institutions in the coming years.

We should not deceive ourselves into thinking that change is not needed.

Notes

1 News Desk, "For the First Time, Ukraine Attacks Russian Positions Using Solely Ground, FPV Drones," *Kyiv Independent,* December 21, 2024, https://kyivindependent.com/for-first-time-ukraine-attacks-russian-positions-using-solely-ground-fpv-drones/.

2 U.S. Department of the Army, *Field Manual 3-90, Tactics* (U.S. Government Publishing Office, 2023), 19–21, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN38160-FM_3-90-000-WEB-1.pdf.

3 Martin van Creveld, *Command in War* (Harvard University Press, 1985), 264.

4 Virgil, *The Aeneid*, trans. Sarah Ruden (Yale University Press, 2008), Book 2.

5 Sun Tzu, *The Art of War*, ed. Ralph Sawyer (Westview Press, 1994), 117–140; Michael Handel, *Masters of War: Sun Tzu, Clausewitz, and Jomini* (Frank Cass, 1992), 102–6.

6 Douglas Stuart and William Tow, "The Theory and Practice of Chinese Military Deception," in *Strategic Military Deception*, ed. Donald Daniel and Katherine Herbig (Pergamon Press, 1981), 292–316.

7 Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (RAND Corporation, 2018), 67–72.

8 Examples include: Katri Pynnöniemi and András Rácz, eds., *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine* (Finnish Institute for International Affairs, 2016), https://fiia.fi/en/publication/fog-of-falsehood; Nicola Bonsegna, "The Strategic Role of Decoys in the Conflict in Ukraine," *Defence Horizon Journal* (blog), October 31, 2024, https://tdhj.org/blog/post/decoys-conflict-ukraine/; Marie Snegovaya, *Russia Report I: Putin's Information Warfare in Ukraine* (Institute for the Study of War, 2015), https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

9 Scott Gerwehr and Russell W. Glenn, *Unweaving the Web: Deception and Adaptation in Future Urban Operations* (RAND Corporation, 2003), xii, https://www.rand.org/pubs/monograph_reports/MR1495.html.

10 Cambridge Dictionary online, "Deception," accessed April 2025, https://dictionary.cambridge.org/dictionary/english/deception.

11 Donald Daniel and Katherine Herbig, eds., *Strategic Military Deception* (Pergamon Press, 1981), 3.

12 Charles Cruickshank, *Deception in World War Two* (Book Club Associates, 1979).

13 Roy Godson and James Wirtz, eds., *Strategic Denial and Deception: The Twenty-First Century Challenge* (National Strategy-Information Center, 2002), 2.

14 Conrad Crane, "Conclusion: The Future of Deception Operations," in *Weaving the Tangled Web: Military Deception in Large-Scale Combat Operations*, ed. Christopher Rein (Army University Press, 2018), 233.

15 Norman Dixon, *On the Psychology of Military Incompetence* (Pimlico, 1976), 119–120.

16 U.S. Joint Staff, *Joint Publication 3-13.4*: *Military Deception* (U.S. Department of Defense, January 26, 2012), I-1, https://jfsc.ndu.edu/portals/72/documents/jc2ios/additional_reading/1c3-jp_3-13-4_mildec.pdf.

17 U.S. Marine Corps, *Marine Corps Doctrinal Publication 8: Information* (Department of the Navy, June 21, 2022), 2–23, https://www.marines.mil/Portals/1/Publications/MCDP%208.pdf.

18 NATO Standardization Office, *Allied Joint Publication-3.10.2: Allied Joint Doctrine for Operations Security and Deception*, Edition A Version 2 (NATO, March 2020), 4, https://assets.publishing.service.gov.uk/media/6422d0ba60a35e00120caf09/20230327-AJP_3_10_2_Ops_and_Deception-O.pdf.

19 Morgan Maier, *A Little Masquerade: Russia's Evolving Employment of Maskirovka* (School of Advanced Military Studies United States Army Command and General Staff College, 2016), https://apps.dtic.mil/sti/pdfs/AD1022096.pdf.

20 Anthony H. Cordesman, *Chinese Strategy and Military Modernization in 2016: A Comparative Analysis* (Center for Strategic and International Studies, December 2016), https://www.jstor.org/stable/resrep23376; David M. Finkelstein, *The PLA's New Joint Doctrine* (Center for Naval Analyses, 2021); https://www.cna.org/reports/2021/09/the-plas-new-joint-doctrine; Edmund Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (RAND Corporation, September 2020), https://www.rand.org/pubs/research_reports/RRA394-1.html.

21 Cole Herring, "How to Challenge China's Military Deception Tactics," Irregular Warfare Initiative, December 19, 2024, https://irregularwarfare.org/articles/how-to-challenge-chinas-military-deception-tactics/; Thomas Haydock, *Defeating Deception: Outthinking Chinese Deception in a Taiwan Invasion* (Association of the United States Army, July 31, 2024), https://www.ausa.org/publications/defeating-deception-outthinking-chinese-deception-taiwan-invasion.

22 Michael Pillsbury, "Chinese Deception Doctrine: A View from Open Sources," in *The Art and Science of Military Deception*, ed. Hy Rothstein and Barton Whaley (Artech House, 2013), 212–213.

23 Daniel and Herbig, *Strategic Military Deception*, 5–6.

24 U.S. Marine Corps, *Marine Corps Doctrinal Publication 8: Information*, 2–23, https://www.marines.mil/Portals/1/Publications/MCDP%208.pdf.

25 Barton Whaley, "Toward a General Theory of Deception," *Journal of Strategic Studies* 5, no. 1 (1982), 178–192; Daniel and Herbig, *Strategic Military Deception*; Jon Latimer, *Deception in Warfare* (John Murray Publishers, 2001); Christopher Rein, ed., *Weaving the Tangled Web: Military Deception in Large-Scale Combat Operations* (Army University Press, 2018); and Michael Dewar, *The Art of Deception in Warfare* (New York: Sterling Publishing, 1989).

26 Barton Whaley, *Stratagem: Deception and Surprise in War* (MIT Press, 1969), 3.

27 Armée de Terre, *Tactique Générale (General Tactics),* 2nd ed. (Economica, 2014).

28 British Army, *Land Operations* (Land Warfare Development Centre, undated).

29 U.K. Ministry of Defense, *Multi-Domain Integration: Joint Concept Note 1/20* (U.K. Development, Concepts, and Doctrine Centre, November 2020), https://assets.publishing.service.gov.uk/media/6579c11a254aaa000d050c6e/20201112-ARCHIVE_JCN_1_20_MDI_Official.pdf.

30 U.S. Joint Staff, *Joint Publication 3-13.4*: *Military Deception*.

31 U.S. Army, *FM3-13.4: Army Support to Military Deception* (Headquarters Department of the Army, February 2019).

32 NATO Standardization Office, *Allied Joint Publication-3.10.2*, 6–7.

33 NATO, *Allied Joint Doctrine for Operations Security and Deception*, 2.

34 U.S. Joint Staff, *Joint Publication 3-13.4: Military Deception*, ix.

35 U.S. Marine Corps, *Marine Corps Doctrinal Publication 8: Information* (2022), 2–22.

36 Central Intelligence Agency, *Freedom Information Act response* (Reference F-2015-02095, December 2015).

37 Dewar, *The Art of Deception in Warfare*, 194–203.

38 Deception Research Program, *Deception Maxims: Fact and Folklore* (Central Intelligence Agency Office of Research and Development, June 1981), 5–45.

39 Williamson Murray and MacGregor Knox have differentiated between these two concepts. Military revolutions are wholesale changes to societies and their ability to engage in war. They are less frequent but have more impact because they recast society and the state, as well as military institutions. Revolutions in military affairs are "clusters of less all-embracing changes" in which military organizations focus on finding new ways to destroy their enemies. See Williamson Murray and McGregor Knox, *The Dynamics of Military Revolution, 1300–2050* (Cambridge University Press, 2001), 7, 12.

40 Michael C. Horowitz, "Battles of Precise Mass," *Foreign Affairs*, October 22, 2024, https://www.foreignaffairs.com/world/battles-precise-mass-technology-war-horowitz.

41 Stefan Korshak, "Ukraine Drone Production Tops 2.5 Million a Year, Aircraft Numbers on Track to Grow," *Kyiv Post,* February 10, 2025.

42 President Volodymyr Zelensky signed a decree establishing the force on September 16, 2024. See Martin Fornusek, "Zelensky Signs Law Establishing Ukraine's Unmanned Systems Forces," *Kyiv Independent*, September 16, 2024, https://kyivindependent.com/zelensky-signs-law-on-ukraines-unmanned-systems-forces/.

43 This idea of employing robots for the "dirty, dangerous, and dull" tasks is examined in Peter W. Singer, *Wired for War* (Penguin Books, 2009).

44 Sydney Freedberg, "Meet the Army's Future Family of Robot Tanks: RCV," Breaking Defense, November 9, 2020, https://breakingdefense.com/2020/11/meet-the-armys-future-family-of-robot-tanks-rcv/.

45 Mick Ryan, *Human Machine Teaming for Future Ground Forces* (Center for Strategic and Budgetary Assessments, 2018), 14–15.

46 In 2025, Ukraine's military expects to form uncrewed ground vehicle companies in each of its brigades.

47 The DroneFall initiative of the Come Back Alive Foundation is one such initiative. This is now being widely deployed by frontline units. See Olena Hrazhdan, "Come Back Alive Says 'Dronefall' Project Downed Russian Drones Worth $65M," *Kyiv Post*, March 22, 2025, https://www.kyivpost.com/post/49369.

48 Joe Lacdan, "Joint Counter-Small UAS Office Conducts Successful Counter Drone-Swarm Demonstration," U.S. Army, July 26, 2024, https://www.army.mil/article/278404/joint_counter_small_uas_office_conducts_successful_counter_drone_swarm_demonstration; "DoD Announces Strategy for Countering Unmanned Systems," U.S. Department of Defense, December 5,

2024, https://www.defense.gov/News/Releases/Release/Article/3986597/dod-announces-strategy-for-countering-unmanned-systems/. Companies, such as Anduril https://www.anduril.com/capability/counter-uas/ and AIM Defence https://www.aimdefence.com, among many others, have also developed counter-drone technologies, but are yet to be battle tested.

49 Edward Geist and Marjory Blumenthal, "Military Deception: AI's Killer App?," *War on the Rocks*, October 23, 2019, https://warontherocks.com/2019/10/military-deception-ais-killer-app/.

50 John Ferrari and Hallie Coyne, "Deception Is the Biggest Threat to American Security," *RealClear Defense*, July 21, 2021, https://www.realcleardefense.com/articles/2021/07/21/deception_is_the_biggest_threat_to_american_security_786460.html.

51 Author interview with Lieutenant General Kyrylo Budanov, Ukrainian military intelligence, conducted March 11, 2025. Mick Ryan, "What I Learnt About the Future of War in Ukraine This Week," *Australian Financial Review*, March 14, 2025, https://archive.is/PI6ud#selection-1267.0-1267.58.

52 Allie Funk, Adrian Shahbaz, and Kian Vesteinsson, *Freedom on the Net 2023: The Repressive Power of Artificial Intelligence* (Freedom House, 2023), https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence; see also Jessica Brandt, "Propaganda, Foreign Interference, and Generative AI," *Brookings*, November 8, 2023, https://www.brookings.edu/articles/propaganda-foreign-interference-and-generative-ai/.

53 Yong Jian, "China Explores Military Applications with DeepSeek," *Asia Times*, March 1, 2025, https://asiatimes.com/2025/03/china-explores-military-applications-with-deepseek/.

54 See Ryan Greenblatt, Carson Denison, Benjamin Wright, et al., "Alignment Faking in Large Language Models," *arXiv*, December 20, 2024, https://www.anthropic.com/research/alignment-faking; Billy Perrigo, "Exclusive: New Research Shows AI Strategically Lying," *Time*, December 18, 2024, https://time.com/7202784/ai-research-strategic-lying/.

55 Rhiannon Williams, "AI Systems Are Getting Better at Tricking Us," *MIT Technology Review*, May 10, 2024, https://www.technologyreview.com/2024/05/10/1092293/ai-systems-are-getting-better-at-tricking-us/.

56 Currently Starlink has over 7,100 satellites in orbit approximately 550 kilometers above the Earth. Tereza Pultarova, "Starlink Satellites: Facts, Tracking, and Impact on Astronomy," *Space.com*, March 28, 2025, https://www.space.com/spacex-starlink-satellites.html.

57 Nivedita Bhattacharjee, Eduardo Baptista, Lisandra Paraguassu, and Ricardo Brito, "Chinese Rivals to Musk's Starlink Accelerate Race to Dominate Satellite Internet," Reuters, February 24, 2025, https://www.reuters.com/technology/musks-starlink-races-with-chinese-rivals-dominate-satellite-internet-2025-02-24/.

58 U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (Office of the Secretary of Defense, 2019), 50–51; Phil Stewart, "U.S. Studying India Anti-Satellite Weapons Test, Warns of Space Debris," Reuters, March 28, 2019, https://www.reuters.com/article/world/us-studying-india-anti-satellite-weapons-test-warns-of-space-debris-idUSKCN1R826U/.

59 Joe Saballa, "Five Chinese Satellites Engage in 'Dogfighting' Drills in Space: US Officials," *Defense Post*, March 19, 2025, https://thedefensepost.com/2025/03/19/chinese-satellites-dogfighting-drills/.

60 Clémence Poirier, *Hacking the Cosmos: Cyber Operations Against the Space Sector* (Centre for Security Studies, 2024), https://css.ethz.ch/en/center/CSS-news/2024/10/hacking-the-cosmos-cyber-

operations-against-the-space-sector-a-case-study-from-the-war-in-ukraine.html.

61 David Hambling, "Volunteers Worldwide With 3D Printers Are Aiding Ukraine's War Effort," *Forbes*, June 7, 2024, https://www.forbes.com/sites/davidhambling/2024/06/07/how-volunteers-worldwide-are-helping-ukraines-war-with-3d-printers/.

62 Rueben Dass, "3D Printing in Conflict Zones: A Game Changer?," Global Network on Extremism and Technology, October 14, 2024, https://gnet-research.org/2024/10/14/3d-printing-in-conflict-zones-a-game-changer/.

63 Australian Government, *New and Advanced Materials* (Industry Commission, Report No. 42: March 8, 1995), xxvi.

64 Susi Wallner, "Top 10 Materials Industry Trends and Innovations in 2022," *StartUs Insights*, August 20, 2020, https://www.startus-insights.com/innovators-guide/top-10-materials-industry-trends-innovations-2020-beyond/.

65 Australian Government, *Advanced Materials and Manufacturing: Implications for Defence to 2040* (Defence Science and Technology Group, 2018), 10.

66 "Meta-Material Magic: Demystifying the Science of Cloaking," *Mad Scientist Laboratory*, November 30, 2023, https://madsciblog.tradoc.army.mil/469-metamaterial-magic-demystifying-the-science-of-cloaking/.

67 Lindsay Rand and Berit Goodge, "Information Overload: The Promise and Risk of Quantum Computing," *Bulletin of Atomic Scientists*, November 14, 2019, https://thebulletin.org/2019/11/information-overload-the-promise-and-risk-of-quantum-computing/; Michael Biercuk and Richard Fontaine, "The Leap into Quantum Technology: A Primer for National Security Professionals," *War on the Rocks*, November 17, 2017, https://warontherocks.com/2017/11/leap-quantum-technology-primer-national-security-professionals/.

68 Jonathan Dowling and Gerard Milburn, "Quantum Technology: The Second Quantum Revolution," *Royal Society* 361 (2003): 1656–7; Elsa Kania and John Costello, *Quantum Hegemony: China's Ambitions and the Challenge to U.S. Innovation Leadership* (Center for a New American Security, 2018), 2–5.

69 Tom Stefanick, "The State of U.S.-China Quantum Data Security Competition," Brookings, September 18, 2020, https://www.brookings.edu/articles/the-state-of-u-s-china-quantum-data-security-competition.

70 Elsa Kania, "China's Quantum Future: Xi's Quest to Build a High-Tech Superpower," *Foreign Affairs,* September 26, 2018, https://www.foreignaffairs.com/articles/china/2018-09-26/chinas-quantum-future.

71 Matt Swayne, "Chinese Scientists Report Using Quantum Computer to Hack Military-Grade Encryption," *Quantum Insider*, October 11, 2024, https://thequantuminsider.com/2024/10/11/chinese-scientists-report-using-quantum-computer-to-hack-military-grade-encryption/.

72 A qubit, or quantum bit, is the basic unit of information used to encode data in quantum computing and can be best understood as the quantum equivalent of the traditional bit used by classical computers to encode information in binary. Josh Schneider and Ian Smalley, "What Is a Qubit?," *IBM Blog*, https://www.ibm.com/think/topics/qubit.

73 Stephen Nellis, "Amazon Unveils Quantum Chip, Aiming to Shave Years Off Development Time," Reuters, February 27, 2025, https://www.reuters.com/technology/artificial-intelligence/amazon-unveils-quantum-chip-aiming-shave-years-off-development-time-2025-02-27/.

74 "Quantum Computing Stocks Rise as Microsoft's New Chip Heats up Debate over Technology," Reuters, February 21, 2025, https://www.reuters.com/technology/quantum-computing-stocks-rise-microsofts-new-chip-heats-up-debate-over-2025-02-20/.

75 Catherine Bolgar, "Microsoft's Majorana 1 Chip Carves New Path for Quantum Computing," Microsoft, February 19, 2025, https://news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/.

76 U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China, 2024* (Office of the Secretary of Defense, 2024), 26, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF.

77 Michael J.D. Vermeer and Evan D. Peet, *Securing Communications in the Quantum Computing Age* (RAND Corporation, 2020), 1, https://www.rand.org/pubs/research_reports/RR3102.html.

78 Mick Ryan, *War Transformed* (U.S. Naval Institute Books, 2022), 93.

79 "Fire Information for Resource Management System," NASA, https://shorturl.at/VKKF2.

80 "Why Russian Radios in Ukraine Are Getting Spammed with Heavy Metal," *The Economist*, March 28, 2022, https://www.economist.com/the-economist-explains/2022/03/28/why-russian-radios-ukraine-war-intercepted-heavy-metal.

81 Kateryna Bondar, *Does Ukraine Already Have Functional CJADC2 Technology?* (Center for Strategic and International Studies, 2024), https://www.csis.org/analysis/does-ukraine-already-have-functional-cjadc2-technology.

82 Bondar, *Understanding the Military AI Ecosystem in Ukrain*e, 2–3, https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine.

83 Samuel Bennett, *The Role of AI in Russia's Confrontation with the West* (Center for a New American Security, 2024), https://www.cnas.org/publications/reports/the-role-of-ai-in-russias-confrontation-with-the-west.

84 See Gina Cavallaro, "The Transparent Battlefield: Combat Training Centers Sharpen Unit Tactics for High tech Fight," Association of the United States Army, June 25, 2024, https://www.ausa.org/articles/transparent-battlefield-combat-training-centers-sharpen-unit-tactics-high-tech-fight; Dorsel Boyer and ISC Robert K. Becker, "How Ukraine Overcame the Transparent Battlefield to Achieve Operational Surprise in Kursk," TRADOC G2, September 19, 2024, https://oe.tradoc.army.mil/product/how-ukraine-overcame-the-transparent-battlefield-to-achieve-operational-surprise-in-kursk/.

85 An important example of this was the Hamas deception plan executed in the lead-up to its October 7, 2023, attack on southern Israel. See Yoav Zitun, "How Hamas Outsmarted Israel: The Deception That Led to the October 7 Intelligence Breakdown," Ynet, February 28, 2025, https://www.ynetnews.com/article/bkd8rnrqkl.

86 Ryan, *War Transformed*, 83.

87 Daniel Byman and Emma McCaleb, "Understanding Hamas's and Hezbollah's Uses of Information Technology," Center for Strategic and International Studies, July 31, 2023, https://www.csis.org/analysis/understanding-hamass-and-hezbollahs-uses-information-technology.

88 Jack Watling, Oleksandr V Danylyuk, and Nick Reynolds, *Preliminary Lessons from Ukraine's Offensive Operations, 2022–23* (Royal United Services Institute, July 2024), 31, https://static.rusi.org/lessons-learned-ukraine-offensive-2022-23.pdf.

89 This evolution in Russian ground tactics was raised multiple times by Ukrainian brigades during co-author Mick Ryan's March 2025 research visit to Ukraine. See also Michael Kofman, *Assessing Russian Military Adaptation in 2023* (Carnegie Endowment for International Peace, October 2024), https://carnegieendowment.org/research/2024/10/assessing-russian-military-adaptation-in-2023; and U.S. Army, *ATP 7-100.1: Russian Tactics* (February 2024), https://irp.fas.org/doddir/army/atp7-100-1.pdf.

90 Giorgio Di Mizio and Michael Gjerstad, "Ukraine's Ground-Based Air Defence: Evolution, Resilience, and Pressure," International Institute for Strategic Studies, February 24, 2024, https://www.iiss.org/online-analysis/military-balance/2025/02/ukraines-ground-based-air-defence-evolution-resilience-and-pressure/.

91 Roman Romaniuk, "They Set Targets Deep Inside Russia on Fire: The Untold Story of the 14th Unmanned Aerial Vehicle Regiment," *Ukrainska Pravda*, March 17, 2025, https://www.pravda.com.ua/eng/articles/2025/03/17/7503165/.

92 A description of these Russian counter-strike activities was provided by Ukrainian military intelligence chief, General Kyrylo Budanov, during a research visit to Ukraine in March 2025.

93 Lara Seligman, Paul McLeary, Alexander Ward, and Veronika Melkozerova, "Ukraine Uses Secretly Shipped U.S. Missiles to Launch Surprise Strike," *Politico*, October 17, 2023, https://www.politico.com/news/2023/10/17/ukraine-uses-secretly-shipped-u-s-missiles-to-launch-surprise-strike-00121932.

94 In Australian Army doctrine, the combination of these three is called "fighting power."

95 Peter Singer and Emerson Brooking, *LikeWar: The Weaponization of Social Media* (Houghton Mifflin Harcourt, 2018), 273.

96 Mick Ryan and Marcus Thompson, "Social Media in the Military: Opportunities, Perils and a Safe Middle Path," *Grounded Curiosity*, August 21, 2016, https://groundedcuriosity.com/social-media-in-the-military-opportunities-perils-and-a-safe-middle-path/.

97 "Digital 2025 Global Overview Report," We Are Social, https://wearesocial.com/au/blog/2025/02/digital-2025/.

98 And they can do it quickly. As a study by Massachusetts Institute of Technology researchers found that social media has enabled false news to travel faster and penetrate further than true stories. Analyzing major news stories over a 10-year period, including 126,000 stories and 3 million tweets, the study found that false information outperforms true information. See Sorough Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science*, March 9, 2018, https://science.sciencemag.org/content/359/6380/1146.

99 U.S. preemption activities, before the war, are described in Jessica Brandt, "Preempting Putin: Washington's Campaign of Intelligence Disclosures is Complicating Moscow's Plans for Ukraine," Brookings, February 18, 2022, https://www.brookings.edu/blog/order-from-chaos/2022/02/18/preempting-putin-washingtons-campaign-of-intelligence-disclosures-is-complicating-moscows-plans-for-ukraine/. Post-invasion preemption with intelligence is explored in Shannon K. Crawford, "Preemptive, Public U.S. Strikes Winning Intelligence War with Russia: Analysis," ABC News, April 15, 2022, https://abcnews.go.com/Politics/preemptive-public-us-strikes-winning-intelligence-war-russia/story?id=84015518; and Douglas London, "How Intelligence Is Helping to Win the Unthinkable War with Russia," *The Hill*, March 30, 2022, https://thehill.com/opinion/national-security/600293-how-intelligence-is-helping-to-win-the-unthinkable-war-with-russia/.

100 Jennifer Kavanagh, "The Ukraine War Shows How the Nature of Power Is Changing," Carnegie Endowment for International Peace, June 16, 2022, https://carnegieendowment.org/2022/06/16/ukraine-war-shows-how-nature-of-power-is-changing-pub-87339.

101 Alan Suderman and Ali Swenson, "Right-Wing Influencers Were Duped to Work for Covert Russian Operation, U.S. Says," Associated Press, September 6, 2024, https://apnews.com/article/russian-interference-presidential-election-influencers-trump-999435273dd39edf7468c6aa34fad5dd.

102 Andrés Monroy-Hernández, et al., "The New War Correspondents: The Rise of Civic Media Curation in Urbane Warfare," *Proceedings of the 2013 Conference on Computer-Supported Cooperative Work*: 1443–1452, https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/civic-media-warfare-CSCW2013.pdf.

103 This combination of new and old ways of reporting on wars is explored in Gillian Vernick, "Visual Forensics Merge with Traditional War Reporting in 'First Social Media War,'" Reporters Committee for Freedom of the Press, March 7, 2022, https://www.rcfp.org/ukraine-first-social-media-war/.

104 Christopher Warren, "Trending in the Trenches: Social Media is Giving Birth to a New Kind of War Journalism," *Crikey*, March 7, 2022, https://www.crikey.com.au/2022/03/07/war-journalists-social-media-ukraine/.

105 See Daniel Byman, Daniel Linna, and V. S. Subrahmanian, "Should Democratic Governments Use Deep Fakes?," *Lawfare*, May 9, 2024, https://www.lawfaremedia.org/article/should-democratic-governments-use-deepfakes; and Josh A. Goldstein and Andrew Lohn, *Deepfakes, Elections, and Shrinking the Liar's Dividend* (Brennan Center for Justice, January 23, 2024), https://www.brennancenter.org/our-work/research-reports/deepfakes-elections-and-shrinking-liars-dividend.

106 Christoph Deppe and Gary S. Schaal, "Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept," *Frontiers* 7 (2024), https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full.

107 Robert "Jake" Bebber, *Cognitive Competition, Conflict, and War: An Ontological Approach* (Hudson Institute, May 2024), 9, https://www.hudson.org/defense-strategy/cognitive-competition-conflict-war-ontological-approach-robert-jake-bebber.

108 Deppe and Schaal, "Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept," https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full.

109 U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China, 2024*, 37, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF.

110 U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China, 2024*, 27, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF.

111 Dima Adamsky, *The Russian Way of Deterrence* (Stanford University Press, 2024), 40–57.

112 "Cognitive Warfare: Strengthening and Defending the Mind," NATO Allied Command Transformation, April 5, 2023, https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/.

113 Monroy-Hernández et al., "The New War Correspondents: The Rise of Civic Media Curation in Urbane Warfare," https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/civic-media-warfare-CSCW2013.pdf.

114 Tom Simonite, "A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be," *Wired*, March 17, 2022, https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/.

115 Peter Suciu, "Putin's Deepfake Doppelganger Highlights the Danger of the Technology," *Forbes*, December 15, 2023, https://www.forbes.com/sites/petersuciu/2023/12/15/putins-deepfake-doppelganger-highlights-the-danger-of-the-technology/.

116 Ryan, *War Transformed*, 83–4.

117 Max Hunder, "Ukraine Collects Vast War Data Trove to Train AI Models," Reuters, December 21, 2024, https://www.reuters.com/technology/ukraine-collects-vast-war-data-trove-train-ai-models-2024-12-20/; David Kirichenko, "The Rush for AI-Enabled Drones on Ukrainian Battlefields," *Lawfare*, December 5, 2024, https://www.lawfaremedia.org/article/the-rush-for-ai-enabled-drones-on-ukrainian-battlefields.

118 Mick Ryan, "What I Learnt About the Future of War in Ukraine This Week," *Australian Financial Review*, March 14, 2025, https://archive.is/PI6ud#selection-1267.0-1267.58.

119 Elizabeth Dwoskin, "Israel Built an 'AI Factory' for War. It Unleashed It in Gaza," *Washington Post*, December 29, 2024, https://www.washingtonpost.com/technology/2024/12/29/ai-israel-war-gaza-idf/.

120 The literature on this part of the war remains immature. However, some good sources include Kavanagh, "The Ukraine War Shows How the Nature of Power Is Changing," https://carnegieendowment.org/2022/06/16/ukraine-war-shows-how-nature-of-power-is-changing-pub-87339; Michaela Dodge, *Russia's War in Ukraine and Implications for Its Influence Operations in the West* (National Institute for Public Policy, June 7, 2022), https://nipp.org/wp-content/uploads/2022/06/IS-524.pdf; and Suzanne Smalley, "Russian Information Operations Focus on Dividing Western Coalition Supporting Ukraine," *CyberScoop*, July 7, 2022, https://cyberscoop.com/russian-information-operations-dividing-west-ukraine.

121 Francis G. Hoffman, *Mars Adapting: Military Change During War* (U.S. Naval Institute Press, 2021).

122 Mick Ryan, "Dispatch from Ukraine: The Adaptation Battle Intensifies," *Interpreter* (blog), Lowy Institute, March 17, 2025, https://www.lowyinstitute.org/the-interpreter/dispatch-ukraine-adaptation-battle-intensifies.

123 Scott Gerwehr and Russell W. Glenn, *Unweaving the Web: Deception and Adaptation in Future Urban Operations* (RAND Corporation, 2003), 55.

124 Author interview with senior officer in Ukrainian Ground Forces, in Kyiv, March 10, 2025. Name withheld by request.

125 Author interview with Ukrainian brigade commander, March 2025.

126 The role of vision in organization change is the subject of an excellent study by Carl Builder and others that focused on the U.S. Army at the end of the Cold War but supplies enduring and widely applicable principles for the development and use of organizational vision. John K. Setear et al., *The Army in a Changing World: The Role of Organisational Vision* (RAND Arroyo Center, June 1990), vi, https://www.rand.org/content/dam/rand/pubs/reports/2006/R3882.pdf.

127 Donn A. Starry, "To Change an Army," *Military Review*, March 1983, 23.

128 Author interview with Colonel Vadym Sukharevskyi, in Kyiv, March 15, 2025.

129 Dewar, *The Art of Deception in Warfare*, 194, 200.

130 U.S. Joint Staff, *Joint Publication 3-13.4*: *Military Deception* (2012), ix.

131 Scott Gerwehr and Russell W. Glenn, *Unweaving the Web: Deception and Adaptation in Future Urban Operations* (RAND Corporation, 2003), xiv.

132 Dewar, *The Art of Deception in Warfare*, 194.

133 One example of this was the December 2022 attack on a Russian barracks in Donetsk that killed dozens of Russian soldiers. "Alleged HIMARS Strike Killed 'Hundreds' of Russian Troops During Putin's New Year Address in Donetsk's Makiivka – Media," *Euromaidan Press*, January 2, 2023, https://euromaidanpress.com/2023/01/02/alleged-himars-strike-killed-hundreds-of-russian-troops-during-putuns-new-year-address-in-donetsks-makiivka-media/.

134 Olena Hrazhdan, "Come Back Alive Says 'DroneFall' Project Downed Russian Drones Worth $65 Million," *Kyiv Post*, March 22, 2025, https://www.kyivpost.com/post/49369.

135 Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (Farrar, Straus and Giroux, 2020), 11.

136 U.S. Marine Corps, "Distributed Maritime Operations," August 2, 2021, https://www.marines.mil/News/News-Display/Article/2708130/distributed-maritime-operations-dmo/.

137 Dupuy, *The Evolution of Weapons and Warfare*, 288–311.

138 Laura Tingle, "The Opposition is 'Flooding the Zone' With Foggy Ideas Instead of Focused and Disciplined Attacks," Australian Broadcasting Corporation News, March 22, 2025, https://www.abc.net.au/news/2025-03-22/flooding-the-zone-coalition-peter-dutton-referendum-donald-trump/105078038.

139 David Glantz, *Soviet Military Deception in the Second World War* (Routledge, 1989), 559–562.

140 Donald Wright, "Deception in the Desert: Deceiving Iraq in Operation Desert Storm," in *Weaving the Tangled Web,* ed. Christopher Rein (Army University Press, 2018), 215–228.

141 T.X. Hammes, *Game-Changers: Implications of the Russo-Ukraine War for the Future of Ground Warfare* (Atlantic Council, April 2023), 11–13, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/game-changers-implications-of-the-russo-ukraine-war-for-the-future-of-ground-warfare/.

142 John Hughes-Wilson, *Military Intelligence Blunders* (Robinson Publishing, 1999), 18.

143 Nearly every Ukrainian officer interviewed by the author in March 2025 raised deception as a critical issue in contemporary operations in Ukraine, whether in land, sea, or air activities. See also Christopher Miller, "The Decoy Weapons Leading Russian Forces Astray in Ukraine," *Financial Times*, September 22, 2023, https://www.ft.com/content/b0581f55-a449-439c-a92f-1dfb1ca5a181.

144 Bonsegna, "The Strategic Role of Decoys in Warfare," https://tdhj.org/blog/post/decoys-conflict-ukraine/.

145 John Hudson, "Ukraine Lures Russian Missiles with Decoys of U.S. Rocket System," *Washington Post*, August 30, 2022, https://www.washingtonpost.com/world/2022/08/30/ukraine-russia-himars-decoy-artillery/.

146 Stephen W. Miller, "Battlefield Decoys and Deception: Reaffirmed in Ukraine," *Armada International*, September 20, 2023, https://www.armadainternational.com/2023/09/battlefield-decoys-and-deception-reaffirmed-in-ukraine/; "Decoys and Deception – Ukraine's Use of Fake Weapon Systems," *Kyiv Post*, September 12, 2023, https://www.kyivpost.com/post/21544.

147 Bonsegna, "The Strategic Role of Decoys in Warfare," https://tdhj.org/blog/post/decoys-conflict-ukraine/.

148 José Hernández-Orallo and Karina Vold, "AI Extenders: The Ethical and Societal Implication of Humans Cognitively Extended by AI," *AIES '19: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society,* 2019, 507–513, https://dl.acm.org/doi/10.1145/3306618.3314238.

149 Michael G. Anderson, "The Case for Deception in Operational Success," *Military Strategy Magazine* 8, no. 2 (Fall 2022): 38–42, https://www.militarystrategymagazine.com/article/the-case-for-deception-in-operational-success/.

150 Megan Garber, "Ghost Army: The Inflatable Tanks That Fooled Hitler," *The Atlantic*, May 23, 2013, https://www.theatlantic.com/technology/archive/2013/05/ghost-army-the-inflatable-tanks-that-fooled-hitler/276137/; Lynn Neary, "Artists of Battlefield Deception," NPR, September 25, 2007, https://www.npr.org/2007/09/25/14672840/artists-of-battlefield-deception-soldiers-of-the-23rd.

151 Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (March 2025), 29, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

NEW AMERICA