PSYCHOLOGY AND EDUCATION (2025) 62(05):332-359
ISSN: 1553-6939

Needs of National Defense and Vulnerability in the Context of the Information Revolution in Military Affairs

Dr. SORAYA ZAOUCHI[1]

[1]University of Algiers 3, Faculty of Political Science and International Relations (Algeria).

The E-mail Author: sorayazaouchi@gmail.com

Received: 07/10/2024 **Published: 08/05/2025**

Abstract:

All national defense needs in the information revolution have become arguments for military governance regarding the possibility of resolving controversial strategic issues between great powers, as well as the importance of collective management of problems arising from vulnerability, so that the suspicion and fear that typically govern international military relations disappear, or at least diminish, as is common in the realist/neorealist tradition. 1 Therefore, the primary goal of military governance in the information revolution is to demonstrate the high potential for controlling military relations through collective will and multilateral strategic dialogues, which provide each party with a complete picture of the other's intentions and enable it to correct distorted perceptions. The ultimate goal, of course, is to spare the world the tragic effects of all-out wars.

Keywords: National defense, security, information revolution, strategy, military security.

Introduction:

The demands of national defense have evolved in direct response to the escalating instability characterizing both the local and regional security environments. This evolution has intensified security concerns among policymakers, prompted by the emergence of both traditional and non-traditional threats, ranging from military and civilian to humanitarian and natural in origin. These developments unfold within the

expanding influence of what Robert R. Tomes [1]and other strategic thinkers describe as the “Information Revolution in Military Affairs.” [2]In effect, the influence of this revolution has become what Thomas Bruneau and Harold Trinkunas term a "global trend," impacting all societal sectors in ways that are simultaneously beneficial and detrimental.

From a theoretical standpoint, the information revolution has been posited as a response to the intricate challenges of security. Strategists contend that its core objective is to diminish what Clausewitz famously referred to as "the fog of war." However, the central dilemma lies in the dual nature of this revolution: while it addresses issues of information scarcity and enables integrated situational awareness across strategic and operational combat landscapes, thereby meeting certain national defense requirements, it also introduces profound gaps and vulnerabilities. These risks affect not only military targets but extend significantly into the civilian domain as well.

Within this broader framework of inquiry, several critical questions emerge: What precisely does the revolution in military affairs entail? What are the conceptual and analytical implications of the information revolution in military contexts? How has it reshaped strategic approaches? What are its operative tools? What specific defense needs have arisen from this transformation? What operational and tactical challenges accompany its application in contemporary warfare? And most importantly, what significant vulnerabilities are exposed as a result of its implementation?

These inquiries will be addressed through the following thematic areas:

First: Conceptual Definitions

Second: Technology and the Information Revolution in Military Affairs

Third: The Information Age and the Changing Nature of Combat

[1] Robert R. Tomes, US Defense Strategy from Vietnam to Operation Iraqi Freedom: Military Innovation and the New American Way of War, 1973–2003 (New York: Routledge Taylor & Francis Group, 2007), pp. 29–31.
[2] Thomas Bruneau and Harold Trinkunas, “Global Trends and Their Impact on Civil-Military Relations,” in Global Politics of Defense Reform, ed. Thomas Bruneau and Harold Trinkunas (United States of America: Palgrave Macmillan, 2008), pp. 05–09.

Fourth: Components of the Information Revolution in Military Affairs

Fifth: Adapting to the Requirements of the Information Revolution

Sixth: The Cracks within the Information Revolution in Military Affairs

First: Conceptual Definitions

Definition of the Revolution in Military Affairs

Although the term "Revolution in Military Affairs" is not yet universally entrenched within the discourse of strategic analysis and international relations, its usage gained considerable momentum following the Second Gulf War in 1991. Nonetheless, a substantial number of definitions remain dispersed across scholarly works that examine the transformative influence of emerging military technologies on contemporary combat systems.

One prominent definition is provided by Robert R. Tomes, who describes the revolution as "a significant change in the nature of combat driven by the innovative application of new technologies in combination with fundamental changes in doctrine, operational practices, and military organizations... [It requires] radical changes in the management of military operations and, at times, even in the very nature of warfare itself."[3]

Similarly, Williamson Murray and MacGregor Knox emphasize that "Revolutions in military affairs always occur within a context of politics and strategy, and that context is everything."[4]

Brian M. Downing, for his part, defines the revolution in military affairs as "the process by which small feudal armies were replaced by large armies financed by a centralized state and equipped with complex and expensive weapons. [5]

[3] Robert R. Tomes, US Defense Strategy from Vietnam to Operation Iraqi Freedom: Military Innovation and the New American Way of War, 1973–2003 (New York: Routledge Taylor & Francis Group, 2007), pp. 01–04.
[4] Robert R. Tomes, Ibid., p. 12.
[5] Robert R. Tomes, Ibid., p. 29.

The military revolution is primarily a political process in terms of its definition and consequences, rather than being solely of a purely military nature. It reflects the complex politico-military transformations that characterized the 16th and 17th centuries in Europe, which took place under social and political conditions shaped by war."[6] This definition emphasizes that the evolution in military structure and capability cannot be isolated from the broader sociopolitical transformations that accompanied the consolidation of state power and institutional modernization during this historical period.

In the same context, William S. Cohen, who served as the U.S. Secretary of Defense under President Bill Clinton during the 1990s, offered a definition that situates the revolution within the broader context of systemic military transformation. He stated: "A revolution in military affairs occurs when the military dimensions of the state offer the opportunity to transform its strategy, military doctrines, training, education, organization, equipment, operations, and tactics in order to achieve decisive military outcomes in fundamentally new ways." [7]

The underlying principle in Cohen's definition highlights a comprehensive transformation that spans both tangible and intangible dimensions of military development. It encompasses strategic thinking, doctrinal evolution, and operational adaptation, as well as the practical demands of training in newly developed weaponry, communication systems, computerized operations, and digital warfare infrastructure.[8] Yet, despite the evolving methods and tools, the strategic objectives remain fixed, namely, to optimize military efficiency in service of political ends through the application of force.[9]

Turning to the contributions of Colin Gray on the subject of the revolution in military affairs, several noteworthy definitions emerge from his work. In one instance, he defines it as "a radical change in the nature and conduct of war… Unlike strategy and war, defining this concept requires great care regarding what is included and

[6] Colin S. Gray, Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History, foreword by Williamson Murray (London: Frank Cass, 2005), p. 01.

[7] Colin S. Gray, Ibid., p. 66.
[8] Colin S. Gray, Ibid., p. 68.
[9] Mikkel Vedby Rasmussen, The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century (UK: Cambridge University Press, 2006), p. 43.

what is excluded [from developments and changes in military affairs].” This caveat underlines the complexity of characterizing such a revolution, which cannot be reduced to merely technological or tactical innovation, but must also consider what developments qualify as truly transformative within the conduct of warfare.[10]

In another formulation, Gray describes the revolution in military affairs as “the peak event in battle where new systems, operational concepts, and organizations are employed, which clearly demonstrates the dramatic change in the conduct of warfare.” This definition underscores the operational visibility of change, transformations that are not merely theoretical but observable in the field through the application of advanced systems and novel forms of organization. Elsewhere, he defines it more succinctly as “a fundamental change in the nature of combat,” thereby reinforcing the foundational shift implied by such a revolution.[11]

In a further analytical context, Gray asserts that “the revolution in military affairs is better described as a process rather than an event. It serves the same conceptual function as the idea that strategic concepts developed since the modern era play a role in shaping the nature of combat through continuous global transformation.” This interpretation places emphasis on the revolution as an ongoing progression rather than a discrete moment in time, aligning it with the broader evolution of strategic thought and military doctrine under the pressure of global change. He also offers an additional definition, describing it as “the changing means and methods of combat,” further highlighting its dynamic nature.

Jeffrey R. Cooper provides another perspective by defining the revolution in military affairs as “a significant break in military capability and effectiveness [between two distinct eras or periods in the history of international strategy].” This formulation focuses on the temporal discontinuity it introduces, marking a clear departure from past practices and heralding a new phase in the strategic capabilities of military forces.

Andrew F. Krepinevich contributes yet another significant definition: “What is a military revolution? It is what happens when new technologies are applied to a

[10] Mikkel Vedby Rasmussen, Ibid., p. 43.

[11] Colin S. Gray, Ibid., p. 69.

significant number of military systems, accompanied by innovative operational concepts and organizational adaptations, in a way that fundamentally alters the nature and conduct of conflict. It therefore results in a significant, whether large or small, increase in the potential lethality and military effectiveness of armed forces." This statement encapsulates the essence of the military revolution by linking technological innovation to systemic transformation, leading to enhanced combat potential and operational efficacy.

The revolution in military affairs is also defined as "revolutionary changes derived from fundamental, qualitative changes in the tools of armed conflict, methods of battle, force organization, and military training and education."[12]

As for the meaning of the term in Soviet military thought, it was "associated with the new development of a set of concepts, arguments, and theories. It relates to the parallels between advanced conventional capabilities and the longstanding discourse over decades about multifaceted changes in strategy and combat involving nuclear weapons."[13]

From the perspective of the RAND Corporation: "The revolution in military affairs necessitates a change model in the nature and conduct of military operations, in which outdated or inappropriate [competencies and combat methods] are discarded in favor of the more essential competencies of the dominant player, or where a fundamental or more modern competency is created."

Others consider the revolution in military affairs as "the [process] that alters the way in which action is taken... [targeting three essential components]: technological innovation, operational concept (or doctrine), and organizational adaptation."[14]

Strategy, conceptually, can be defined in its relationship to the revolution in military affairs as "the art and process of conceptualizing the forms of military power required for national security or defense strategy, managing resources to provide military

[12] Robert R. Tomes, US Defense Strategy from Vietnam to Operation Iraqi Freedom: Military Innovation and the New American Way of War, 1973–2003 (New York: Routledge Taylor & Francis Group, 2007), pp. 47–52.
[13] Mikkel Vedby Rasmussen, The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century (UK: Cambridge University Press, 2006), p. 65.
[14] Thomas K. Adams, The Army After Next: The First Postindustrial Army (London: Praeger Security International, 2006), p. 12.

power, and using that power effectively to achieve the objectives outlined in the national strategy. At the most fundamental level, strategy involves the instrumental relationship between ends and means, a relationship partially defined by decisions about resource allocation."[15]

In the broader sense of the relationship between strategy and revolutions in military affairs, the term "grand strategy" was introduced, which for Colin Gray refers to "the deliberate deployment of all state assets, not merely the use of military power."[16]

Some view the concept of strategy from the perspective of the information revolution in military affairs as "a way to rationalize the application of modern technology in combat."[17]

Strategy is also defined as a concept that expresses "the process by which military power is translated into political effect. Therefore, strategy is not war itself; rather, it is the process through which war functions as a political act." Or, put differently, it is "the process that transforms military power into political impact."[18]

Military transformation. Since the notion of revolution inherently involves (partial or complete) changes in methods, doctrines, tactics, and the art of operations, some strategic theorists have proposed the term "Military Transformations" as a synonym for the "Revolution in Military Affairs[19]." However, for a transformation to truly reflect the meaning of revolution, it must entail an element of discontinuity. This requirement remains relative, given that revolutions in military affairs typically unfold over extended and overlapping periods of time.

Historically, the concept of transformation in military affairs has been reflected in the emergence of several military strategies, which, in fact, signify profound developments in military doctrines and the art of operations. Examples of such

[15] Robert R. Tomes, US Defense Strategy from Vietnam to Operation Iraqi Freedom: Military Innovation and the New American Way of War, 1973–2003 (New York: Routledge Taylor & Francis Group, 2007), pp. 01–04.
[16] Colin S. Gray, War, Peace and International Relations: An Introduction to Strategic History (London and New York: Routledge Taylor & Francis Group, 2007), p. 184.
[17] Mikkel Vedby Rasmussen, The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century (UK: Cambridge University Press, 2006), p. 51.
[18] Thomas M. Kane and David J. Lonsdale, Understanding Contemporary Strategy (London and New York: Routledge Taylor & Francis Group, 2012), pp. 01–03.
[19] Colin S. Gray, Ibid., pp. 01–02.

strategies include the concept of strategic containment in the 1940s, nuclear deterrence and then limited war in the 1950s, strategic stability and arms control in the 1960s, détente in the 1970s, ballistic missile defense and competition strategies in the 1980s.

These transformations have continued up to the present day and will persist into the future, for instance, the emergence of the U.S. missile shield strategy and the countermeasures adopted by Russia and China, as well as the emergence of combat strategies for asymmetric warfare in the 1990s and early 21st century.

Second: Technology and the Information Revolution in Military Affairs

One of the dominant and driving forces behind the information revolution in military affairs is the emergence of complex new technologies, which have imposed a new combat paradigm and necessitated the formulation of new strategic and operational concepts to match the significant advancements introduced in combat tools.

This influence has become dominant due to the astonishing tools employed by the U.S. military in modern conflicts such as those in Afghanistan and Iraq, as well as in other regions like the Horn of Africa and Yemen. Among these tools, a notable example is the “Predator”, the name given to Unmanned Aerial Vehicles (UAVs), which the U.S. military deployed during the 2001 war in Afghanistan.

In truth, the year 2001 merely marked the ignition point for internal conflicts, the war on terror, guerrilla warfare, and secessionist battles, which collectively became a vast experimental ground for testing, modifying, and further refining the tools of the information revolution in military affairs. It also became a testing ground for newly developed doctrines aligned with this revolution in addressing all forms of unconventional conflicts.

What is even more alarming is the fact that several countries have joined the race for dominance in the information revolution in military affairs, including Russia, China, India, Israel, Germany, and others, such that the use of information revolution technologies is no longer limited to states but has also extended to armed non-state groups.

The first known use of UAVs by such groups was by Hezbollah during its conflict with Israel in 2006, followed by Hamas in the 2014 war on the Gaza Strip, and there were attempts by ISIS to use them during the Battle of Mosul in October 2016.

The growing international investment in the information revolution and the pursuit of acquiring military information technologies is the most compelling argument used by proponents of the information revolution in military affairs. They argue that it has redefined the concept of war and reshaped the understanding of threats and risks, in addition to drawing a preliminary picture of what future warfare might look like. The basic assumption proposed in this regard is that the rapid development in innovative technologies will contribute to reshaping war management in a way that previously did not exist. Accordingly, countries that succeed in gaining superior technological advancement will also gain strategic weight in the future.

These advanced technologies require vast financial resources, highly developed infrastructure, professional and technical competencies, and scientific expertise. This implies that countries with such resources are likely to enjoy strategic superiority on the battlefield in the future, or at the very least, new powers may emerge in the military field with greater strategic advantage alongside traditional powers.

The persistence of operational and tactical challenges posed by unconventional warfare has amplified the practical relevance of the information technology revolution rather than diminishing it. This is due to the increasing tendency among modern armies to rely more on technology than on human soldiers to manage the battlefield, in other words, replacing human combatants with robotic ones (such as unmanned aerial vehicles).

Put differently, the escalating military risks in unconventional wars have deepened the transformations in military affairs driven by the information technology revolution, which now pervades almost all combat, intelligence, support, and reinforcement activities involved in managing modern warfare.

At the same time, these changes have accelerated in parallel with technological developments in military strategy formulation, doctrines, operational art, and even combat tactics. An example of this is the development of the "AirLand Battle" principle, which is in fact inspired by the “Battle in Depth” doctrine devised by the Soviet army during World War II. It refers to the conceptualization of the frontline

as a box rather than a line, a box that contains a number of simultaneous operations, characterized by superior firepower used to crush enemy forces.[20]

One of the earliest advocates of the dominant role of technology in reshaping the nature of future combat was former U.S. Secretary of Defense William Cohen, who stated in 1997 that information technology would enable U.S. armed forces to "collect and distribute the rapid flow of information to U.S. forces across the battlespace, while denying the enemy the ability to do the same."

More explicitly, the information revolution in military affairs enables combat units to fight as if in broad daylight by transmitting all information, data, and imagery to soldiers about what is happening on the battlefield, under all possible combat conditions, including adverse weather and nighttime darkness. Meanwhile, it forces enemy forces to fight in total darkness by depriving them of any information about the battlefield environment.

In the past, traditional methods were used to train soldiers to fight in environments where they lacked prior information, including nighttime combat. One notable example comes from the Prussian military academy, which used to simulate real combat scenarios for its cadets by having them play chess while blindfolded.

The students had to memorize the layout of the chessboard, understand the opening moves, anticipate the opponent's reactions, and rely on memory and rational deduction to assess what their opponent might do. When a student held a chess piece, he needed to know the enemy's previous position and assess his possible offensive or maneuvering options. [21]The key to winning a blindfolded chess match was extreme caution and using powerful pieces only at the right time or when the conditions of play allowed. An error in calculation would cost the game, but on the battlefield, it could cost one’s life. The use of powerful chess pieces in this context resembles Clausewitz's concept of deploying overwhelming force at the decisive point.

Supporters of the information revolution in military affairs hope that technology will help remove the blindfold from the chess player at the Prussian military academy by

[20] Mikkel Vedby Rasmussen, The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century (UK: Cambridge University Press, 2006), p. 45.
[21] Mikkel Vedby Rasmussen, Ibid., p. 55.

enabling combatants to access critical information about the terrain they are fighting on, the enemy's nature, environmental conditions, sociological characteristics, and accurate assessments of enemy strength, logistical capabilities, and ability to recover from combat losses. In more technical terms, it aims to enable combat units to achieve "Full-Spectrum Dominance" over the combat theater, thereby reducing the likelihood of vulnerability, deadly enemy responses, or surprise due to factors not accounted for in battle plans.[22]

Mikkle Vedby Rasmussen metaphorically articulated the promised potential of the information revolution when evaluating the U.S. military's "Joint Vision 2010" by stating: "This is a guiding principle of Joint Vision 2010 for the Joint Chiefs of Staff, aimed at ensuring that U.S. military operations play the game of war without a blindfold, while ensuring the enemy remains blindfolded. By connecting U.S. military infrastructure (such as tanks or aircraft carriers) to the 'System of Systems,' American forces become capable of integrating existing military systems into a unified information system, allowing them to achieve 'Dominant Battlespace Awareness.'"[23]

This is not merely a theoretical operational description, it has become a set of practical applications tested on the battlefield. Combat units have been trained to use and adapt to them in ways that ensure effective and professional engagement. Statistically speaking, during its 2003 invasion of Iraq, the U.S. military deployed more than 100,000 GPS units to track and monitor the locations of American soldiers across the vast combat environment that is Iraq.[24]

As a result, Central Command managed the battle remotely, observing combat operations on screens, identifying the positions of its forces, understanding their support needs and the dangers they faced, and directing concentrated firepower and air support toward high-risk threat zones.

Third: The Information Age and the Changing Nature of Combat

[22] Mikkel Vedby Rasmussen, Ibid., p. 56.
[23] Mikkel Vedby Rasmussen, Ibid., p. 59.
[24] Mikkel Vedby Rasmussen, Ibid., p. 60.

The main hallmark that defines the revolution in military affairs is the fundamental transformation in the nature of combat, driven by a dominant variable that imposes itself on the strategic environment, and which varies from one context to another. In the information age, the technological developments, especially those that emerged in the civilian sector, have imposed significant changes on the character of warfare.

These changes first manifested clearly on the battlefield during the international war on Iraq in 1991. Although the roots of this revolution are relatively deep within strategic history, the year 1991 is often marked as the point of departure for the information revolution in military affairs.

At the core of smart weapons warfare lies the computer, software, and information systems, all integrated into the new generation of weapons installed on aircraft, tanks, submarines, ships, and missiles. These technologies effectively, at least theoretically, and to a large extent practically, enhance targeting precision, reduce soldier casualties, and accelerate the resolution of conflict.[25]

For this reason, the information revolution in military affairs, particularly as implemented by the United States Armed Forces, has been built upon the following pillars: information dominance or knowledge superiority over the battlespace; networking of forces to exploit that information dominance; and precision targeting. The common thread linking all these elements is advanced technology, the principal driver of the information revolution.

In practical terms, however, these elements have proven most effective in conventional warfare, where rules of engagement are typically well-defined. In contrast, their effectiveness in irregular warfare remains limited, despite initial indications of their potential to address strategic challenges posed by asymmetric conflict.

The most prominent and tangible manifestation of the information revolution in military affairs, especially in conventional combat, has been summarized by U.S. military theorists as superiority in: Command, Control, Communication, Computing, Intelligence, Surveillance, Targeting, and Reconnaissance, abbreviated as CISTAR.[26]

[25] Colin S. Gray, War, Peace and International Relations: An Introduction to Strategic History (London and New York: Routledge Taylor & Francis Group, 2007), p. 242.
[26] Colin S. Gray, Ibid., pp. 240–42.

Through this superior strategic capability, no conventional army in the world is theoretically able to win on the battlefield against such dominance. Nonetheless, this remains a theoretical claim, since the element of surprise continues to be an inseparable feature of war, as emphasized by Clausewitz.

At the same time, this operational and tactical superiority, through the lens of neorealism, generates increasing concern among other actors, quickly translating into major drivers for the development of counter-strategies or preparations for counter-revolutions that the U.S. military might not be fully prepared to face.[27]

Fourth: Components of the Information Revolution in Military Affairs

1. The Revolution in Military Doctrine, Operational Art, and Combat Tactics

Like other military revolutions, one of the most evident outcomes of the information revolution is the remarkable innovation in military doctrines, operational art, and combat tactics. These developments were driven by growing strategic challenges encountered by both American and Soviet forces in Eastern Europe and Afghanistan during and after the Cold War, many of which were discussed earlier in our analysis of military revolutions from the mid-20th century through the early 21st-century conflicts.

The core premise behind strategic thinking in this revolution is the development of combat capabilities and operational and logistical potential to conduct warfare without resorting to nuclear weapons. That is, it centers on the question of how to win a war against a nuclear-armed adversary (particularly in Europe) without actually using nuclear arms. Victory in such a war would only be possible if the military doctrine empowered the armed forces to seize the initiative, control the strategic environment, and keep enemy forces under fire and within range of attack.

These conceptual components of the information revolution in military affairs were clearly embodied in the 1991 Gulf War through surveillance, targeting, decision

[27] Robert Gilpin, "War and Change in World Politics," in International Relations Theory: Realism, Pluralism, Globalism, 2nd ed., ed. Paul R. Viotti & Mark V. Kauppi (New York: Macmillan Publishing Company, 1993), pp. 142–146.

support, and precision-guided weapon systems, all seamlessly integrated into high levels of command, control, and improved coordination across the depth and breadth of the vast battlefield.[28]

In reality, there is no single "ideal" doctrine for this revolution, but rather a set of sub-doctrinal ideas and principles that were tested in direct battlefield scenarios, among them Rapid Dominance and Rapid Decisive Operations.[29]

Practically speaking, bold steps were taken to develop the U.S. Army's combat doctrine, operational art, military organization, and training in new combat tactics. These innovative developments took place under the leadership of General Creighton Abrams, head of the Joint Chiefs of Staff, despite the fact that he faced significant political and financial obstacles: weak political and budgetary support for new weapons systems, growing opposition to any increase in military spending, and general unwillingness to prepare for a new regional conflict following the Vietnam War.

Among the most practical steps taken toward innovating doctrine, operational art, and combat tactics was the establishment of the Training and Doctrine Command (TRADOC). This institution was tasked with reorganizing and modernizing doctrinal development and defining combat roles within the Army, in a manner that could persuade American political leaders and members of Congress of the necessity to allocate funding to support the technological modernization of new combat equipment.

2. The Promising Role of Air Power in Harnessing the Information Revolution

One of the key manifestations of the information revolution in the air power sector is the emergence of what came to be known as the AirLand Battle Doctrine in American strategic thought. Its tenets were outlined in a special manual for the U.S. Air Force in 1971, titled *United States Air Force Basic Doctrine (AFM 1-1)*. The

[28] Robert R. Tomes, US Defense Strategy from Vietnam to Operation Iraqi Freedom: Military Innovation and the New American Way of War, 1973–2003 (New York: Routledge Taylor & Francis Group, 2007), p. 60.
[29] Robert R. Tomes, Ibid., p. 61.

AirLand Battle Doctrine was introduced in response to the challenges facing the "Flexible Response Doctrine" against Soviet forces in Europe. It offered an alternative formula for engagement using highly equipped conventional forces capable of rapid deployment, air superiority, and containment of counterattacks.

The primary mission of the air force was defined as providing essential support to ground forces during their engagement with the enemy, or while advancing into the strategic depth of enemy territory, utilizing advanced technologies for guidance, precision targeting, and identification of hostile fire sources.

The conceptualization of new roles for air power introduced substantial shifts in aerial combat thinking and gave rise to new doctrines for managing air warfare or supporting ground operations. These were applied extensively during *Operation Desert Storm* in 1991 and the *invasion of Iraq* in 2003. In both wars, air power demonstrated its capabilities and effectiveness in executing these new roles.[30] Notably, it facilitated the construction of a strategic air bridge, aerial refueling for fighter jets, fuel tankers, and heavy airlift aircraft. This signified a significant development in the AirLand Battle Doctrine, enabling mobile armored and troop transport units on the ground to be accompanied and shielded from enemy air strikes.

As Robert R. Tomes put it, the air force began delivering fighter pilots to the battlefield rather than merely bombers with bombs and missiles, increasing the number of tactical support aircraft. By the mid-1980s, B-52 bombers had started training for conventional warfare and played a major role in the air campaign during the 1991 Gulf War.

The rapid modernization of the air force led to strategic rethinking about expanding its missions to include striking any target anywhere in the world, day or night, that posed a threat to American interests. In the second decade of the 21st century, Russia began to emulate the U.S. strategy in developing the capabilities of its air force to conduct combat operations on a global scale.

The main driver behind this global expansion of air power capabilities lies in technological advances and innovations in aerospace industries, communications,

[30] Robert R. Tomes, US Defense Strategy from Vietnam to Operation Iraqi Freedom: Military Innovation and the New American Way of War, 1973–2003 (New York: Routledge Taylor & Francis Group, 2007), p. 63.

and highly complex radar systems. In the United States, for example, a major milestone occurred in April 1973 when communication systems and coordination across different military sectors were unified into a single advanced communication program known as the Defense Navigation Satellite System. Later in September, this program was enhanced by adapting satellite orbits to naval time systems and the signal frequencies proposed by the Air Force.

The effectiveness of air power in global engagement missions was further reinforced by the innovation of the Global Positioning System Navstar (GPS), which enables precise location targeting and rapid response. Since 1974, efforts to improve GPS performance have continued by installing the system on satellites that conduct daily geographical scans of the Earth. In this context, the U.S. launched its first space rocket, Atlas, carrying a satellite named Block-1 equipped with GPS technology in 1974.

Strategic theorists view GPS as a revolutionary advancement in military communications. Over time, it was generalized for civilian use in sectors such as environmental monitoring and public services, similar to the evolution of the Internet from military to commercial use.

The information revolution in U.S. military affairs was also bolstered by new generations of advanced fighter aircraft, including the Lockheed F-117 Nighthawk stealth bomber and the Northrop B-2 Spirit. Moreover, a military program was launched to design new bombers, motivated by challenges faced by U.S. B-52 bombers due to Soviet air defense systems employed by the Viet Cong during the Vietnam War. Strategic statistics indicate that 5% of those aircraft were downed in that war.

Credit for the development of the aforementioned stealth aircraft goes to the mathematical research of Bill Schroeder and software engineering of Denys Overholser. Schroeder based his work on the 19th-century equations of physicist James Clerk Maxwell on reflected energy in spaces, as well as radar reflectivity studies by German engineer Arnold Johannes Sommerfeld, and early 1960s research by Soviet scientist Pyotr Ufimtsev on electromagnetic reflections.

Schroeder was able to solve the problem posed by anti-aircraft missiles targeting B-52s by designing an aircraft with angular panels that deflected radar waves,

preventing detection on enemy radar screens. These aircraft were also equipped with highly complex onboard computer systems, developed by Schroeder and Overholser, which enabled physical assessments for target identification and precision strikes using what is known as the Radar Cross Section (RCS).[31]

3. The Superior Role of Information

Strategic historians point out that the earliest signs of electronic warfare emerged during World War II, when the British intercepted encrypted German communications originating from Poland, using the encrypted communication machine known as ENIGMA. As a result, all German plans, particularly those related to Hitler's preparations for invading the Soviet Union and conducting airborne operations in Greece, were exposed to the British.

The use of the Enigma system ceased in 1974, after which F. W. Winterbotham published his book on the interception of encrypted German calls and messages under the title *The Ultra Secret* (1974). "Ultra" was the codename given to the British operation of intercepting and obstructing encrypted communications through the Enigma cipher machine.

In reality, the British were not the only ones who succeeded in intercepting German communications during the war; the Americans also succeeded by intercepting calls between Japanese military commanders and breaking the code, which enabled them to win the Battle of Midway. One of the most strategically significant consequences that sparked a shift in how modern warfare was perceived was the revelation of information's dominant role in increasing situational awareness on the battlefield, providing insight into the enemy's offensive or defensive capabilities, and redefining the role of intelligence in combat operations.

[31] Robert R. Tomes, Ibid., p. 66.

Put simply, information's dominant role in the combat environment lies in its ability to provide continuous surveillance capabilities over the theater of war and achieve complete control over the enemy's military forces.[32]

One of the most vital areas of superiority enabled by the information revolution is what is commonly referred to as electronic warfare, a domain powered by computers and the computational skills of engineers, and waged in the realm of virtual communications. Historically, electronic warfare was introduced as a new domain of modern conflict in 1978, when NATO defense planners classified it among six core issues for modernizing conventional forces. The other five were: "protective aircraft for defense against surprise attacks; anti-armor weaponry; war reserve stocks to provide deep logistical support for potential defense; mobile air defense to shield ground forces against Soviet air navigation; and advanced air-delivered munitions to improve firepower."[33]

Electronic warfare was activated in the late 1970s through what was then called the System of Systems, the actual operational engine of the young information revolution. It functioned by linking advanced ground radar systems with airborne or satellite-mounted sensor systems to support and enhance the process of information gathering and distribution to combat units.

This was done through what became known as the Joint Tactical Information Distribution System (JTIDS). In other words, preparations for electronic warfare were carried out by creating an integrated information system across all defensive and offensive units involved in the battlefield, including warships and submarines. Ultimately, this produced an interactive operational picture, enabling centralized geospatial awareness for strategic defense transformation at the dawn of the new millennium.[34]

4. Operational Capabilities on the Battlefield

[32] Robert R. Tomes, US Defense Strategy from Vietnam to Operation Iraqi Freedom: Military Innovation and the New American Way of War, 1973–2003 (New York: Routledge Taylor & Francis Group, 2007), pp. 67–68.
[33] Robert R. Tomes, Ibid., p. 80.
[34] Robert R. Tomes, Ibid., p. 87.

What most captivated the attention of military leaders regarding the information revolution in military affairs was the operational, even tactical, capabilities enabled by rapidly advancing information technologies. These technologies are evolving toward increased digitalization, virtualization, and a dramatic reduction in the constraints of time and space on the conduct of warfare.[35]

The profound, observable transformation in the nature of combat due to the information revolution is best captured in new operational elements summarized by Robert R. Tomes and other strategic theorists as: "temporal and spatial control, boldness, and flexibility, core components of the approach to winning open battles." Temporal control refers to the speed in dealing with threats before they materialize, while spatial control implies destroying enemy forces before any direct engagement by ground units or others.[36]

Temporal control under the information revolution is evident in the compression of movement and engagement timelines, closing distances that were once measured in hours to mere minutes. Similarly, spatial control has shifted through improved targeting capabilities. Advances in computer technology have enhanced the performance of self-guided or "smart" munitions that can distinguish their targets from among many similar or decoy targets.

Moreover, the development of computer software has brought the combat environment onto computer screens, enabling the tracking of a missile's trajectory toward its target, monitoring enemy movement on the ground, and viewing air-to-air engagements between aircraft or missiles across expansive airspaces. These objects move at supersonic speeds, yet they are now traceable on screens. In essence, computer technology has compressed thousands of miles into mere centimeters.

There was a clear determination within the Joint Chiefs of Staff and among field commanders to pursue "precision munitions, advanced automation, and other capabilities emerging from the digital age and the computer revolution" in order to gain operational superiority over Soviet forces, and later, over Russia and China.[37]

[35] David Gompert, "Freedom and Power in the Information Age," in Global Studies: The Changing Role of Information in War, ed. Zalmay Khalilzad and John White, Vol. 53 (Abu Dhabi: Emirates Center for Strategic Studies and Research, 2004), pp. 13–22.
[36] Robert R. Tomes, Ibid., p. 89.
[37] Robert R. Tomes, Ibid., p. 90.

Naturally, this intense pursuit of strategic superiority is driven by the distinct American strategic culture, characterized by an offensive mindset and a desire for dominance. Historically, this culture traces its roots back to the early settlers who conquered the "New World" and exterminated its indigenous inhabitants.

Fifth: Adapting to the Demands of the Information Revolution

The rapid advancements in precision military technology have necessitated the adaptation of institutional structures, combat doctrines, operational art, and tactics to the demands of the information revolution in military affairs. Due to its leadership and multi-level superiority in this field, the U.S. military is considered the pioneer in swiftly adapting to the requirements of digital warfare. The awareness of this need among American military commanders and strategic theorists is grounded in Carl von Clausewitz's proposition that "a sound theory of war never collides with reality."[38]

Indeed, superiority in warfare tools generates a strategic condition that compels military organizations to adapt rapidly, demanding change not only in their institutional frameworks but also in thinking, practical application, and combat conduct on the battlefield. This need for transformation and adaptation was expressed by General Eric K. Shinseki during the annual meeting of the U.S. Army Association on October 12, 1999, when he declared: "We are working to transform the Army as quickly as possible." His underlying assumption was that recent developments had laid the foundation for rapid and radical change under the banner of Army Transformation, aimed at making the military lighter, more agile in defeating adversaries, and less dependent on heavy and burdensome logistical support.[39]

This Army transformation process was envisioned to be driven by a combination of: information technologies, enhanced battlefield sensors, robotics, new equipment, and further innovations in doctrine, organization, and provisioning, all leading toward the creation of an entirely new combat force known as the Objective Force.[40]

[38] Thomas K. Adams, The Army After Next: The First Postindustrial Army (London: Praeger Security International, 2006), p. 07.
[39]Thomas K. Adams, Ibid., p. 08.
[40] Thomas K. Adams, Ibid., pp. 09–12.

From the perspective of Andrew W. Marshall (Director of the Office of Net Assessment within the U.S. Department of Defense during the 1990s), the transformation process targets three essential domains critical to building military effectiveness: technological innovation, operational concept (or doctrine), and organizational adaptation. While militaries are often inclined to imitate and resist change, the painful legacy of the Vietnam War, combined with the allure of emerging technologies, fostered a level of flexibility that paved the way for the emergence of new doctrines and strategic ideas. These include concepts such as systems of systems, information dominance, and asymmetric warfare.

All of these terms encapsulate major developments in military technology, such as precision-guided munitions, remote-controlled battlefield sensors, and reconnaissance satellites, which typically operate in synchronization through digital communications. This interconnectivity crystallized the concept of network-centric warfare as a central element of the information revolution in military affairs.

Combat adaptation and military transformation were not limited to technical or engineering domains. The process expanded, driven by urgent operational demands in modern warfare, to encompass the revision, development, and even creation of new strategies, doctrines, operational methods, and combat approaches. One doctrine that emerged from advancements in military technology is the concept of Active Defense, first innovated by the Israeli army and used during the 1973 war against Arab forces. It was later adopted by the U.S. Army in the early 1980s.[41]

According to Thomas K. Adams, Active Defense involves: “the full integration of all capabilities, land, sea, and air combat systems, along with rapid shifts of firepower and maneuver to concentrate decisive combat force at the right time and place on the battlefield.” Conceptually, Active Defense is built on a simple idea: that the best defense is a proactive offensive that targets enemy territory and strategic centers before they can be used in military action. This is achieved by deploying combat units across various sectors to produce the desired strategic effect. In other words, the optimal means of achieving strategic defense is through tactical offense.

Another innovation stemming from the impact of the information technology revolution in military affairs is the concept of the Information Army, closely tied to

[41] Thomas K. Adams, Ibid., pp. 12–13.

the digitalization of the battlefield. In fact, this concept is a necessary outcome of the increasing digitization of modern combat tools, particularly relevant to asymmetric warfare environments. One of its most prominent applications occurred during the U.S.-led international coalition's war against ISIS in 2014.

In the United States, the military structure that embodies the concept of the Information Army is known as Army XXI, which adopted capability-based operations in place of the former threat-based doctrine. The rationale behind this shift was the absence of a traditional external threat similar to the Soviet Union during the Cold War. Instead, the prevailing threat facing American military power had become the rise of terrorism, which struck deep into U.S. territory in 2001.[42]

Strategic priority for the Information Army was not centered on achieving strategic balance, as is the case in the realist tradition of strategic defense. Instead, it focused on confronting threats posed by actors that are unorganized, whose capabilities are unknown, and whose locations are undefined, yet are highly dangerous, with attacks that inflict deep and damaging blows to national security.[43]

Therefore, the core of military confrontation shifted to the accurate collection of information regarding such threats, their tracking, surveillance, the execution of carefully selected special operations, and ensuring civilian separation from military operations. These are all essential elements that characterize this particular combat environment. In this sense, information becomes the heart of the battlefield.[44]

In other words, the operational orientation moves toward the increasing digitization of the battlespace, through the preparation of an army that no longer relies on massive offensive power to break through enemy defenses, but instead operates by managing computerized systems and electronic sensors.

From a theoretical standpoint, uncertainty in the context of neorealism is addressed by increasing military force through numerical superiority and the accumulation of equipment. In contrast, for Army XXI, uncertainty is tackled through "emerging

[42] Thomas K. Adams, Ibid., p. 13.
[43] Thomas K. Adams, Ibid., p. 17.
[44] Kenneth N. Waltz, "Structural Realism After the Cold War," in Perspectives on World Politics, 3rd ed., ed. Richard Little and Michael Smith (London, New York: Routledge Taylor & Francis Group, 2006), pp. 101–11.

technologies that can enhance effectiveness across various future battlefields... This means that information technology connects sensors and combat units, microcomputers, and enabler units, contributing to situational awareness and allowing commanders to make fast and accurate tactical decisions."[45]

In this view, the armed forces become lighter, more agile, and capable of rapid deployment to areas of conflict and international crises. They are also more responsive to diverse unconventional threats in ways that align with the objectives of rapid dominance and control over the combat environment, while impeding or even preventing enemy attacks. Achieving this depends on skillful utilization of emerging technologies for expanded reconnaissance and enhanced intelligence-gathering capabilities. When deployment occurs, it must be supported by fast and effective logistical backing.[46]

More precisely, the digital army is prepared to realize what is known as Full-Dimensional Dominance, a mission that reflects modern armies' adaptation to the digital revolution in military affairs. This concept signifies the ability to deter or win conflicts during direct military intervention across all dimensions of military planning: strategic, tactical, operational, and intelligence/situational awareness of the battlefield. It also includes efficient handling of various forms of non-traditional threats such as counterinsurgency, counterterrorism, and everything falling under the term Operations Other Than War, typically associated with low-intensity conflicts in areas deemed to be vital spheres of state influence.[47]

Another noteworthy aspect of military transformation and adaptation, prominently observed during the Kosovo War of 1998, was the growing digitization of warfare, specifically through the use of the internet in military communications during combat. Soldiers became increasingly proficient in using digital communications, whether to obtain critical battlefield information or to transmit data back to command centers. This was achieved via complex communication systems linked to ground-based relay stations, satellite networks, and airborne platforms, all managed by a vast array of experts, specialized engineers, contractors, and consultants.

[45] John J. Mearsheimer, The Tragedy of Great Power Politics (New York, London: W. W. Norton & Company, 2003), pp. 33–55.
[46] Thomas K. Adams, Ibid., p. 18.
[47] Thomas K. Adams, Ibid., p. 19.

This interconnected system became known as the Tactical Internet, which ensured the smooth flow of information between central command, field commanders, and small unit leaders. Technically, the Tactical Internet includes "a networked radio system composed of the Enhanced Position Location Reporting System (distinct from GPS), a Single Channel Ground radio, and an Airborne Radio System."[48]

The widespread implementation of the Tactical Internet in the combat zone serves the broader goal of dispersing the fog of war, a challenge famously identified by Carl von Clausewitz, and aligns with the aim of attaining full situational awareness of the battlefield, as advocated by proponents of the info-communicative theory in strategic analysis. However, citing the benefits of digitization does not imply that all communication problems have been solved or that the challenges of uncertainty have been entirely overcome.[49]

Rather, battlefield units now face fewer difficulties in tracking enemy movements, anticipating possible surprise attacks, assessing the enemy's capacity for mobilization, and determining their ability to secure the necessary logistical support. Put differently, the Tactical Internet has enabled what is now widely referred to by strategic theorists and military analysts as the creation of the Operational Common Picture, achieved through the digitization of the battlefield.[50]

Sixth: The Fractures of the Information Revolution in Military Affairs

Despite the multiplicity of sources available for disseminating information about the battlefield environment, sources that appear instantaneous and unrestricted by governmental oversight, these sources themselves suffer from significant fractures in their credibility and coherence. They are often subject to manipulation, saturation, misinformation, exaggeration, and black propaganda, all employed in pursuit of particular strategic goals. Thus, instead of dispelling uncertainty, information can

[48] Thomas K. Adams, Ibid., p. 21.
[49] David Gompert, "Freedom and Power in the Information Age," in Global Studies: The Changing Role of Information in War, ed. Zalmay Khalilzad and John White, Vol. 53 (Abu Dhabi: Emirates Center for Strategic Studies and Research, 2004), pp. 13–24.
[50] Thomas K. Adams, Ibid., p. 22.

become a source of confusion among international actors on the one hand, and a tool for spreading fear and disarray among public opinion on the other.

A pertinent example of this fracture in the information revolution's role of clarifying battlefield realities is what the media dubbed the "Battle of Aleppo" in August 2016. During this episode, both the Syrian government and opposition factions vying for control over the northern city of Aleppo waged a parallel media war centered on the portrayal of military successes and failures. The conflict evolved into an information war more than a physical one, with each side claiming territorial gains or refuting those of the other, often inflating the significance of controlling an uninhabited street or village as if it were a major military breakthrough.[51]

In this context, the information revolution turns into a mechanism for generating suspicion and confusion, casting ambiguity over the actual events occurring on the battlefield. Suspicion, within the information age, stems from deception, disinformation, or what Clausewitz referred to as “the fog of war”, along with gray propaganda as identified by communication experts, and cognitive saturation of public perception with fabricated visuals and contradictions that lead to a general state of distrust in everything.

Proponents of cognitive theory in foreign policy analysis, Robert Jervis being a prominent example, have long discussed the epistemic and behavioral obstacles, and even technical limitations, that can hinder the delivery of appropriate information to decision-makers at the right time for proper response. These challenges include information overload, omission, excessive addition, concealment, data surplus, and the cognitive fatigue that affects personnel working on computers to receive and process data.

This was evident in sudden terrorist attacks in major cities around the world, despite these cities being equipped with extensive surveillance camera networks, as well as in online recruitment of fighters and clashes between armed groups and government forces in various conflict zones. Often, following tragic incidents, officials from ministries of defense or foreign affairs announce that they are working to identify the attackers and their motives, or issue warnings to the public about potential upcoming

[51] Abdellatif Hamza, Media and Propaganda (Baghdad: Al-Maaref Press, 1968), pp. 159–166.

attacks, which often never occur, since the timing and location of the attack are at the discretion of the perpetrators.

Worse still, there are numerous cases where terrorist groups publicly announce their intent to launch attacks against specific states or regions and then execute them as threatened. For instance, the Paris attacks carried out by ISIS on November 13, 2015, killed 149 people and injured 352, 99 of them critically. Likewise, ISIS executed three attacks in Belgium following the arrest of Salah Abdeslam on March 18, 2016, resulting in 34 deaths and over 230 injuries. These attacks occurred just three days after the arrest, on March 22, 2016.

Thomas Kane and his colleague provide a real-world example from World War II that underscores the critical importance of information in generating strategic advantage in actual war environments. During the North African campaign between the Allies and Germany, "General Montgomery received intelligence from Ultra [British intelligence], which made him aware of the severe logistical difficulties facing Rommel.

However, Montgomery's inherent caution prevented him from pursuing Rommel's forces with effective offensive vigor, thereby missing the opportunity to destroy them."[52] Thus, the challenge is not merely obtaining accurate information to secure military gains, but deploying that information effectively on the battlefield to neutralize, halt, or exhaust enemy forces, this being the objective and essential condition for winning a war.[53]

Quoting Gray, Kane and his co-author summarize the role of actionable intelligence: "As Colin Gray emphasized, it is good to have accurate information, but on its own, it does not destroy a single piece of enemy equipment." The same principle applies to the relationship between information and uncertainty: it is not the acquisition of data that matters most, but its use in dispersing the fog of war and forming a

[52] Robert Jervis, "Perception and Misperception in International Politics," in International Relations Theory: Realism, Pluralism, Globalism, 2nd ed., ed. Paul R. Viotti and Mark V. Kauppi (New York: MacMillan Publishing Company, 1993), pp. 286–99.
[53] Thomas M. Kane and David J. Lonsdale, Understanding Contemporary Strategy (London and New York: Routledge Taylor & Francis Group, 2012), pp. 77–78.

comprehensive and clear picture of the strategic environment and enemy capabilities, in line with the info-communicative theory of security construction.[54]

The emphasis on the idea that obtaining accurate information has neither operational nor strategic impact, nor does it inherently influence the combat environment or the course of war, unless accompanied by effectiveness in exploiting and employing that information to achieve tactical or operational objectives, underscores the enduring nature of warfare, regardless of the evolution or conceptual shifts brought by various military revolutions.[55] The Information Revolution in military affairs, like earlier revolutions, represents merely a phase in the ongoing evolution of strategic-military affairs at the levels of tools, concepts, and methods. However, the essential nature of war remains unchanged as an act of violence involving the use of weapons to accomplish political aims.

According to Clausewitz, the nature of war comprises four elements that persist across time and space, regardless of how combat tools, methods, or tactics develop. These elements are: engagement with the enemy, the climate of war, and the polymorphic character of warfare. Together, they form the enduring structure of war throughout strategic history.[56]

From a critical standpoint, the Information Revolution in military affairs has not altered the intrinsic nature of war. Instead, it has added further layers of complexity to combat methods and tactics. While it may have reduced human casualties, it simultaneously escalated security concerns and expanded their scope to encompass both military personnel and civilians. In effect, it has drawn civilians into the battlefield alongside the military, as in the case of cyber warfare in the digital domain.

Conclusion

[54] Thomas M. Kane and David J. Lonsdale, Understanding Contemporary Strategy (London and New York: Routledge Taylor & Francis Group, 2012), p. 79.
[55]David Gompert, "Freedom and Power in the Information Age," in Global Studies: The Changing Role of Information in War, ed. Zalmay Khalilzad and John White, Vol. 53 (Abu Dhabi: Emirates Center for Strategic Studies and Research, 2004), pp. 13–24.
[56] Thomas M. Kane and David J. Lonsdale, Understanding Contemporary Strategy (London and New York: Routledge Taylor & Francis Group, 2012), p. 80.

Clausewitz captured one of the manifestations of the unchanging nature of war with the term "the climate of war", which includes the elements of danger, uncertainty, exhaustion, and opportunity. In other words, the contextual conditions of warfare reveal it to be an inherently complex process with multifaceted dimensions.[57]

The Information Revolution, with its advantages and fractures, has merely added more complexity to the equation: in combat methods, operational art, and tactical approaches. Inevitably, this has led to the emergence of compound military strategies, strategies that incorporate an undefined array of factors, components, considerations, and operational domains.

[57] Thomas M. Kane and David J. Lonsdale, Understanding Contemporary Strategy (London and New York: Routledge Taylor & Francis Group, 2012), p. 81.