National Security and the Third-Road Threat

Toward a Comprehensive Theory of Information Warfare

Daniel Morabito*

Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.

Giulio Douhet, *The Command of the Air*

The United States is losing an information war with its competitors. China and Russia have attacked the United States for decades, costing our country billions of dollars. These activities have sown division, extremism, and violence among the American people, and undermined societal norms and democracy. Despite this national security threat, the US government remains poorly organized to employ its information instruments of power. The US military in particular lacks a unified theory, definition, doctrine, and organizational structure for information warfare (IW).

Early Information Advantage

Information has been a vital component of warfare since the earliest recorded battles. In the 1469 BC Battle of Megiddo, the Hyksos King of Kadesh, who led a revolt of Palestinian and Syrian tribes against the Egyptian pharaoh, Thutmose III, was missing critical information as to the disposition of the Egyptian army.[1] Anticipating an Egyptian attack on the stronghold city of Megiddo, the Hyksos king assessed the large Egyptian army would likely approach using one of two larger roads to the east and west of the city, and he divided his forces to intercept them. Using information gained from his scouts and discerning that the rebel leaders expected him to approach by these two broad roads, Thutmose instead chose a third, narrow road that led to the south of the city.[2]

The pharaoh's advisors begged him not to use this road, as it was only 30 feet wide in places with heights on either side that would invite an enemy ambush. Had the rebel army chosen to acknowledge their vulnerability and position themselves defensively on this third road, they would have had a tremendous

*A version of this article first appeared as a three-part series in Over the Horizon, the digital journal of the USAF Air Command and Staff College.

advantage. They might have defeated the Egyptian army or forced them to withdraw. Too late, and with their army divided and focused to the east and west, the rebels "realized that their enemy had done the thing they had not calculated on and had surprised them."[3]

The pharaoh's early information advantage and the rebel army's failure to acknowledge the third-road threat allowed the Egyptians to establish a positional advantage relative to large portions of the rebel army that were then caught outside their city and cut off from reinforcements. It also enabled a cognitive advantage—surprise—over the occupants of the city and the divided army outside. The Egyptians, using their positional advantage gained through information advantage, overwhelmingly defeated the divided army, laid siege to the city, and captured it.[4]

When news of the rebel army's crushing defeat reached the remaining Mesopotamian cities that had not yet joined the rebellion, they were deterred from joining the Hyksos king and voluntarily sent tribute to Thutmose indicating they did not want war, further evidence of how actions in the information environment reverberate throughout other domains to influence attitudes and behaviors. Having forged its reputation as a military power at the Battle of Megiddo, Egypt established itself as the regional hegemon for the next two decades.[5] This, the first recorded battle of history, illustrates how the interplay of information across all domains contributes to decisive effects at the tactical, operational, and strategic levels. Furthermore, it reveals the ability of information to establish advantages across other instruments of power.

The Enemy Lies at Your Fingertip

> *The skillful leader subdues the enemy's troops without any fighting; he captures their cities without laying siege to them; he overthrows their kingdom without lengthy operations in the field. . . . Without losing a man, his triumph will be complete.*
>
> Sun-Tzu, *The Art of War*

Military power projection as a function of information, distance, and geography has shaped the character of war from the first recorded conflicts to today.[6] As warfighting technology evolves, the speed at which a combatant can traverse space and attack an adversary has increased tremendously, with each conflict and technological advancement altering the character of war.[7] Given recent advances in high-speed network connectivity and information technology, geography and distance no longer protect the United States from direct and persistent information-based attacks. The global trend toward faster data transfer across increasingly connected devices—the so-called internet of things—means adversaries now maintain a presence in American homes, delivered through smartphones and other technology.

Within this rapidly evolving information environment, China and Russia are waging information wars against the United States calibrated to advance their national interests while avoiding direct and decisive military conflict with the West. Their strategies center on exploiting America's emphasis on free speech and freedom of the press which, by constitutional mandate, may not be infringed except under extraordinary circumstances. Consequently, the information environment competitive space is ill-suited for Department of Defense (DOD) intervention, exposing a gap in civilian and military thinking about how to defend the nation.

The US military's power comes from those it represents—the attitudes, knowledge, and beliefs of the American people are a national center of gravity and strategic concern. A consequence of the deluge of competing adversarial narratives, delivered by America's enemies through the internet of things, is that many Americans cannot discern between fake news and truth. This flood of narratives leaves the population misinformed, uncertain, and prone to attitudes, knowledge, and beliefs shaped by social media filtering and bias.[8]

Simultaneously, the American military prioritizes preparing for large-scale combat operations to deter near-peer military competitors and, if conflict occurs, to win decisively.[9] This focus leaves the Department of Defense ill-prepared and poorly postured to counter peer competitors in the information environment, lacking doctrine, an organization, and even a definition for information warfare. Meanwhile, America's enemies use the ubiquitous connectivity of the internet to bypass the country's traditional military defenses, directly and maliciously sowing division and mistrust among the American people on an unprecedented scale.

The US government must aggressively pursue social, legal, and organizational change to counter these enemies within the information environment. To do this effectively, it must understand how IW is used against the United States today as well as how it may be used in the future. While the US government struggles to understand and counter this form of warfare, the Department of Defense must buy time for US democracy to adapt to this new fight by developing a unified theory of information warfare that robustly informs how it competes both within the information environment and across the continuum of military conflict.

Information Warfare Theory

> *The aggressor is always peace-loving (as Napoleon Bonaparte claimed to be); he would prefer to take over a country unopposed.*
>
> Carl von Clausewitz, *On War*

Using information for military advantage is as old as the earliest recorded battles, yet defining the phenomenon as a type of warfare has proven frustratingly

elusive.[10] The phrases information warfare and information operations (IO) are often used interchangeably, with little clarity as to what they mean and how they manifest across the competition continuum.[11] Joint doctrine provides no definition for IW and defines IO as "the integrated employment, during *military operations*, of *information-related capabilities* in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own [emphasis added]."[12] This definition is lacking as it constrains IO to "military operations" and describes the phenomenon using presupposed "information-related capabilities."

Similarly, the US Air Force recently described information warfare as "the employment of *military capabilities* in and through the information environment to deliberately affect adversary human and system behavior and preserve friendly freedom of action during cooperation, competition, and conflict [emphasis added]."[13] This description is also lacking because it defines IW based on presupposed "military capabilities."

Both definitions describe IW and IO from military perspectives within the system they seek to understand. This is a mistake as, according to military theorist John Boyd, "one cannot determine the character or nature of a system within itself."[14] Such efforts generate confusion and disorder, ultimately impeding action and magnifying friction. As a result, both definitions do little to illuminate how the United States and others might compete within the information environment using novel capabilities across the continuum of military conflict.

The US military lacks a sufficient, comprehensive doctrinal understanding of IW, resigning IO to a mere tertiary function supporting the primary focus of large-scale combat operations. For example, the December 2020 release of Joint Publication 5-0, *Joint Planning*, makes only a single reference to information operations, describing it as an example of "requested military flexible deterrent options" without elaborating on what that means or how it should be integrated into Joint planning.[15]

Joint Publication 5-0 makes meager efforts to include information environment considerations during Joint planning by adding a statement that "the Joint force synchronizes operations in the information environment to shape the perceptions, decisions, and actions of relevant actors" and adds "information environment (including cyberspace), and electromagnetic spectrum" considerations within the course-of-action development step of the Joint planning process.[16] Meanwhile, China and Russia have already operationalized IW theory and integrated it into their operational art, considering information warfare sufficient in its own right to triumph in competition below the threshold of armed conflict.[17]

United States military doctrine must define IW based on the phenomenon's basic elements and emergent properties. Such a definition will inform capability development and employment based on the broader nature and character of the information environment, rather than unnecessarily constraining IW thought to expressions of preexisting military capabilities.

The next section posits a theory of IW from its most basic elements through its implementation as a weapon used to support national interests. It reveals IW as a manifestation of the Clausewitzian clash of wills expressed through competing narratives and shaped by access, trust, and cognition.[18] The section concludes with a proposed novel information warfare taxonomy, definition, and theory of victory.

Constructing Knowledge

In order to define information warfare, one must understand how data, information, and knowledge interact within information ecosystems to create individual and shared perceptions of reality. Data, the most abstract form of information, is derived from individual processes of observation, measurement, or sensing. Data can be quantitative or qualitative but has minimal to no relational information or context. The binary encoding of information used by computers and the internet are excellent examples of data that is unintelligible until it is converted into information through the addition of context.

Information is less abstract and consists of data organized by relational context through processes of sorting, classifying, or indexing. This process of the relational grouping of data based on context is the most primitive form of intelligence. As such, the informational content of each data object is higher than pure data alone. Information paired with an intended receiver is called a message.

Knowledge exists in the thought-world of the observer as a theoretical description of a phenomenon under study.[19] It is a mental model of an observed phenomenon or interpretation of information.[20] Access to the phenomena or information about it is thus a requirement for knowledge creation. Knowledge is formed by cognition of the static and dynamic relationships of information informed by context, emotion, and exposure to past observations.[21] The accuracy of knowledge is probabilistic and must be continuously assessed against new observations to infer its relative validity, a measure of trust. Valid knowledge infers predictability of the observed phenomenon, presenting a kind of foresight.

Cognition, the conversion of information to knowledge, is continuous and occurs through conscious and unconscious reasoning, phenomena described by Daniel Kahneman's two-systems theory. System 1 thinking uses heuristics to quickly filter information and reach conclusions subconsciously and with minimal effort. System 2 is deliberate, conscious thinking that requires one's attention and

effort and which produces some level of cognitive strain.[22] Although fast and less effortful, System 1 thinking is especially problematic as it actively filters information that does not fit one's preconceptions of reality, reducing one's likelihood of discovery and reinforcing preconceived notions.

Finally, cognition includes emotive factors and can answer questions about what one feels about what they think, and about what one knows about what they feel. As illusionists have known for centuries, the cognitive features of human biology can be hacked or tricked to induce people to reach perceptions in their thought-world that are entirely unsupported by reality.

Access, trust, and cognition are necessary for knowledge creation and are therefore fundamental to the information environment. This suggests a novel model for visualizing the information environment with knowledge as the emergent property of the integration of the fundamental elements (fig. 1).

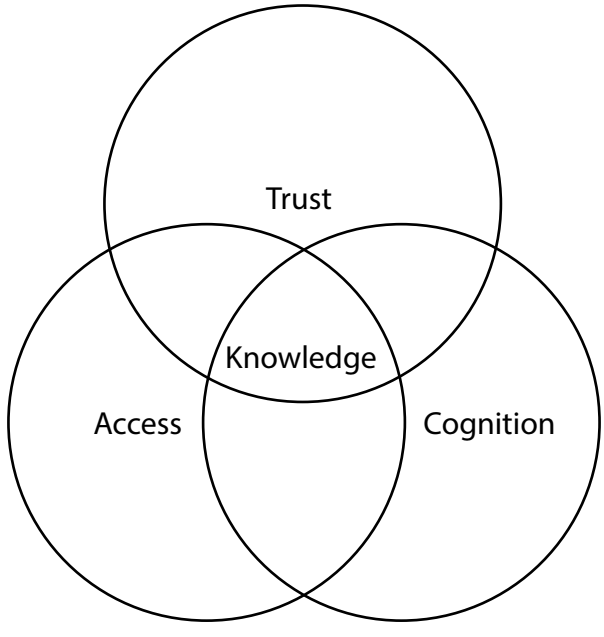

Figure 1. Fundamental elements of the information environment
Created by the author

This unique model defines the information environment using the fundamental elements of knowledge rather than defining it as a combination of "dimensions" paired with pre-existing military capabilities as is seen in Russian, Chinese, and American military conceptions.[23]

Data, information, and knowledge exist within a global super information ecosystem comprised of all the smaller information ecosystems, which may overlap

or exist independent of one another. These information ecosystems are the physical and social information environments that people interact with and inhabit. The physical information ecosystems are the worlds people inhabit and can be directly and immediately observed. The social ecosystems extend people's perceptions to the broader world, well beyond their immediate environment, through social interactions and access enabled by means of communication such as writing and the internet. Fragmentation of information ecosystems occurs when access between ecosystems is reduced or does not exist.

It is important to emphasize that the preponderance of people's individual knowledge about the broader world is obtained through social interaction with others. This concept is often referred to as "the sociology of knowledge," where the individual's perceived reality, apart from that personally experienced, is "socially constructed."[24] In order to reduce uncertainty, the social construction of knowledge requires access to the social ecosystems of others, along with trust in the validity of shared information. Finally, the persistence of shared knowledge creates norms that can harden within people's mental models into heuristics that may or may not accurately fit one's continuously evolving environment, creating bias. The attributes of fragmentation, uncertainty, and bias comprise the first three problems of knowing.

Problems of Knowing

Three problems of knowing—fragmentation, uncertainty, and bias—emerge from the dysfunction or denial of the three fundamental elements of the information environment: access, trust, and cognition. Three additional problems emerge from vulnerabilities within the interplay of overlapping fundamental elements—root of trust, misinformation, and filtering. Combined, the six problems of knowing define the vulnerability space within the information environment model. As such, they are also described as attack vectors and are required for theorization about IW capabilities.

Fragmentation. As previously noted, information ecosystems are fragmented relative to other ecosystems when they have few or no connection paths between them. Fragmentation is categorized as physical, sociostructural, or voluntary. Physical fragmentation occurs as a consequence of the geographic separation of people groups. An instance of physical fragmentation resulting in surprise would be the "discovery" of the New World by Christopher Columbus. Similarly, the sight of a Western European was "new" to the indigenous North Americans as this knowledge was absent from their information ecosystem.

Sociostructural fragmentation occurs from efforts to control or deny information to others to preserve power hierarchies, worldviews, or paradigms. An ex-

ample of this fragmentation is the trade guilds of the Middle Ages that sought to reduce trade competition through the preservation of specialized knowledge and craftsmanship. In today's information-centric society, sociostructural fragmentation includes the use of multilevel information security policies that preserve confidentiality through application of access controls.[25] Voluntary fragmentation occurs as an outward expression of rejecting unwanted information. Individuals may voluntarily attempt to avoid information from intruding into their ecosystems by deliberately cutting themselves off from it. Examples include ignoring or avoiding disturbing or degrading phenomena.

Filtering. Another problem of knowing emerges from the interaction between access to information and the heuristics that support cognition. Filtering occurs when a second party controls which information gets delivered to a person or when the information delivered to a person is ignored due to their heuristics. This problem is especially challenging because the information previously experienced by a person solidifies their heuristics. In turn, these heuristics can subconsciously filter out information that does not match preexisting mental models, a function of System 1 thinking also described as confirmation bias. Confirmation bias creates a reinforcement loop that continuously filters new information that does not match pre-existing bias until something occurs that does not match the preexisting mental model but that demands System 2's attention.

Uncertainty. A third problem of knowing is if and how much a person can trust the validity of information gleaned from others, which manifests itself as uncertainty. Since most knowledge comes from others instead of one's own personal observation and creation, trust is a measure of the validity of information received from others.[26]

Root of trust. A fourth problem of knowing, root of trust, exists within the interplay between the elements of access and trust and the problems of fragmentation and uncertainty. The root of trust problem extends directly to the discipline of information management where practitioners are concerned with the confidentiality, integrity, and availability of information. Among many threats, cybersecurity analysts concern themselves with preserving the integrity of data using check bit, hashing, and encryption algorithms to avoid data manipulation that could impact future information and knowledge. Of course, one must also trust the algorithms themselves are effective and have not been tampered with, and then one must also trust the hardware the algorithms use for their calculations, which means one must trust the hardware designers and manufacturers.

This multilayered trust hierarchy problem, often referred to as the "root of trust problem," was foreseen as far back as 1984 when computer science pioneer Ken Thompson published "Reflections on Trusting Trust."[27] The theoretical answer to

ensuring high truth and low uncertainty requires the validity of information is not assumed if it was not personally created, and yet the overwhelming preponderance of information people continuously rely on comes from and is created by others. Human perceptions are based on trusting information from others who, in turn, base their perceptions on trusting information from others. As several security researchers have metaphorically described trust, "it's turtles, all the way down."[28]

Bias. A fifth problem of knowing, cognitive bias, is a consequence of how the human brain employs heuristics to interpret the environment while minimizing distractions and cognitive strain rapidly and efficiently. A heuristic is a cognitive shortcut that allows the subconscious, System 1, to reach a quick and reasonably accurate conclusion despite time constraints or limited information.[29] Some heuristics are innate to human nature while others are developed through repeated exposure to ideology, phenomena, or emotional events.[30] The problem of heuristics arises when the brain uses them to reach conclusions unsupported by reality. Further, when heuristics fail, the failures are unlikely to be detected until a significant event forces one's conscious thinking to recognize the mistake. This failure is called cognitive bias.

Social psychologist Jonathan Haidt identified especially powerful heuristics that are relevant to information warfare due to their strong ability to motivate individuals and groups. Haidt asserts there are "six psychological systems that comprise the universal foundations of the world's many moral matrices."[31] Each of his six moral psychological systems is labeled with value and antivalue pairs, where values are desired or accepted traits and antivalues are traits or actions that moral intuition rejects. These six foundations are care/harm, liberty/oppression, fairness/cheating, loyalty/betrayal, authority/subversion, and sanctity/degradation.

What makes this theory significant is that it provides a framework for understanding how moral biases influence global populations. In particular, the theory describes how groups use morality to motivate and order their societies according to social systems.[32] "Moral systems are interlocking sets of values, virtues, norms, practices, identities, institutions, technologies, and evolved psychological mechanisms that work together *to suppress or regulate self-interest and make cooperative societies possible* [emphasis added]."[33]

When it comes to power, the concept of a moral high ground is an appropriate metaphor since moral foundation biases shape how people interpret the world and motivate the actions they take within it, giving a moral positional advantage to some at the expense of others. These moral matrices shape people's biases and bind them into cooperative groups with shared values. At the same time, they blind people to the perspectives of others.[34]

This dynamic is important because if one understands the moral heuristics which drive a group of people, one can selectively present them with information that exploits and amplifies their naturally occurring potential for biased thinking and thus manipulate their behavior. In this way, bias can be weaponized to change behavior, potentially to violent extremes. Haidt's moral framework-based heuristics are just some of many heuristics that may exist within a population. Their relevance lies in their seemingly universal applicability to human behavior and potential for weaponization.

Misinformation. A sixth problem of knowing—misinformation—broadly captures subcategories of incorrect information, regardless of intent. When used to refer to a specific incident of false information, misinformation is generally assumed to be false information that is created or shared without the intent of causing harm. But when harm is intended, the subcategories of disinformation and malinformation are used. Disinformation "is an intentional spreading of misinformation in pursuit of a purpose-driven outcome."[35] Malinformation is data that reflects reality but is presented in a contextually misleading way.[36] In each case, the information is shared in the form of a message, manifesting itself in many different forms such as oral or written stories, images, and videos.

The proliferation of social media creates a global IW battleground in which, according to some researchers, "the defining feature is that messages are the munition."[37] These messages shape knowledge to align with or counter narratives—individual and shared stories people use to establish and reinforce mental models while making sense of perceived information. Finally, "propaganda" is misinformation used to "promote or publicize a particular political cause, ideological perspective, or agenda."[38]

Information Warfare Taxonomy

The elements of the IW theory outlined above are visualized beginning with the IW trinity, which positions individual and group perceptions of knowledge in the center of three overlapping rings of trust, access, and cognition (fig. 2). The six attack vectors of fragmentation—root of trust, uncertainty, misinformation, bias, and filtering—are shown as arrows pointing toward the IW elements that they exploit to create effects within the center. The resulting graphic depicts a taxonomy of IW.

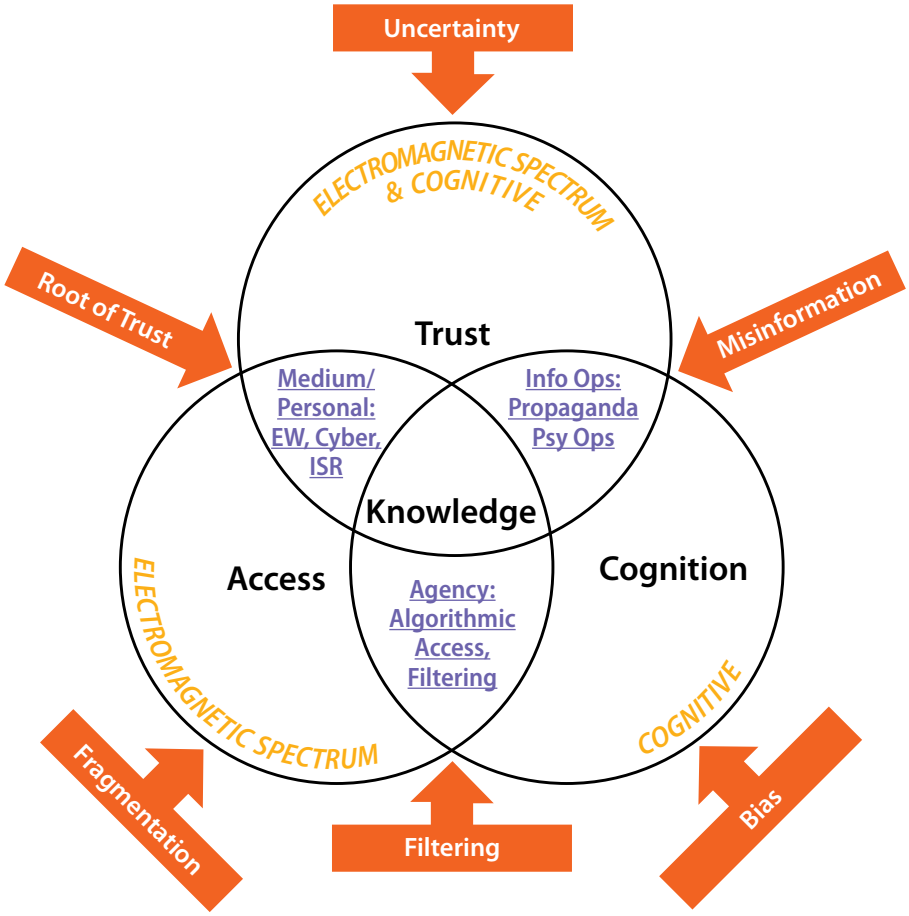

Figure 2. Taxonomy of information warfare
Created by the author

The graphic posits three unique inferences. First, the information warfare environment is a blend of two domains, the cognitive domain imbued with trust and cognition, and the electromagnetic spectrum domain, which serves as the medium for information transfer and extends cognitive expressions of trust into the electromagnetic spectrum (in italics, fig. 2).

Second, three unique areas of overlap exist between each pair of rings that exclude the third ring. These areas possess unique characteristics and attack vectors. A nonexhaustive list of characteristics within each overlapping area is underlined for clarity. Finally, all three rings exist simultaneously. The character of each ring is continuously shaped by its relationship and interactions with the other two.

This taxonomy is a new way of conceptualizing IW based on its fundamental elements. These elements make up the IW trinity and reveal six IW attack vectors

that exist across the full spectrum of information conflict. The result is a theoretical foundation that supports and informs a richer definition of IW.

Information Warfare Defined

Given this theoretical foundation, the article proposes the following working definition: Information warfare is the manipulation of knowledge through access, trust, and cognition to change the attitudes or behaviors of an individual or system. The aim of this definition is attitudinal or behavioral change, a concept not captured in a single English word, but one conceptualized within the Greek word *metanoia*, a "shift in mind" caused by new information or a new perspective and corresponding to a change in behavior.[39] Metanoia is the nature of IW.

This definition is supported by the three fundamental elements of the information environment—access, trust, and cognition. In contrast to the Air Force description, this definition allows capabilities to be developed across all instruments of power to achieve effects throughout the IW taxonomy, regardless of the level of competition. Notably, this definition accommodates current US military information warfare functions of cyberspace; intelligence, surveillance, and reconnaissance; electromagnetic warfare; electromagnetic spectrum management; and IO.

Simultaneously, this definition achieves overlap with the IW doctrine of America's competitors, such as Russia's *informatsionnaya voyna* (information war) functions of network operations, electronic warfare, psychological operations, and IO, and China's concept of "Informatized War," which privileges information advantage within the cyber, space, and electromagnetic domains.[40]

Crucially, the secondary regions of overlap reveal a conspicuous area of the triad not currently captured as a US doctrinal IO function or information-related capability. This space—the overlap of the fundamental elements of access and cognition—is where both physical and cognitive filtering mechanisms operate. This is significant because "the highest forms of communicative-based power in networked societies are the abilities to set the parameters for and guide the directional flow of discussions taking place within the network."[41] In this area of the triad, external filtering trains cognitive heuristics which, in turn, filter out information inconsistent with current mental models.

This suggests a role within IW for managing this battlespace that manipulates the relationship between fragmentation and bias and that can be heavily influenced by human-machine filtering such as machine-learning algorithms. In contrast with the United States, this is an IW function that US adversaries, particularly Russia and China, are already aggressively pursuing.

Theory of Victory

Like conventional warfare, the objective of IW is to achieve political objectives by coercing the enemy to do one's will.[42] But in contrast to the direct violence associated with conventional war, IW seeks to achieve its objective primarily by manipulating the fundamental elements of access, trust, and cognition.

Similarly, as the ultimate aim of conventional war is to disarm the enemy to impose one's will, the ultimate aim of IW is to disable the enemy's ability to use data, information, and knowledge to achieve its objective.[43] This aim is achieved when "the previous direction of messages [which inform and motivate] a political or military effect is . . . changed," thereby establishing a strategic, operational, or tactical information advantage.[44] China's theorists seem to agree, having stated in their 2013 *Science of Military Strategy* publication that information dominance is achieved when friendly forces can "seize and preserve the freedom and initiative to use information [while] simultaneously depriving an opponent" of the same.[45]

China's Information War

> *Most importantly, we must concentrate our efforts on bettering our own affairs, continually broadening our comprehensive national power, improving the lives of our people, building a socialism that is superior to capitalism, and laying the foundation for a future where we will win the initiative and have the dominant position.*
>
> Xi Jinping, speech to the Chinese Communist Party, January 5, 2013

The Chinese Communist Party (CCP) has clear, ambitious goals to solidify its long-term political control over China while securing increased global influence at the expense of the United States. According to the 2017 *US National Security Strategy*, China is first among nations competing with the United States for global influence as it seeks to "shape a world antithetical to US values and interests."[46]

The Biden administration considers China "the only competitor potentially able to mount a sustained challenge to a stable and open international system."[47] Most recently, Chinese media reported that President Xi Jinping considers the United States to be "the biggest source of chaos [and] the biggest threat to China's development and security."[48] China seeks to "displace the US in the Indo-Pacific region, expand the reaches of its state-driven economic model, and reorder the region in its favor."[49] Globally, China seeks to supplant the United States as the world's superpower while securing access to energy reserves and other vital national interests that will bolster China's continued growth.

After a perceived "century of humiliation," China sees itself as an ancient power, oppressed by foreigners but destined to return to preeminence as a regional hegemon. The CCP touts itself as "heir to a great civilization."[50] Led by Xi, the CCP

seeks power through "Socialism with Chinese Characteristics," achieved through a narrative of China's rejuvenation.[51] The CCP seeks to fundamentally revise the world order and international norms in a way that places China in the center and serves the party's "authoritarian goals and hegemonic ambitions" through the establishment of a socialist international order.[52] The party intends to displace "the United States as the world's foremost power and restructure the world order to conform to the CCP's distinctive way of empire."[53] This is the objective of the China Dream, China's century-long unifying goal of restoring itself to preeminence by 2049.

China is an especially formidable IW adversary because the CCP believes it can "achieve its objectives through methods other than the use of brute military force."[54] With its propaganda-laden Marxist past, authoritarian present, and ambitious future, the IW trinity and attack vectors present an elegant way for China to achieve Sun Tzu's supreme art of war: "subdue the enemy's army without fighting at all."[55] This is especially true against an American adversary slow to confront the vulnerabilities inherent to the information environment relative to the Department of Defense and to the fundamental American values of freedom of speech and freedom of the press.

From its inception, the CCP used misinformation to achieve its political ends, considering thought management and propaganda against its own citizens to be the "lifeblood of the Party."[56] Mao Tse-tung, chairman of the CCP and founder of the People's Republic of China, overtly advocated for propaganda stating, "we should carry on constant propaganda among the people . . . so that they will build their confidence in victory."[57] The CCP organizes its misinformation efforts through many bureaucratic government organizations focused on its internal citizenry and on the populations of other countries. The United Front Work Department is one such organization and is responsible for "building support for the CCP and its policies among domestic ethnic groups, religious groups, the worldwide Chinese diaspora, and political, economic, and social elites in Hong Kong, Macao, and Taiwan."[58]

According to a 2019 Office of the Secretary of Defense report to Congress, "China conducts influence operations against media, cultural, business, academic, and policy communities of the United States, other countries, and international institutions to achieve outcomes favorable to its security and military strategy objectives . . . [the party] seeks to condition foreign and multilateral political establishments and public opinion to accept China's narrative."[59]

An example of this influence is the Ministry of Culture and Tourism that filters exposure to China's country and culture by arranging free and low-cost trips for journalists, politicians, sports stars, and other social influencers who might be

willing to present a noncritical view of China when grassroots foreign support is needed.[60] Simultaneously, China denies access to individuals and corporations who portray China or the CCP in a negative light or who express sympathies contrary to China's interests.[61]

This aggressive filtering extends to China's printing industry that openly censors books printed within the country for export by demanding the removal of content that portrays China negatively or that does not align with its strategic goals.[62] Such censoring extends to the US sports and movie industries where threats to deny filming and lucrative distribution opportunities in China influence US production decisions while suppressing opinions counter to China's aims.[63] It is notable that Hollywood hasn't made a movie critical of China since 1997. Recently, China's National Film Administration directed the country's cinemas to show propaganda films a minimum of twice per week to commemorate the CCP's centennial anniversary.[64]

These efforts contribute to China's whole-of-government approach to achieving its national interests. To that end, China's Science of Military Strategy doctrine includes a section on "effective control," which describes the need to "energetically grasp military struggle while coordinating with political, economic, cultural, and diplomatic means under unified national deployment."[65] China's response to the COVID-19 pandemic provides a below-the-threshold-of-war example of how it applies the IW trinity and attack vectors to achieve effective control.

Under the CCP's guidance, China's informatized organizations used all means at their disposal to shape public opinion by controlling access to information, generating uncertainty about narratives that depicted China negatively, and appealing to the biases in each targeted population through misinformation.[66] China's filtering and fragmentation of information from health experts and journalists, its global delivery of misinformation narratives using social and mainstream media, and its efforts to generate uncertainty about the nature of the virus all demonstrate the aggressiveness and robustness of China's IW capabilities.[67]

Further, China seeks information advantage through hacking and other illegal access to advanced technologies and trade secrets from companies, universities, and the defense sectors of multiple nations. China's intellectual property theft has cost the United States approximately $250 billion per year over the past decade, with amounts in some years exceeding $600 billion. China's annual intellectual property theft approaches the US military's annual defense budget and exceeds the total profits of the top 50 US companies.[68] It has been called "the greatest transfer of wealth in history."[69]

The benefits to China include access to specialized knowledge, enabling it to pursue additional information advantages against governments, organizations, and

persons across the globe.[70] Indeed, China's sustained efforts to gain access to the intellectual property of the breadth of US industry and defense contractors may compromise the root of trust of US hardware and software systems, generating uncertainty about the reliability of US networks and infrastructure. Finally, the scale of this intellectual property theft presents the possibility that China may have more information about US weapon system capabilities and vulnerabilities than that possessed by the US government.[71]

Finally, the CCP prepares its army to win Informatized Local Wars between information-based opponents.[72] Xi restructured the People's Liberation Army (PLA) in 2015, including standing up the Strategic Support Force which conducts many aspects of IW, including intelligence, technical reconnaissance, cyberespionage, cyberattack, cyberdefense, electronic warfare, and aspects of information technology and management.[73]

Some researchers claim when Xi speaks of a "fully modernized force in 2035," he "no doubt envisions a PLA capable of conducting joint informatized operations in the context of systems-destruction warfare, giving the CCP a tool to achieve political objectives while controlling the scope and scale of conflict."[74] The PLA sees the information domain as "first and foremost in importance." It treats information dominance in the form of controlled and persistent access within the cyber, space, and electromagnetic spectrum domains early in a conflict as a pretext for achieving victory, while seeking to fragment or otherwise deny the same to its enemies.[75]

China has a robust IW capability honed from decades of IO performed against its domestic population and overseas adversaries. It is adept at using all elements of IW to achieve information advantage. This information advantage supports every Chinese national interest, and every national interest serves to reinforce the legitimacy and stability of the authoritarian CCP regime.

Recommendation

> *Our open economies and open societies have allowed the CCP to have an undue influence on our public sphere. . . . It will take recognition of this influence and a major strategic adjustment to correct this.*
>
> Anne-Marie Brady, "China Wants Face and We Are Left with the Cost"

A recently declassified intelligence report determined the United States "has not sufficiently adapted to a changing geopolitical and technological environment increasingly shaped by a rising China and the growing importance of interlocking non-military transnational threats. . . . Absent a significant realignment of resources, the U.S. government . . . will fail to achieve the outcomes required to enable continued U.S. competition with China on the global stage for decades to come, and

to protect the U.S. health and security."[76] The United States is unable to effectively compete within the information environment due to a "lack of bureaucratic coherence and leadership."[77] Meanwhile, every American is vulnerable to information warfare as an unwitting victim within the information environment.[78]

To reverse this trend, the United States must define information warfare in a way that empowers a doctrinal framework for thinking, communicating, planning, and acting within the information environment while organizing to meet the threat.

This article presents a novel theory of IW constructed using first principles of information theory to create a comprehensive IW taxonomy that includes the IW trinity of access, trust, and cognition, along with six IW attack vectors. This taxonomy provides a solid foundation for conceptualizing information warfare and informs how the United States defends itself while pursuing national interests within the information environment. This theory should be extended to create robust IW doctrine that elaborates upon the full IW taxonomy.

Conclusion

> *These events were not the products of ineluctable forces outside the boundaries of human choice; they were the results of decisions and actions by people who had opportunities to choose and act otherwise.*
>
> D. H. Fischer, *Washington's Crossing*

Shortly after Russia used information warfare to tarnish the American election process in 2019, the CCP proved the profound danger it presents to itself and to the world in its deliberate mishandling of COVID-19.[79] The same "you die, I live" worldview is using IW to pursue information advantage in artificial intelligence, quantum computing, robotics and automation, space, oceanic engineering, biotechnology, advanced pharmaceuticals, and next-generation energy and power generation. Both countries continue to use IW to directly support their national interests while damaging and discrediting their global competitors, including the United States.[80]

The lessons from the Battle of Megiddo apply today as they did 3,500 years ago. The focus and capacity of America's instruments of power stand divided between competing with China and Russia militarily and economically. These are the two roads on which the United States expects their approach. The IW fight is America's third road, and it leads deep into the nation, directly to the hearts and minds of its citizens—the US government's center of gravity. The United States must orient itself to counter how China and Russia are choosing to fight—information warfare. We ignore it at our peril. ✪

Daniel Morabito

Lieutenant Colonel Daniel "Plato" Morabito, commander of the 834th Cyberspace Operations Squadron, 67th Cyberspace Wing, Joint Base San Antonio, Texas, holds a master of science in leadership and information technology from Duquesne University, a master of science in cyberspace operations from the Air Force Institute of Technology, a master of military operational art and science from the USAF Air Command and Staff College, and a master of arts in military operations from the US Army Command and General Staff College.

Notes

1. Richard Dupuy and Trevor Dupuy, *The Encyclopedia of Military History: From 3500 BC to the Present* (New York: Harper and Row, 1970), 5.
2. Eric H. Cline, *The Battles of Armageddon: Megiddo and the Jezreel Valley from the Bronze Age to the Nuclear Age* (Ann Arbor, MI: University of Michigan Press, 2002), 18–19.
3. Harold Hayden Nelson, *The Battle of Megiddo* (Chicago: University of Chicago Press, 1913), 38.
4. Nelson, *The Battle of Megiddo*, 22–38.
5. Dupuy and Dupuy, *Encyclopedia of Military History*, 6.
6. Jeffrey M. Reilly, *Operational Design: Distilling Clarity from Complexity* (Maxwell AFB, AL: Air Force Research Institute, 2012), 21–23.
7. James J. Schneider, *Vulcan's Anvil: The American Civil War and the Emergence of Operational Art,* Theoretical Paper No. 4 (Fort Leavenworth, KS: School of Advanced Military Studies, 1995), 10–11.
8. Sara Kitsch et al., *Quick Look: Inoculation Theory*, (Stillwater: The Media Ecology and Strategic Analysis Group (MESA), School of Media and Strategic Communications, Oklahoma State University, November 2020), https://nsiteam.com/.
9. Donald J. Trump, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 25, https://www.acq.osd.mil/.
10. Edward Waltz, *Information Warfare Principles and Operations* (Boston: Artech House, 1998), 19–30.
11. Office of the Joint Chiefs of Staff (CJCS), *Competition Continuum,* Joint Doctrine Note 1-19 (Washington, DC: CJCS, 2019), 2-4; and Bradley Young and Jonathan Wood, "The Army's Information Operations Profession Has an Identity Crisis," *Proceedings* 147, no. 3 (March 2021), https://www.usni.org/.
12. CJCS, *Information Operations,* Joint Publication (JP) 3-13 (Washington, DC: CJCS, 2014), GL-3.
13. US Department of the Air Force (DAF), "Sixteenth Air Force (Air Forces Cyber)," DAF (website), August 27, 2020, https://www.16af.af.mil/; and CJCS, JP 3-13, ix.
14. John Boyd, *A Discourse on Winning and Losing* (Maxwell AFB, AL: Air University Press, 2018), 237; and Carl von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989), 75.
15. CJCS, *Joint Planning,* JP 5-0 (Washington, DC: CJCS, 2020).
16. CJCS, JP 5-0, II-10, III-33.
17. Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare* (Arlington, VA: Center for Naval Analysis, 2016), 3; and Edmund Burke et al., *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 6–8, https://www.rand.org/.

18. Iain King, "Toward an Information Warfare Theory of Victory," Modern War Institute, October 19, 2020, https://mwi.usma.edu/.

19. Susan J. Milton and Jesse C. Arnold, *Introduction to Probability and Statistics: Principles and Applications for Engineering and the Computing Sciences* (New York: Tata McGraw-Hill, 2007), 1.

20. Venkatesh Rao, *Tempo: Timing, Tactics and Strategy in Narrative Decision-Making* (La Vergne, TN: Ribbonfarm, 2011), 42.

21. Waltz, *Information Warfare*, 83–85.

22. Daniel Kahneman, *Thinking, Fast and Slow* (New York: Allen Lane, 2011), 21–24.

23. Bryan Clark, Daniel Patt, and Harrison Schramm, *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations* (Washington, DC: Center for Strategic and Budgetary Assessments, February 11, 2020), 22; and CJCS, JP 3-13, I-1–I-3.

24. Peter Berger and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge* (New York: Anchor Books, 1967), 3.

25. Matt Bishop, *Computer Security: Art and Science* (Upper Saddle River, NJ: Addison-Wesley, 2002), 124.

26. Berger and Luckmann, *Social Construction*, 61.

27. Ken Thompson, "Reflections on Trusting Trust," *Communications of the ACM* 27, no. 8 (August 1984): 763, https://www.cs.cmu.edu/.

28. Jonathan M. McCune et al., "Turtles All the Way Down: Research Challenges in User-Based Attestation" (paper presented at 2nd USENIX Workshop on Hot Topics in Security, Boston, MA, August 2007), https://www.usenix.org/.

29. Michael Janser, *Cognitive Biases in Military Decision Making* (Carlisle Barracks, PA: US Army War College, 2007), 1, https://apps.dtic.mil/.

30. Jonathan Haidt, *The Righteous Mind: Why Good People Are Divided by Politics and Religion* (New York: Vintage, 2012), 153.

31. Haidt, *Righteous Mind*, 211.

32. Haidt, *Righteous Mind*, 16–17.

33. Haidt, *Righteous Mind*, 314.

34. Haidt, *Righteous Mind*, 221–22.

35. Zachery Kluver et al., *Propaganda: Indexing and Framing the Tools of Disinformation*, Quick Look (Stillwater: MESA, School of Media and Strategic Communications, Oklahoma State University, December 2020), 3, https://nsiteam.com/.

36. Claire Wardle and Hossein Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe (CoE) Report DGI (Strasbourg, France: CoE, September 27, 2017), 20, https://rm.coe.int/.

37. King, "Theory of Victory," 4.

38. Kluver et al., *Propaganda*, 1.

39. Peter M. Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization,* rev. ed. (New York: Currency, 2006), 13–14.

40. Connell and Vogler, *Cyber Warfare*, 3; and Burke et al., *Operational Concepts*, 6-8.

41. Kluver et al., *Propaganda*, 1.

42. Clausewitz, *On War*, 75.

43. Clausewitz, *On War*, 77.

44. King, "Theory of Victory," 5; and Timothy D. Haugh, Nicholas J. Hall, and Eugene H. Fan, "16th Air Force and Convergence for the Information War," *Cyber Defense Review* 5, no. 2 (Summer 2020): 29, https://www.jstor.org/.

45. Xiaosong Shou, ed., *The Science of Military Strategy* (Beijing: Military Science Press, 2013), 245.

46. Trump, *National Security Strategy*, 25.

47. Joseph R. Biden Jr., *Interim National Security Strategic Guidance* (Washington, DC: The White House, March 2021), 8, https://www.whitehouse.gov/.

48. Yuying Ma, "He Bin Made a Speech at a Seminar on the Study and Implementation of the Fifth Plenary Session of the 19th Central Committee of the Communist Party of China at the County Level," *Qilian News*, February 25, 2021, https://web.archive.org/.

49. Trump, *National Security Strategy*, 25.

50. Policy Planning Staff, Office of the Secretary of State, *The Elements of the China Challenge* (Washington, DC: US Department of State, December 2020), 6, https://www.state.gov/.

51. Michael A. Peters, "The Chinese Dream: Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era," *Educational Philosophy and Theory* 49, no. 14 (November 2017): 1299–1304, https://doi.org/.

52. Policy Planning Staff, *China Challenge,* 1.

53. Policy Planning Staff, *China Challenge*, 7.

54. Dennis J. Blasko, "Special: Sun Tzu Simplified: An Approach to Analyzing China's Regional Military Strategies," Project 2049 Institute, April 10, 2015, https://project2049.net/.

55. Roger T. Ames, *Sun-Tzu: The Art of Warfare: The First English Translation Incorporating the Recently Discovered Yin-ch'ueh-shan Texts* (New York: Ballantine Books, 2010), 111.

56. Anne-Marie Brady, *Marketing Dictatorship: Propaganda and Thought Work in Contemporary China* (Lanham, MD: Rowman and Littlefield, 2009), 1.

57. Mao Tse-tung, "On the Chungking Negotiations," in *Selected Works of Mao Tse-tung*, vol. 4, October 17, 1945, 59–60, https://www.marxists.org/.

58. Larry Diamond and Orville Schell, eds., *Chinese Influence and American Interests: Promoting Constructive Vigilance* (Stanford, CA: The Hoover Institution, 2018), 138, https://www.hoover.org/.

59. Office of the Secretary of Defense (OSD), *Annual Report To Congress: Military and Security Developments Involving the People's Republic of China 2019* (Washington, DC: OSD, May 2, 2019), i, https://media.defense.gov/.

60. Anne-Marie Brady, "Magic Weapons: China's Political Influence Activities under Xi Jinping" (paper presented at the Taiwan Foundation for Democracy Conference, Arlington, VA, September 16–17, 2017), https://www.wilsoncenter.org/.

61. Sitong Guo et al., "The Tweet Heard Round the World: Daryl Morey, the NBA, China, and Attribution of Responsibility," *Communication & Sport* (December 2020), https://doi.org/.

62. Harrison Christian, "Kiwi Publishers Face Censorship Demands from Chinese Printers," Stuff, August 18, 2019, https://www.stuff.co.nz/; and Sarah Wu and Joyce Zhou, "Editing History: Hong Kong Publishers Self-Censor under New Security Law," Reuters, July 13, 2020, https://www.reuters.com/.

63. Victor Cha and Andy Lim, "Flagrant Foul: China's Predatory Liberalism and the NBA," *Washington Quarterly* 42, no. 4 (December 2019): 23–42, https://doi.org/; and Ben Cohen, "LeBron James Says Tweet Supporting Hong Kong Protests Was 'Misinformed,'" *Wall Street Journal*, October 14, 2019, https://www.wsj.com/.

64. Anne-Marie Brady, "China Wants Face and We Are Left with the Cost," commentary (Ottawa, Ontario: Macdonald-Laurier Institute, March 2020), 1, https://www.macdonaldlaurier.ca/; and Rebecca Davis, "China's Film Authority Orders All Cinemas to Screen Propaganda Films at Least Twice a Week," *Variety,* April 2, 2021, https://variety.com/.

65. Xiaosong, *Military Strategy*, 112.

66. Eric Chan and Peter Loftus, "Chinese Communist Party Information Warfare. US-China Competition during the COVID-19 Pandemic," *Journal of Indo-Pacific Affairs* (Summer 2020): 146–54, https://media.defense.gov/.

67. Chan and Loftus, "Information Warfare," 146–54.

68. Policy Planning Staff, *China Challenge*, 10.

69. Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'" *Foreign Policy*, July 9, 2012, https://foreignpolicy.com/.

70. Policy Planning Staff, *China Challenge*, 6–7.

71. Shannon Vavra, "NSA Warns Defense Contractors of Recent Chinese Government-backed Hacking," Cyberscoop, October 20, 2020, https://www.cyberscoop.com/.

72. Burke et al., *Operational Concepts*, 7.

73. Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *Cyber Defense Review* 3, no. 1 (Spring 2018): 111–15, https://cyberdefensereview.army.mil/.

74. Burke et al., *Operational Concepts*, 6.

75. Burke et al., *Operational Concepts*, 7.

76. House Permanent Select Committee on Intelligence (HPSCI), *The China Deep Dive: A Report on the Intelligence Community's Capabilities and Competencies with Respect to the People's Republic of China*, redacted unclassified summary (Washington, DC: United States House of Representatives, September 30, 2020), 8, https://intelligence.house.gov/.

77. James Micciche, "U.S. below War Threshold Options against China," Divergent Options, September 21, 2020, https://divergentoptions.org/.

78. Scott Padgett and Stefan Banach, "Winning the Real War: Designing Virtual Armies," Small Wars Journal, April 9, 2019, 2021, https://smallwarsjournal.com/.

79. HPSCI, *China Deep Dive*, 3.

80. Policy Planning Staff, *China Challenge*, 13, 33.