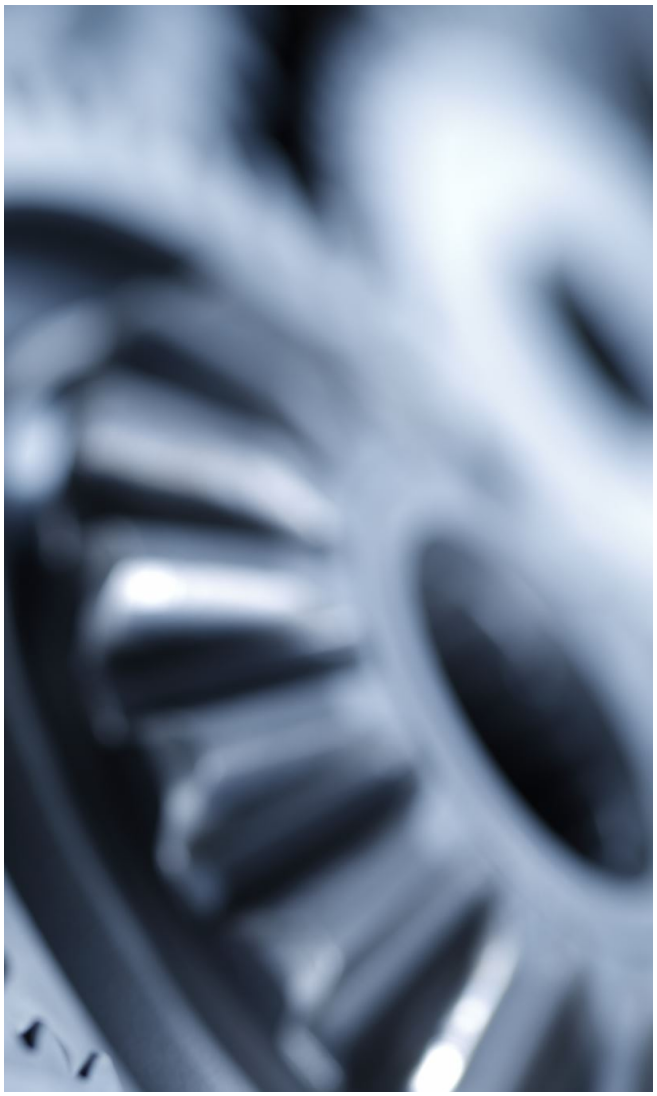
Information Maneuver in Military Operations



AUGUST 2021

STRATEGIC MULTILAYER ASSESSMENT

Author:
Lt Gen (Ret) Robert J. Elder, D.Engr
George Mason University

Series Editor: Ali Jafri, NSI Inc.

LTG (ret.) Robert J. Elder, D.Engr, George Mason University

Lieutenant General Robert Elder (USAF, retired) joined the George Mason University faculty as a research professor with the Volgenau School of Engineering following his retirement from military service as the Commander of 8th Air Force and US Strategic Command's Global Strike Component. He currently conducts research in the areas of command and control, deterrence, escalation control, competition short of armed conflict, crisis management, and international actor decision-making. General Elder served as the Central Command Air Forces Deputy Commander for Operation Enduring Freedom, Air Operations Center Commander and Deputy Air Component Commander for Operation Iraqi Freedom, and Commandant of the Air War College. He was the first commander of Air Force Network Operations and led the development of the cyberspace mission for the Air Force. He received his Doctorate in Engineering from the University of Detroit.

Information Maneuver in Military Operations

LTG (ret.) Robert J. Elder, D.Engr, George Mason University[1]

Treating information as a form of maneuver can provide powerful advantages to commanders and political leaders responsible for US and partner national security. The components of successful maneuver first proposed by van Creveld, Canby, & Brower in 1994—positioning, tempo, *Schwerpunkt*, surprise and deception, cross-domain synergy, flexibility, unity of effort, and opportunism—can also serve as elements of a framework to anticipate an adversary's integrated use of information to undermine US and partner interests. Employed as a form of maneuver, information is valuable because it serves as virtual representations of both physical and cognitive realities which can be created, stored, and exchanged in all environments and, when properly communicated, can influence the actions and behaviors of others. Because of the US military's traditional reliance on attrition warfare, few US military leaders are experienced or comfortable with the concepts of maneuver and less so with the use of information operations to outmaneuver an adversary as a means to victory. However, as a means to combat the US asymmetric advantage in physical power, many US competitors have turned to information as a means to outmaneuver the United States and deny it the benefits of its asymmetric advantages in other areas.

Overview: Concept of Maneuver Warfare

This paper argues that applying traditional principles of maneuver to the use of information in joint operations can provide powerful advantages to commanders and political leaders responsible for US and partner national security. Maneuver attempts to minimize actual fighting. Before the fight, maneuver warfare seeks ways to place the enemy at a disadvantage by taking up favorable positions, or else by first confronting part of the enemy's forces within a limited area to obtain an advantage over the force as a whole. Once the fight is over, maneuver warfare takes maximum advantage of the positive outcome by continuing to pursue the enemy, keeping him off balance, and striking into his vitals (van Creveld et al., 1994). Throughout its history, the US military has preferred to conduct operations based on overpowering its adversaries and achieving victory through attrition or threat of defeat through the employment of overwhelming force, and maneuver warfare has received secondary attention. The enclosed text box provides a review of the basic tenets of maneuver warfare, and subsequent sections

[1] *Contact Information*: relder@gmu.edu

will describe how its principles can be applied to the integrated employment of information as a key element of all-domain military and whole of government operations.

Six Concepts of Maneuver Warfare (van Creveld et al., 1994)

In van Creveld, Canby and Brower's 1994 work, entitled *Air Power and Maneuver Warfare*, the authors outline six concepts of maneuver warfare. They are as follows:

- **Tempo:** Rather than speed, tempo refers to the act of transitioning from one mode of an action to another before the adversary can react; this reflects an ability to get "inside" the adversary's decision cycle.
- ***Schwerpunkt*:** Defined as "main emphasis" at the center of gravity, use of this concept relies on identifying the optimal time and place to strike the enemy with the most amount of force; this is most effective when concentrated on areas that are simultaneously vital and weakly defended.
- **Surprise:** Often based on deception, surprise allows actors to confound their opponent, disorient them, and introduce an element of uncertainty into their plans.
- **Combined arms:** This concept refers to the practice of grouping varying capabilities, which allow actors to overwhelm their opponent, who is made vulnerable to diverse arms.
- **Flexibility:** Building on the preceding principles' reliance on rapid adaptation of resources to a fluid situation, flexible organizations are those that are well-rounded, self-contained, and not too specialized.
- **Decentralized command:** The act of empowering lower levels of command, which itself relies on synchronicity with the commander's objective.

Attrition warfare is linear and direct, with the objective of destroying an enemy's assets one by one until the enemy can no longer hold the field. In contrast, maneuver warfare attacks links between enemy forces (supply lines, command and control, reinforcements, communications) so that the enemy loses the ability for coherent attack or defense. Attrition warfare attacks an enemy's strengths, while maneuver warfare exacerbates an enemy's weaknesses. Furthermore, attrition warfare focuses on immediate battlefield dynamics, while maneuver warfare takes a longer view of the evolution of battlefield dynamics. For this reason, commanders engaged in maneuver warfare need to think several moves ahead of their adversaries (van Creveld et al., 1994).

Attrition and maneuver also differ in the way weapons are employed. Attrition warfare seeks to destroy as many assets as possible, whereas maneuver warfare seeks to create tactical advantages favorable to greater strategic goals (van Creveld et al., 1994). In the competition operations that the United States and its adversaries routinely experience and conduct themselves, information is used to maneuver their respective competitors into situations favorable to their objectives. In attrition warfare, the defense relies on the strength of its prepared positions and confronts the attack head on. In a maneuver defense, the basic tactic from which all variations are run is the side step, like that of the bullfighting matador (van Creveld et al., 1994).

In traditional small-unit operations, maneuver relies primarily on stealth and stalking—using terrain for cover and positioning for the right moment to attack. With larger physical units, maneuvering and maintaining the element of surprise is more difficult because of the sheer size and complexity of the logistics apparatus. In practice, success often amounts to pinning the enemy's front and attacking its flanks and rear. British military theorist B. H. Liddell Hart drew a comparison between this process and boxing, specifically where one arm parries and distracts the opponent while the other strikes. Artificial flanks are created to drive wedges through enemy forces, destroying their cohesion and ability to counterattack while creating opportunities for surprise. A key element is cutting the enemy's lines of communication so as to prevent its coordination (van Creveld et al., 1994).

Van Creveld et al. also stress the importance of opportunism, which is the use of "non-linear" formations to attack weaknesses as they present themselves, enabled by focusing on higher-level objectives rather than just specific tasks. Opponents of the United States employ opportunism very effectively, but Americans are much more regimented. Because of their training and experience, they tend to find maneuver warfare counterintuitive. An additional aspect of maneuver warfare that van Creveld et al. stress is positioning, which is a question of exploiting the terrain, maintaining cover, and jockeying for position, all the while waiting for the opportune moment to arrive (van Creveld et al., 1994).

Because of the US military's historic reliance on attrition warfare, few US military leaders are experienced or comfortable with maneuver warfare concepts, and less so the use of information operations (IO) to outmaneuver an adversary as a means to achieve successful strategic or operational outcomes. However, as a means to combat the US asymmetric advantage in physical power, many of its competitors have turned to information as a means to outmaneuver the United States and deny it the benefits of its asymmetric advantages in other areas. US military commanders and their planners should treat the influence effects of information as a powerful form of maneuver—our competitors certainly do. The next section will review contemporary doctrinal concepts of information, followed by sections illustrating how each element of maneuver warfare applies to the effective employment of information-related capabilities in operations across all domains.

Review of Information Concepts in Joint Doctrine

The US military views information from many different doctrinal and conceptual perspectives. For example, information is commonly considered as an instrument of national power, alongside the diplomatic, military, and economic instruments. It is also considered an operational variable for purposes of strategy development and analysis in the PMESII (political, military, economic, social, information, and infrastructure) construct. Joint Publication 3-13 (Joint Staff, 2014) describes information as an environment: "The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information . . . It consists of

three interrelated dimensions: physical, informational, and cognitive" (pp. ix-x). This section argues that although US joint doctrine defines information as an environment, its importance comes not from being an operational environment but because information serves as virtual representations of both physical and cognitive realities which can be created, stored, and exchanged in all environments (i.e., semaphore flags, newspapers, signs, markers, and so on). Virtual representations also exist in cyberspace, which, because of its dissemination speed and global reach, has made cyber operations a valuable tool for military operations (Joint Staff, 2018).

JP-1, Doctrine of the Armed Forces of the United States, refers to information as the seventh joint function of the military, alongside command and control (C2), intelligence, fires, movement and maneuver, protection, and sustainment (Joint Staff, 2017b). The doctrinal challenge is that information is considered an environment, but as a joint function, information ops are a part of every environment. In 2018, the Department of Defense issued the Joint Concept for Operations in the Information Environment (Joint Staff, 2018), which explains that the information environment directly affects and transcends all operating environments. It states that the information environment comprises and aggregates numerous social, cultural, cognitive, technical, and physical attributes that act upon and affect knowledge, understanding, beliefs, world views, and, ultimately, actions of an individual, group, system, community, or organization.

People attribute meaning to information when it makes sense to them, particularly if it reduces their uncertainty about the state of the world. They do this to non-man-made information when they attribute a thunderclap to an angry god or a sound wave, or a disease to a demon or a virus. Clearly, some meanings are fanciful, and some reflect reality. People are constantly generating information, intentionally or not, and other people perceive and assign meaning to it based on how they understand it. When people intentionally generate information, they create virtual representations. When the information is understood the way the communicator intended, then one has communicated effectively (L. Kuznar, personal communication, June 17, 2021). In this way, the interpretation of information can lead to judgments and perceptions that influence others' decisions and behaviors, which is ultimately the goal of military operations. Information maneuver employs information capabilities in multiple domains to create virtual representations that a sender uses to influence the receiver's perception of reality and therefore the receiver's behavior.

In response to a Joint Requirements Oversight Council (JROC) memorandum that asked the services and combatant commands to implement approaches to close information-related capability gaps (Joint Requirements Oversight Council, 2019), the Joint Staff J39 Strategic Multilayer Assessment office launched a project entitled "Integration of Information in Joint Operations" (IIJO) to address how Joint Force commanders, Joint Force and Service component commanders, and their respective staffs can best understand and integrate information and influence into operational-level planning, execution, and assessment activities across the competition continuum. One of the key questions the Air Force

posed was “What are the characteristics of information as a form of operational maneuver and power?” This paper addresses this question using a framework adapted from one that Martin van Creveld et al. first proposed in 1994 (van Creveld et al., 1994).

Elements of Information Maneuver in Military Operations

Van Creveld et al.’s six elements of maneuver warfare reviewed above are relevant to the employment of information in joint and whole-of-government operations, in part because they have analogous manifestations in the use of information generally. Beyond the six principles that van Creveld et al. delineate, the authors also devote discussion to two other critical concepts: positioning and opportunism. These latter two, in addition to the previously-discussed six, each have modern-day applications that warrant further study. Each element and its manifestations are reviewed in turn.

Positioning

Proper positioning is critical to maneuver and requires an understanding of fronts and flanks, obfuscation, and the utility of altering the standard environment. In the case of information, this standard environment is termed the “noise floor.” In traditional small-unit operations, the essence of maneuver consists of “stealth and stalking.” The purpose of positioning is to “drive wedges through the enemy forces, destroy their cohesion, carve them up into separate parts, prevent them from mounting counterattacks, and beat them in detail-if possible by cutting their lines of communication rather than by attacking their front” (van Creveld et al., 1994). Information is particularly well suited for these purposes.

Consider how information positioning has been performed in recent history. Since early 2014, Russia has employed a highly complex socio-psychological information warfare campaign in Ukraine known as “reflexive control.” Reflexive control involves using information to shape an adversary’s perceptions and decision calculus such that the adversary voluntarily acts in ways advantageous to Russian objectives. Moscow has persuaded the United States and its European allies to remain largely passive during the Kremlin’s efforts to dismantle Ukraine through military and non-military forms of reflexive control (Snegovaya, 2015).

Russian information operations, above all, rely on Russia’s ability to take advantage of pre-existing dispositions among its enemies to choose its preferred courses of action. “The primary objective of the reflexive control techniques Moscow has employed in the Ukraine situation has been to persuade the West to do something its leaders mostly wanted to do in the first place, namely, remain on the sidelines as Russia dismantled Ukraine” (Snegovaya, 2015, p. 7). In this way Russia was able to avoid a direct physical confrontation with the United States and Europe but still achieve its desired objectives. In the Ukrainian context, the applications of Russia’s reflexive control techniques have included 1) operations designed to deny or obfuscate the presence of Russian forces in Ukraine, 2) purposeful concealment of

Russian objectives in the conflict, and 3) maintaining a veneer of plausible legality for Russian actions, "requiring the international community to recognize Russia as an interested power rather than a party to the conflict, and pointing to supposedly-equivalent Western actions such as the unilateral declaration of independence by Kosovo in the 1990s" (Snegovaya, 2015, pp. 7).

Another form of positioning used by both state and non-state actors is to increase the standard social media "noise floor" through a constant barrage of engagement on various platforms, posting, sharing, liking, and disseminating misinformation (Chabuk and Jonas, 2018). A recent non-military example is Russia's use of Facebook advertising for both the Black Lives Matter and Blue Lives Matter groups during recent protests in the United States. The House Intelligence Committee found that the Kremlin-linked Internet Research Agency was responsible for a total of 3,519 known paid ads on Facebook that directly reached more than 11.4 million American users of the platform. This use of social media demonstrates a deep understanding of using noise as a means of positioning (Chabuk and Jonas, 2018).

Tempo

For maneuver warfare to be employed effectively in practice, a vital element is tempo, the ability to transition from one action mode to another before a competitor can react to the first. Tempo is not the same as speed; it has perhaps been defined best by retired USAF Colonel John Boyd as "the observation-orientation-decision-action cycle, sometimes called the OODA Loop . . . The idea is to get 'inside' the loop by transitioning from one mode of action to another before the other party can react. As this happens, the opponent progressively loses coherence in its actions . . . The idea is to move faster than the other can react and to react faster than the other can move" (van Creveld et al., 1994, p. 3).

As an example of how to set the conditions for information tempo, Russia has deployed a vast and complex global effort to shape the narrative about the Ukraine conflict through traditional use of media and social media, and it has used this to achieve considerable influence over domestic politics in several Western Balkan countries (Snegovaya, 2015). "In addition to official government-to-government contacts, Moscow has established ties with a range of parties that have an anti-NATO and Eurosceptic bent" (Bechev, 2019, p. 20). Russia also wields considerable influence in internally polarized countries. It plays on internal divisions to maximize its geopolitical clout and fight the West. "The cases of North Macedonia and Montenegro shed light on the mechanics of Russian involvement. In both countries. Russia attempted to obstruct integration into NATO taking advantage from domestic turmoil" (Bechev, 2019, pp. 20).

Another Russian tempo tool is subversion, which Bechev characterizes as "exemplified by tactics such as (dis)information campaigns and open or covert support for radical anti-Western actors (parties and civic associations)" (Bechev, 2019, p. 11). He provides examples of recent Russia attempts to block NATO accession by Montenegro and North Macedonia by amplifying internal crises (Bechev, 2019). The operational advantages to this philosophy are also highlighted by Bechev, which include low cost and

the ability to outsource to formal and informal channels; this allows Russia to vault itself to co-equal status with the West and generate strategic bargaining chips for Moscow (2019).

The large number of different tools allows Russia to shift its lines of operations rapidly before Western nations can formulate a response, as well as to mitigate any counter-strategies that its opponents begin to execute.

Schwerpunkt

An example of Schwerpunkt condition setting in information operations is China's use of information influence campaigns in support of CCP-friendly candidates and its efforts to undermine the credibility of Taiwan's democracy. In this context, China's efforts attempted to "shape the production, dissemination, and consumption of information in Taiwan," going well beyond traditional disinformation efforts (Doshi, 2020). This is in keeping with the People's Liberation Army's "Three Warfares" concept, which is comprised of "public opinion/media warfare, psychological warfare, and legal warfare" (Bagchi, 2017). These three components are critical to China's strategic approach and were employed in the 2017 China-India border standoff (Doklam Standoff) between the Indian Armed Forces and the People's Liberation Army of China over Chinese construction of a road in Doklam near a tri-junction border area. China used the concept of "public opinion/media war" to generate (domestic and international) public support in favor of Chinese actions during the incident; to this end, Chinese state organs and officials, through their public statements, attempted to dissuade India from taking actions understood to be damaging to China in Doklam (Bagchi, 2017).

This competition in the public domain is, according to individuals within the Chinese Communist Party, " 'a contest over 'discourse power,'' or the ability to shape public opinion from the top down for political purposes" (Doshi, 2017). In Taiwan, this is manifested through attempts to control those who create content, publishers and validators, and distributors; the means by which this is conducted vary between positive and negative pressure, which range from media exchanges to intimidation campaigns to legal recourse to the deployment of bots on social media (Doshi, 2020).

US competitors are systematically exploiting multiple points of weakness in the United States and its partners in ways that are unraveling the ability of Western nations to react to competitor information operations. Their Schwerpunkt approach cannot be ignored, and traditional US responses are likely to be ineffective.

Surprise and Deception

Properly executed information maneuver will "throw [the opponent] off balance and introduce an element of uncertainty into [the opponent's] plans" (van Creveld et al., 1994, p. 5). To paraphrase Sun Tzu, it is necessary to find out the enemy's intentions while concealing one's own.

In 2015, a massive Russian information campaign at a "troll farm" in St. Petersburg gained much attention in Western media outlets. This initiative, said to have been funded by oligarch Yevgeny Prigozhin[2], employed hundreds of people, and 13 individuals "including a man with ties to [Russian President Vladimir] Putin, were . . . named in an indictment connected to special counsel Robert Mueller's investigation into Russian interference in the 2016 U.S. presidential election" (Meyers and Evstatieva, 2018). With all of the Western news outlets paying attention, however, the Russian authorities appeared content to leave this location in the foreign media spotlight. Why? This single organization, by virtue of its public profile, came to serve as a sole target of attention, shifting focus from the larger network of troll farms that supported it (Giles, 2015).

After the conflict in Ukraine, observers noticed how malware which was originally intended to generate revenue through ad placement and "clicks" was commandeered to promote pro-Russian videos on YouTube. As analysts watched the activity, it seemed to be a simple clickbait revenue scheme, but the actions quickly pivoted towards propaganda landing sites. This demonstrated an interesting attack method that could be used to artificially inflate the popularity of a piece of content, as well as its visibility (Kogan, 2015).

Other approaches to operational deception are to accustom the enemy to particular patterns of behavior that are exploitable at the time of the attacker's choosing. The United States used this approach very effectively during the preparations for Operation Iraqi Freedom (OIF). During the months before the Baghdad campaign, the coalition expanded Operation Southern Watch, the no-fly zone operations over southern Iraq, from 50 sorties to nearly 800 sorties a day. Called Operation Southern Focus, it was a sophisticated deception effort, desensitizing the Iraqis to the presence of large numbers of aircraft over the southern no-fly zone (Jamieson, 2015).

Iraqi deceptions regarding the state of its nuclear weapon program prior to the initiation of Operation Iraqi Freedom in 2003 created serious unintended consequences. The intelligence community (IC) picked up what it believed to be indications of an advanced nuclear program, although their appraisals were contrary to the assessments of weapons experts. The IC's estimate was due in part to the Iraqi's lack of transparency reinforced by intelligence indicating that Saddam Hussein met frequently with his weapons experts. The Iraqi history of deception, combined with their purposeful opaqueness contributed to an incorrect intelligence estimate which was used to make the case for invasion (Chilcot, 2016).

[2] Prigozhin "has been sanctioned by the U.S. for providing support to the Russian Defense Ministry as it annexed Crimea from Ukraine in 2014" (Meyers & Evstatieva, 2018).

Cross-domain Synergy

Cross-domain synergy is "the complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of others" (Department of Defense, 2012, pp. ii). Viewed from the perspective of information maneuver, it is the coordination and synchronization of diverse means of transmitting information and countering the opponent's information means (both visible actions and messaging). The goal is to create multiple challenges for the adversary that create conundrums and place them on the horns of a dilemma. Creating such conundrums requires the "grouping of diverse arms so that the strength of each arm is brought to the fore so as to expose an enemy weakness to another arm. An apt analogy is the well-known children's game of the intransitive 'rock-scissors-paper'" (van Creveld et al., 1994, pp. 5). Note that the value of combining capability elements for cross-domain synergy is a result of coordination across the diverse arms, rather than cumulative firepower (van Creveld et al., 1994).

As an example, Moscow's 2016 election influence campaign followed a Russian messaging strategy that combined covert intelligence operations, including cyberattacks, with overt messaging by Russian Government agencies, state-funded media, proxies, and trolls (Office of the Director of National Intelligence, 2017). The response to mitigate the effects of one Russian line of messaging operations was quickly countered in ways that suggested that the election process had been undermined, an equally (or perhaps worse) outcome from a US perspective (Hwang, 2019). The 2016 effort was representative of the nature of information campaigns because of the use of formal and informal channels to shape narratives and disseminate disinformation; this reflected similar campaigns in England, Finland, Mexico, Syria, and Ukraine (Hwang, 2019). Additionally, "disinformation was accelerated through online advertising channels," through pre-existing capabilities on popular platforms, and through the Russian practice of generating such disinformation for profit (Hwang, 2019). Lastly, the Russian campaign conducted cyberattacks on US political entities, which presaged similar uses in the 2017 French Presidential election and during the Gulf crisis (Hwang, 2019).

Cyberattacks, particularly those targeting trust and integrity, can have profound effects on interconnected systems; they have a lower threshold and are more difficult to detect and deter (Pollard, 2018). One recent example involved the United Arab Emirates, which was accused of orchestrating the hacking of Qatari government news and social media sites in order to post incendiary false quotes attributed to Qatar's emir, Sheikh Tamim Bin Hamad al-Thani, in May 2017 (DeYoung & Nakashima, 2017). Saudi Arabia, the UAE, Bahrain, and Egypt, in response to comments falsely attributed to the emir, broke relations with Qatar and instituted a trade and diplomatic boycott, which then-Secretary of State Rex Tillerson warned "could undermine U.S. counterterrorism efforts against the Islamic State" (DeYoung & Nakashima, 2017).

Flexibility

Another principal element of maneuver warfare is flexibility. This means that the information capabilities of the Unified Action force, which includes US military, inter-agency, and international capabilities, must be well-rounded, self-contained, and not too specialized. As a minimum, Unified Action implies "whole of government," but for information maneuver it should not be limited to government capabilities alone. Flexibility avoids excessive standardization of component parts for diversity and promotes redundancy, which permits the organization to absorb hits without impairing its ability to function.

Tactically, information warfare gives Russia the element of surprise, providing an advantage in time and efficiency against the enemy's ground forces. In the case of Ukraine, war was not declared, while separatists conducted rapid, high-intensity attacks that limited the time the United States and EU could respond, presenting them with a false picture of the situation. In this way, Russia achieved its objectives in Crimea with very few casualties. The use of information as maneuver provides more flexibility and speed in battlefield responses. For example, Russia's initial denial of the presence of the Russian soldiers in Crimea provided Russia the time to take over strategic positions in Crimea (Snegovaya, 2015).

Unity of Effort

Unity of effort, characterized by decentralized control but with unity of purpose among the partnering actors (whole of government, allies, non-government actors, and others) is a key principle of effective maneuver operations. The use of decentralized control permits flexibility among the partners. In fast and fluidly changing information campaigns, the best command and control will not be able to keep pace with developments. Therefore, it is essential that the division of responsibilities across echelons in these campaigns be well-designed and well-rehearsed. Lower echelons must be granted the rights and means to exercise initiative and adapt to rapidly changing situations, seizing opportunities as they occur (van Creveld et al., 1994). For information maneuver, senior agency leaders and their counterparts must reach agreement on the strategic narrative and messages and use it to provide mission orders to their subordinates. It is also important that echelons at each level are authorized to synchronize and deconflict their activities with one another directly rather than coordinate their actions through higher-level echelons.

China's Strategic Support Force (SSF) houses theater-level command of the country's information-related capabilities: strategic space assets, cyberspace, electronic warfare (EW), information operations, and psychological warfare. To China, information superiority is as important, if not more important, than physical battlefield success. Degrading systems with emerging technologies such as artificial intelligence (AI) is China's newest focus. These new technologies will allow China to expand its capabilities even beyond those of its current information superiority approach (Pollpeter, 2017).

A truly united effort of PRC political, military, and civilian effort allows this SSF to operate successfully in their IO, EW, space, and other objectives, as well as to create and maintain a clear message and goal for the PRC in this new realm. The entire Chinese government has a clear message and goal that the SSF can implement and other joint forces can uphold (Pollpeter, 2017).

Clearly, the United States has nothing comparable, and so while unity of effort is recognized as a basic principle of war, the United States has no effective means to align narratives, messages, and actions to achieve US strategic or operational objectives. Such alignment is the key to properly integrating information into joint operations. Such alignment is relatively simple in an autocratic system, but since democratic systems and their open societies encourage diversity and freedom of thought, achieving a comparable unity of effort across the US government is generally very difficult. There are ongoing high-level government efforts to coordinate narratives and messages through a variety of inter-agency processes, and these initiatives are beginning to demonstrate success at the strategic level. Concepts for coordination, synchronization, and de-confliction among government agencies and other actors are being developed in support of DoD's Command and Control (C2) of the Information Environment efforts, and these will evolve as planners gain experience with integrating information as a key component of joint operations.

Opportunism

Opportunism is the use of "non-linear" formations to attack weaknesses as they present themselves. Opponents of the United States employ opportunism very effectively, but Americans tend to find maneuver warfare of any kind, not just information maneuver, counterintuitive. This may be because US armed forces since the Civil War have had a long tradition of fighting from a position of overwhelming material strength. For them, war has often been a question of maximizing the blows that they could deliver on the basis of available resources, then exchanging blow for blow until the weaker side—almost always the enemy—was reduced through attrition to the point of being no longer combat capable.

As described in the section on Positioning, Russia employed online advertising to exacerbate social divisions in the United States but did not try to advance any particular pro-Russian message; the goal was simply to create social turmoil to weaken US social solidarity (Chabuk & Jonas, 2018).

The major message of most disinformation campaigns in China is simple: How have democratic countries failed? The COVID-19 crisis is no exception. While China grappled with attempts to contain the spread of the virus, the PRC and state media also focused on another spread—the spread of disinformation (Kurlantzick, 2020). This disinformation was characterized by claims emanating from China, as well as Iran and Russia, that democratic states' responses to the COVID-19 outbreak were comparatively disastrous vis-à-vis autocratic states; these messages came alongside demonstrably false claims coming from Beijing (Kurlantzick, 2020).

Both China and Russia's planning is designed to exploit opportunities as they arise. US and most Western military planning is based on the development of campaigns to achieve objectives. These two approaches are not incongruous. They can be orchestrated together to provide the operational oversight US military operations demand while enabling lower echelons to exploit opportunities as they present themselves.

Conclusion

The US military prefers to conduct its operations based on overpowering its adversaries and achieving victory through attrition or by threatening their defeat through the employment of overwhelming force. As a result, few US military leaders are experienced or even comfortable with the use of information operations to outmaneuver an adversary as a means to gain comparative advantage or achieve other strategic or operational objectives. On the other hand, many US competitors have turned to information as a means to outmaneuver the United States and therefore deny the United States the benefits of its asymmetric advantages in physical power.

Adept military practitioners understand the importance of information maneuver: Information moves through every traditional military environment using both physical and electronic means and is capable of creating physical and cognitive effects on a global basis without physical movement of forces. As a result, information can be effectively employed alone, or in conjunction with other joint functions, to achieve strategic and operational objectives without the need for costly attrition operations.

Information maneuver requires that the United States develop means to communicate information to its audiences of interest. It can be done in many ways to include print, social, and broadcast media, personal engagements, television and movies, and properly messaged visible activities. The US military is particularly well suited to conducting visible activities that reinforce US messaging. On the other hand, other than through personal engagements with foreign military leaders or use of cyber techniques, most messaging will be conveyed through non-military means, which will require multi-agency collaboration and coordination. History has shown that information is most powerful when conveyed over multiple means and aligned so that the messages reinforce one another.

Treating information as a form of maneuver offers a useful template for planning the integration of information into joint and unified action operations. The components of successful maneuver—positioning, tempo, Schwerpunkt, surprise and deception, cross-domain synergy, flexibility, unity of effort, and opportunism—also serve as elements of a framework to anticipate an adversary's integrated use of information to undermine US and partner interests. It would be folly for US competitors to take on US asymmetric military advantages directly. The United States must realize that its competitors will seek to exploit their asymmetric information advantages as a means to compete effectively with the

United States and its partners. We should expect them to employ information maneuver at every opportunity.

In today's doctrine, the information operations cell chief is responsible to the Joint Force Commander (JFC) for integrating information related capabilities (IRCs) into the joint operation planning process (Joint Staff, 2014). The growing importance of information—particularly in competition, deterrence, and assurance operations—means this is not enough. Successful commanders in the future will require their subordinate organizations and all members of their operational staffs to become practiced at integrating information into their operational strategies, campaign plans, and schemes of maneuver.

References

Bagchi, I. (2017, August 13). Doklam standoff: China playing out its 'Three Warfares' strategy against India. *The Times of India*. https://timesofindia.indiatimes.com/india/china-playing-out-its-three-warfares-strategy-against-india/articleshow/60036197.cms

Bechev, D. (2019). *Russia's strategic interests and tools of influence in the Western Balkans*. NATO Strategic Communications Center of Excellence. https://stratcomcoe.org/cuploads/pfiles/russias_strategic_interests_in_balkans_11dec.pdf

Bechev, D. (2015, October 12). *Russia in the Balkans: How should the EU respond?* European Policy Centre. http://www.epc.eu/documents/uploads/pub_6018_russia_in_the_balkans.pdf

Chuabuk, T., & Jonas, A. (2018, September). Understanding Russian information operations. *Signal Magazine*, 37-29. https://www.afcea.org/content/understanding-russian-information-operations

Chilcot, J. (2016). *The Report of the Iraq inquiry, Volume IV*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535415/The_Report_of_the_Iraq_Inquiry_-_Volume_IV.pdf

Department of Defense. (2016). *Strategy for operations in the information environment*. https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf

Department of Defense. (2018). *Joint concept for operations in the information environment*. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf

DeYoung, K. & Nakashima, E. (2017, July 16). UAE orchestrated hacking of Qatari government sites. *The Washington Post.* https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html

Doshi, R. (2020, January 9). China steps up its information war in Taiwan*. Foreign Affairs*. https://www.foreignaffairs.com/articles/china/2020-01-09/china-steps-its-information-war-

taiwan?utm_medium=promo_email&utm_source=lo_flows&utm_campaign=registered_user_welcome&utm_term=email_1&utm_content=20210415

Giles, K. (2016, May 20). *The next phase of Russian information warfare.* NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176

Hwang, T. (2019). Maneuver and manipulation: On the military strategy of online information warfare. Army War College Press.

Jamieson, P. D. (2015, September 30). *Southern Iraq.* Air Force Historical Research Agency: https://www.afhra.af.mil/Portals/16/documents/Airmen-at-War/Jamieson_SouthernIraq30Sep15.pdf?ver=2016-08-22-131406-023

Department of Defense. (2012). *Joint Operational Access Concept (JOAC)*. https://archive.defense.gov/pubs/pdfs/JOAC_Jan%202012_Signed.pdf

Joint Staff. (2014). Joint publication 3-13: Information operations. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

Joint Staff. (2016). Defense primer: Information operations cross-domain synergy in joint operations planning guide. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cross_domain_planning_guide.pdf?ver=2017-12-28-161956-230

Joint Staff. (2017a). Joint operations (Joint Publication 3-0). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf

Joint Staff. (2017b). Joint publication 1: Doctrine for the Armed Forces of the United States. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf

Joint Staff. (2018). Cyberspace operations (Joint Publication 3-12). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Joint Staff. (2019). Joint Requirements Oversight Council (JROC) published Joint Requirements Operational Change Memo (JROCM) 068-19.

Kogan, R. (2015, April 29). Bedep trojan malware spread by angler exploit kit gets political*. Trustwave*. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/bedep-trojan-malware-spread-by-the-angler-exploit-kit-gets-political/

Kurlantzick, J. (2020, September 10). *How China ramped up disinformation efforts during the pandemic.* Council on Foreign Relations. https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic

Meyers, J., & Evstatieva, M. (2018, March 15). *Meet the activist who uncovered the Russian troll factory named in the Mueller probe.* NPR.

https://www.npr.org/sections/parallels/2018/03/15/594062887/some-russians-see-u-s-investigation-into-russian-election-meddling-as-a-soap-ope

Office of the Director of National Intelligence. (2017). *Intelligence Community Assessment (ICA), Assessing Russian activities and intentions in recent US elections*. https://www.dni.gov/files/documents/ICA_2017_01.pdf

Osinga, F. (2005). *Science, strategy and war: The Strategic theory of John Boyd*. Eburon Academic Publishers. http://www.projectwhitehorse.com/pdfs/ScienceStrategyWar_Osinga.pdf

Pollard, N. A. (2018, January 16). *Trust War: Dangerous trends in cyber conflict.* War on the Rocks. https://warontherocks.com/2018/01/trust-war-dangerous-trends-cyber-conflict/

Pollpeter, K., Chase, M., & Heginbotham, E. (2017). *The creation of the PLA Strategic Support Force and its implication for Chinese military space operations.* RAND Corporation. https://www.rand.org/pubs/research_reports/RR2058.html.

Snegovaya, M. (2015). Putin's information warfare in Ukraine: Soviet origins of Russia's hybrid warfare. Institute for the Study of War.

van Creveld, M., Canby, S. L., & Bower, K. S. (1994). *Airpower and maneuver warfare*. Air University Press.