Information Warfare and Its 18th and 19th Century Roots

Major Nathaniel D. Bastian, Ph.D.

For Joint Force leaders to visualize and describe how the operational environment shapes the range of military operations, they must have a deep understanding of the capabilities comprising the multi-domain battlefield. The information environment, which Joint Publication (JP) 3-13 defines as the "aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information,"[1] is intrinsically linked to the traditional land, air, maritime and space domains. Moreover, the rapid advancement and application of technologies has directly facilitated the use of information-related capabilities in Joint Force operations.[2] The orchestrated use of these information activities, commonly known as "information operations", aims to gain strategic and operational advantages in the information environment.[3] These advantages are often gained through the manipulation of the information environment using information operations (IO), which, according to JP 3-13, are 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."[4]

Some historians hold that information warfare dates from the beginning of the 20th century, noting, for example, that the French army conducted IO activities in the First World War, using electronic warfare techniques that enabled the interception of wireless and telephone communications.[5] Yet, history confirms otherwise - appreciation for the value of intelligence dates to Sun Tzu and earlier, and 18th and 19th century leaders conducted information warfare using information-related intelligence gathering, military deception, military information support operations, and operations security. Examining these roots of modern-day information operations can yield valuable insights.

MAJ Nathaniel D. Bastian, Ph.D. serves as Senior Data Scientist and Artificial Intelligence (AI) Engineer at the Department of Defense (DoD) Joint Artificial Intelligence Center. He provides technical advisement for AI research, design conceptualization, prototyping, systems architecture, product development, and software deployment, leading to the operationalization of AI-enabled products and technologies to solve novel, complex problems that span the DoD. MAJ Bastian previously served as Operations Research Scientist and Assistant Professor at the Army Cyber Institute at the U.S. Military Academy, where he led cyber research efforts within the Intelligent Cyber-Systems and Analytics Research Laboratory. He holds a Ph.D. degree in Industrial Engineering and Operations Research from the Pennsylvania State University, M.Eng. degree in Industrial Engineering from Penn State, M.S. degree in Econometrics and Operations Research from Maastricht University, and B.S. degree in Engineering Management (electrical engineering) with honors from the U.S. Military Academy at West Point.

A multitude of military capabilities contribute to information warfare. Intelligence gathering is a primary tool for assessing the information environment because it significantly enhances Joint Force leaders' understanding of the relationships among the physical, informational, and cognitive dimensions.[6] The primary purpose of information collection, analysis, and dissemination has not changed, but intelligence gathering has evolved since the 18th century.[7] In the mid-1750s, for example, Frederick the Great employed a most impressive long-term intelligence system for gathering information.[8] In fact, according to Christopher Duffy, Frederick pumped "travelers for news of the tactics and weapons of his potential enemies, and, indeed, for any information that might enable him to build up character-pictures of their rulers and generals."[9] Moreover, he created spy networks by planting Prussian agents in enemy countries to establish information channels, and Duffy contends that he briefed his Prussian officers to conduct reconnaissance on roads, passes, rivers, bridges and other terrain when traveling.[10] Similar to today, Frederick's primary reason for using intelligence gathering on the battlefiel was to learn about an adversary or enemy's potential capabilities or vulnerabilities.[11] Despite his extensive use of intelligence gathering, however, Frederick was often challenged in his efforts to obtain reliable, accurate information about enemy battle plans.[12]

This challenge was underscored by Carl von Clausewitz, who observed that "many intelligence reports in war are contradictory; even more are false, and most are uncertain [...] the reports turn out to be lies, exaggerations, errors, and so on. In short, most intelligence is false, and the effect of fear is to multiply lies and inaccuracies."[13] Despite these inherent imperfections associated with intelligence gathering, its use as an integral component of information warfare is not a modern-day concept. As noted, Frederick the Great conducted information warfare using intelligence gathering because he wanted to leverage the information collected for operational and tactical planning, as well as determine the most effective way to elicit the specific response he desired from the enemy or adversary.[14]

In addition to intelligence gathering,18th century leaders targeted information warfare against enemy decision-making processes. Military deception (MILDEC) is one such information-related capability that these leaders used. They would attempt to influence an adversary's perceptions via actions that they executed deliberately to mislead adversary decision makers.[15] Duffy reports that Frederick the Great thoroughly relished using tricks and ruses to conceal his own intentions; he had roads repaired as if in preparation for a retreat, assigned fictional names to regiments, and even arranged the capture of his couriers who had false messages.[16] As evidenced, Frederick the Great employed MILDEC to lead adversary military decision makers to incorrect conclusions about his force's capabilities and intentions by targeting their informational and cognitive processes.[17] Unlike Frederick the Great, however, Clausewitz viewed MILDEC as mostly ineffective as the general officer qualities of deception (craft, cleverness, and cunning) were not prominent in the history of war.[18] Clausewitz saw limited value in the issuance of false plans, orders and reports to sow confusing in the enemy.[19] Despite Clausewitz's general negative view of MILDEC, he did proffer that "when prudence, judgment, and ability no longer suffice, cunning may well appear the only hope."[20] While Frederick the Great and Clausewitz seem to have disagreed on the effectiveness of using MILDEC, history confirms that 18th century leaders did conduct information warfare by employing IO activities, particularly deception. This resonates with Sun Tzu's perspective that warfare is based upon deception.[21]

Not only did 18th century leaders employ MILDEC as an information-related capability; 19th century leaders also conducted information warfare via military information support operations (MISO). JP 3-13.2 defines MISO as "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives."[22] For example, Michael Hughes suggests that Napoleon often issued proclamations to portray France as the victim of foreign aggression while serving as the French Emperor in the early 1800s.[23] Napoleon ensured that his proclamations were published in newspapers, posted on placards, and spread around adjacent countries to influence the civilian population of the Empire and European neighbors.[24] Hughes also claims that in addition to his widely disseminated proclamations, Napoleon used trusted agents to circulate his Bulletin de la Grande Armée throughout neighboring countries to influence foreign leaders and manipulate public opinion.[25] and dispersing bulletins to "justify France's involvement in the Napoleonic wars and mobilize support for the struggle against the Allies."[26] As evidenced, Napoleon's actions in the 19th century illustrated deliberate employment of MISO as a means of information warfare to leverage the informational element of the instruments of national power to achieve French strategic objectives, and to influence diplomatic, informational, military, economic and other social or infrastructural aspects of the operational environment.[27]

The foregoing 18th and 19th century examples of information warfare illustrate offensive-oriented forms of information-related capabilities. Information warfare also entails defensive-oriented activities designed to safeguard information which the Joint Force depends upon to conduct military operations. One such information-related capability is operations security (OPSEC), which JP 3-13.3 describes as a "capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities."[28] Napoleon's method of disseminating military orders clearly demonstrated his attention to the OPSEC information-related capability. According to Baron de Jomini, for example, Napoleon delivered detached orders to his marshals in a way that prescribed "for each one simply what concerned himself, and only informing him what corps were to operate with him, either on the right or the left, but never pointing out the connection of the operations of the whole army."[29] In this manner, Napoleon employed OPSEC by actively safeguarding critical information via a need-to-know method for orders dissemination. This was further emphasized by Jomini, who stated, "I have good reasons for knowing that he did this designedly, either to surround his operations with an air of mystery, or for fear that more specific orders might fall into the hands of the enemy and assist him in thwarting his plans."[30]

Jomini noted that like Napoleon, Frederick the Great also actively practiced OPSEC measures to identify, control, and protect critical information associated with specific military operations and activities. Jomini illustrated this, reporting that "it is certainly of great importance for a general to keep his plans secret; and Frederick the Great was right when he said that if his night-cap knew what was in his head, he would throw it into the fire."[31] As described, Napoleon and Frederick the Great both conducted defensive-oriented information warfare through the intentional employment of OPSEC as an information-related capability. History also confirms that these two 18th century leaders actively exercised OPSEC processes to prevent adversaries from garnering the information needed to assess friendly capabilities and intentions correctly.[32]

The preceding discussion makes it plain that the concept of information warfare was not born in the early 20th century. The basic ideas date back millennia. 18th and 19th century leaders operationally manipulated the information environment and leveraged other information-related capabilities to conduct information warfare against their adversaries. These leveraged information activities included intelligence gathering, military deception, military information support operations, and operations security.

Nonetheless, the proliferation and application of advanced technology has opened a Pandora's box in terms of the breadth and depth for which the information domain can expand and further impact (positively and negatively) the operational environment and leaders' understanding of it. As such, the rapid and widespread emergence of information-related capabilities and resulting cyber threats has profoundly altered the nature of information warfare, presenting extreme, complex challenges Joint Force leaders must meet if they are to dominate the multi-domain battlefield worldwide. As technological innovations continue, improved methods for conducting information warfare will emerge, especially with the continued revolutionary growth and scalability of techniques that leverage artificial intelligence. The key question that remains is whether the Joint Force will succeed in dominating the information environment in the physical, informational and cognitive dimensions.

NOTES

1. Department of Defense, *Joint Publication (JP) 3-13 Information Operations, Chg. 1* (Washington DC, 2014) I-1.
2. Headquarters, Department of the Army, *Field Manual (FM) 3-0 Operations, Chg. 1* (Washington DC, 2017) 1-6.
3. Ibid., 1-9.
4. Department of Defense, *JP 3-13 Information Operations,* I-1.
5. Jonathan B. A. Bailey, "The First World War and the birth of modern warfare," in *The Dynamics of Military Revolution: 1300-2050,* ed. MacGregor Knox and Williamson Murray (New York: Cambridge University Press, 2001), 147.
6. Department of Defense, *JP 3-13 Information Operations*, II-10.
7. Ibid.
8. Christopher Duffy, *The Army of Frederick the Great* (New York: Hippocrene Books, Inc., 1974), 145.
9. Ibid.
10. Ibid.
11. Department of Defense, *JP 3-13 Information Operations*, II-10.
12. Duffy, *The Army of Frederick the Great*, 145.
13. Carl Von Clausewitz, "Intelligence in War," in *On War*, ed. Michael Howard, trans. Peter Paret (Princeton: Princeton University Press, 1976), 117.
14. Department of Defense, *JP 3-13 Information Operations,* II-10.
15. Ibid.
16. Duffy, *The Army of Frederick the Great*, 146.
17. Department of Defense, *JP 3-13.4 Military Deception* (Washington DC, 2017) II-1.
18. Carl Von Clausewitz, "Cunning," in *On War*, ed. Michael Howard, trans. Peter Paret (Princeton: Princeton University Press, 1976), 202.
19. Ibid.
20. Ibid., 203.
21. Sun Tzu, "On The Art of War," in *Roots of Strategy: The 5 Greatest Military Classics of All Time*, ed. Thomas R. Phillips (Mechanicsburg: Stackpole Books, 1985), 23.
22. Department of Defense, JP 3-13.2 *Military Information Support Operations* (Washington DC, 2017) I-2.
23. Michael J. Hughes, *Forging Napoleon's Grande Armée: Motivation, Military Culture, and Masculinity in the French Army, 1800-1808* (New York: New York University Press, 2012), 29.
24. Ibid., 30
25. Ibid., 31.
26. Ibid.
27. Department of Defense, JP 3-13.2 *Military Information Support Operations*, I-1.
28. Department of Defense, JP 3-13.3 *Operations Security* (Washington DC, 2016) I-1.
29. Antoine Henri de Jomini (Baron de. Jomini), "Chapter VI. Logistics; or, the Practical Art of Moving Armies," in *Summary of the Art of War*, originally published in French in 1836, trans. Capt. G. H. Mendell and Lieut. W.P. Craighill in 1862 (Rockville: Arc Manor, 2007), 193.
30. Ibid.
31. Ibid.
32. Department of Defense, *JP 3-13.3 Operations Security*, I-4.