The Future Is Now

Marine Corps operations in the information environment

by James McGinley & Arthur Speyer

In today's complex operating environment, information is a crucial role at the strategic, operational, and tactical levels. Information is so powerful that it is recognized as both an element of U.S. national power and a joint warfighting function. Technology increases the speed information can travel, and technology diffusion increases the accessibility and lethality of our adversaries' information-enabled weapons.[1] To counter these information-enabled weapons, the Marine Corps needs to be a force equipped to handle and dominate the information environment (IE). Knowing how to maneuver within the IE is essential in modern warfare, and the first step to successfully maneuvering within the IE is understanding what the IE is.[2]

>Dr. McGinley and Mr. Speyer are senior analysts at the Marine Corps Intelligence Activity (MCIA).

Leveraging the information environment will generate our operational tempo. *(Photo by Cpl Tessa Watt.)*

Understanding the IE

The IE is an aggregate of individuals, organizations, or systems that collect, process, or disseminate information, including the information itself. Although the Internet, wireless communications, social media, and automated networks provide new avenues for our adversaries to shape the IE, this evolved IE environment also provides new opportunities for Marines to gain a decisive advantage. Cyber warfare, electronic warfare (EW), influence operations, deception operations, and intelligence, surveillance, and reconnaissance (ISR) activities enhance our ability to interpret and influence the IE. Leveraging the IE is about generating operational tempo, improving effectiveness, and increasing lethality. Understanding the IE enables a force to reduce its own battlefield friction while increasing the enemy's battlefield friction.[3]

Conflict is as much a war of narrative as it is a physical contest. Competitors engage in a battle of narratives, seeking

to shape perceptions and control the dissemination and message of information. Contests in the IE are complex because they combine diplomatic, military, political, humanitarian, security, social, economic, and information dimensions. This complexity creates opportunities for adversaries to exploit, disrupt, and disable command and control systems, hinder critical infrastructure, disseminate disinformation, foster internal dissent, recruit supporters worldwide, and promote their legitimacy while discrediting the legitimacy of others.

The era of U.S. technical dominance is over. Advanced cyber and surveillance capabilities are increasingly available to adversaries. The world is moving toward increased connectivity levels that will further change how people will gather, share, and consume information. Emerging technologies, including the Internet of Things, artificial intelligence (AI), and quantum computing, promise even greater revolutionary changes. Social media gives an asymmetric advantage to adversaries who can quickly produce and disseminate unfiltered information and disinformation to audiences worldwide.[4] Rapidly spreading information will cause Marines to operate and fight in an IE where persistent global surveillance will challenge their ability to approach areas undetected and untargeted.

Marines confront a diverse and complex array of global crises. The IE is a contested environment where adversaries challenge U.S. power projection from many dimensions, including the physical, informational, and cognitive. Forces that build the IE into their operational design will gain a significant advantage. The future IE will be increasingly lethal (placing a premium on maneuver, dispersion, deception, and signature management), increasingly adaptive (elevating the importance of information, intelligence, and decision making), and increasingly interconnected (allowing information and informational activities to converge, amplifying their effects).

Technology

The IE's complexity is fueled by technology. Off-the-shelf unmanned systems, commercially available GPS, and cellular networks combine to facilitate rapid advances in precision lethality. Technology trends will favor the tactical offensive, significantly enhancing an adversary's ability to find and strike massed or high-value targets with precision—often enabled by ISR systems that target battlespace signatures.[5] (See Figure 1.)

Figure 1. *(Figure provided by author.)*

Threats from technology-empowered adversaries will force Marines to rethink how they sense, communicate, and fight in contested IEs. China, Russia, North Korea, Iran, and extremist organizations are expanding their capacity to sense the battlespace, deny communications, attack networks, and manipulate information. Information technology's greatest advantage, and its greatest vulnerability, is its ability to connect. Our adversaries know that we depend on a limited number of critical information capabilities, and our adversaries will attack these capabilities at the exact time we need them the most.[6]

Technology trends will favor the tactical offensive, significantly enhancing an adversary's ability to find and strike massed or high-value targets with precision—often enabled by ISR systems that target battlespace signatures.

Fire and Maneuver

Maneuver warfare is a competition of seeking versus hiding. The proliferation of systems that can rapidly analyze and disseminate data makes it harder for forces to move undetected. Militaries that cling to the past and invest in more expensive and exquisite traditional systems will be detected and destroyed. High-volume, low-cost disposable weapons systems are becoming the norm.

Although technology will not alter the central role of fires (rate, ranges, accuracy, and lethality), technology diffusion will lower the barriers for acquiring a precision fires capability.[7] Fires are not limited to physical projectiles; fires has become the broader ability to project effects onto an enemy, including cyber, EW, directed energy, and information warfare. Fires will grow more ferocious as technology improves lethality through greater precision, and greater precision will give the advantage to the force that fires first.

Russian operations in Ukraine and Syria demonstrate Russia's commitment to the employment of IE as a key warfighting component. Chinese doctrine calls for preparing for not only physical warfare but also legal, cyber, and psychological warfare. Violent extremist organizations gather recruits and financial support through the Internet and social media. All of these actors disseminate biased and false information using digital technologies and exploit global audiences to disrupt and delegitimize U.S. operations.[8]

Space-based Assets

Our space capabilities make it possible for the Marine Corps to sense the battlespace more clearly, communicate with certainty, navigate with accuracy, and strike with precision. Adversaries are aware of these advantages and are fielding capabilities to challenge our space-based assets. From simple jammers to anti-satellite weapons, denying our space capabilities is a central tenet of our adversary's strategies.[9]

China and Russia are pursuing counter-space weapons.[10] Counter-space weapons and threats can include kinetic physical strikes against satellites or ground stations; non-kinetic strikes with lasers, high-powered microwaves, and electromagnetic pulse weapons; electronic attacks through jamming or spoofing; and cyberattacks targeting computers and data.[11] Adversaries will increasingly have access to space-based imagery and weather data; communications; and positioning, navigation, and timing information. Anyone with enough money will be able to buy or rent commercial space assets.

Fires are not limited to projectiles. *(Photo by Cpl Tessa Watt.)*

Weaponized Information

The battle of the narrative is no longer just fought at the strategic level. The perception of events rapidly alters the tactical situation, particularly in crowed urban environments. Technology allows anyone to film, edit, and share information in near-realtime. Every individual can be an information actor and distribute messages, true or false, to a global audience. Deep fake videos allow messages to spread quicker than they can be disavowed. Governments and traditional media are no longer the dominant players in the information space.[12]

An entire generation only knows an Internet world. These digital natives share and receive information in virtual environments in methods that are fundamentally different than the way past generations shared and received information. The spread of mobile technology, particularly in developing nations, has dramatically increased the ability to rapidly access and share information. Individuals leverage social media to energize protests in a fraction of the time it took only a few years ago. Internet-connected personal devices with cameras and full-motion video allow much of the world to share and observe events as they unfold. Adversaries can use the same technological advances for operational purposes as well as for propaganda and disinformation.[13]

Marines will be challenged by state and non-state actors as they attempt to control the narrative. Adversaries use digital technology and social media to disseminate biased and false information to global audiences to disrupt and delegitimize U.S. operations. These disinformation campaigns pose a threat to Marines down to the tactical level as the campaigns can quickly undermine the Marines' relationship with local populations.[14]

Reconnaissance-strike Complex

Adversaries are using the IE to integrate surveillance, maneuver, and strike into a more seamless network. For example, Russia's reconnaissance-strike complex links high-precision, long-range weapons with realtime intelligence data.[15] The ability to hide, mask,

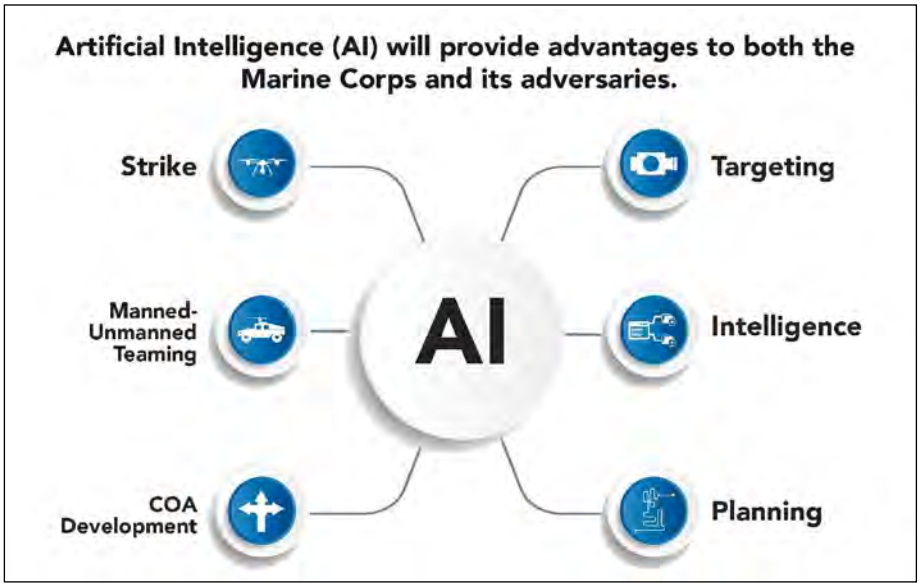

Figure 2. *(Figure provided by author.)*

or deceive unit locations will become increasingly important as the battle of sensors and signatures intensifies.

Advances in the IE are allowing competitors and non-state actors to merge reconnaissance feeds with firing assets to create extremely rapid sensor-to-shooter kill chains. The IE-driven networks will also increase precision, allowing for fewer munitions to be transported, maintained, and stockpiled.[16] Some munitions will be supersonic, whereas others will loiter, hover, or perch. By networking IE-enabled sensors, future munitions will become highly maneuverable and will hunt targets, even in complex urban environments.[17] Some IE-enabled strike platforms will be fused with manned or unmanned teams with the ability to maneuver autonomously and execute fires on command from remote locations. Not all munitions will be kinetic, some loitering systems will conduct EW or wirelessly deploy malware into enemy systems. Large static locations, such as supply depots and forward arming and refueling points, will be increasingly difficult to protect.

The Convergence of Big Data and AI

Every 24 hours, humans create 2.5 quintillion (a billion billion) bytes of new data. This amount of information spurns the rise of big data. Information created within the past 24 months makes up 90 percent of the data available in the world. AI is harnessing big data by making it possible for machines to learn over time, adjusting to the massive flow of new inputs to gain insights, make decisions, and perform tasks without human intervention. Big data feeds AI, and AI empowers big data.[18] (See Figure 2.)

AI and the Kill Chain

The integration of information and firing systems is shortening the time it takes for adversaries to sense the environment. AI is the future of sensor-to-shooter networks. AI-based fire systems create the ability to find, fix, and finish targets faster than a human can. Once deployed, AI-based fire systems progress through the kill chain internally or via a network of autonomous weapons working together. Depending on the level of permissions granted, these weapons will send a signal back once a target is fixed, along with the evidence required to garner strike approval. With approval, a command signal is sent, weapons engage, and the kill chain is complete (finish and feedback). If the weapons are fired with the appropriate approval, then the entire kill chain could be completed autonomously. These integrated enemy networks reduce Marine Corps advantages in shooting, moving, and communicating.[19]

ISR

As inexpensive sensors proliferate and as competitors and adversaries extend the range of sensing systems, ISR networks will expand. Developments in high-performance computing and AI that can rapidly identify events and patterns within large data sets will enhance the ISR sensor integration.[23]

Smart Sensors

Smart sensors receive input from their physical environment and use internal processors to monitor, detect changes, analyze data, and communicate the results or make decisions and control processes. When connected through networks, smart sensors can create a smart grid capable of monitoring and reacting over large areas.[24]

The Targeting Threat

Adversaries will continue to develop long-range strike capabilities with an array of sensor and missile technologies to limit U.S. power projection capabilities. The global proliferation of sensor-capable and weaponized unmanned aerial systems has created a critical need for counter-unmanned aerial systems capabilities. Cyber threats will persist as social media and cyber footprints signal Marines' presence and as cloud-based computing solutions erase the difference between internal and external networks.[25]

Implications

Marines need to view IE operations as integral to the single battle concept. Cyber and electromagnetic space is simply an extension of the physical space; they all enable commanders to maneuver to present the enemy with a dilemma. There are no permissive IEs. In tomorrow's fights, being detected can mean being targeted, which can mean being killed. The force that can sense and understand the actions of its opponents in the IE will fight from an advantageous position.[26] This warfighting approach requires innovative concepts, creative tactics, new systems, and—most importantly—smart Marines.

Notes

1. Christopher Zember, "The Democratization of Science Ushers in a New World Order," *War on the Rocks*, (Online: April 2016), available at https://warontherocks.com.

2. Alexus Grynkewich, "Introducing Information as a Joint Function," *Joint Forces Quarterly*, (Washington, DC: May 2018).

3. Department of Defense, *Strategy for Operations in the Information Environment*, (Washington, DC: June 2016).

4. Christopher Meserole, "Wars of None: AI, Big Data, and the Future of Insurgency," (Washington, DC: Brookings, July 2018).

5. Connie Lee, "Spoofing Risks Prompt Military to Update GPS Devices," *National Defense Magazine,* (Washington, DC: January 2018).

6. Christopher Paul, Colin P. Clarke, Michael Schwille, Jakub P. Hlavka, Michael A. Brown, Steven Davenport, Isaac R. Porche III, Joel Harding, "Lessons for Future U.S. Army Operations in and Through the Information Environment," RAND Corporation, (Washington, DC: June 2018).

7. Isaac Porche, "Redefining Information Warfare Boundaries for an Army in a Wireless World," RAND Corporation, (Washington, DC: 2013).

8. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, (Washington, DC: 2019); and Michael Kofman and Katya Migacheva, "Lessons from Russia's Operations in Ukraine," RAND Corporation, (Washington, DC: May 2017).

9. Defense Intelligence Agency, "Challenges to U.S. Security in Space," (Washington, DC: February 2019).

10. Bruce MacDonald, "China, Space Weapons, and U.S. Security," Council on Foreign Relations, (New York, NY: June 2008).

11. Dan Coats, "Statement for the Record Worldwide Threat Assessment of the U.S. Intelligence Community," (Washington, DC: February 2018); and Lara Seligman, "Russian Jamming Poses a Growing Threat to U.S. Troops in Syria," *Foreign Policy*, (Washington, DC: July 2018).

12. U.S. Army Training and Doctrine Command, "The Death of Authenticity: New Era Information Warfare," (Fort Eustis, VA: May 2019).

13. Jose Antonio Vargas, "Spring Awakening," *The New York Times*, (New York, NY: February 2012); and Elizabeth Gibney, "The Scientist Who Spots Fake Videos," *Nature News*, (London, UK: October 2017).

14. John DeRosa, "Revising the Battle of the Narrative," *Small Wars Journal*, (Online: 2015), available at https://www.smallwarsjournal.com.

15. Les Grau and Charles Bartles, "The Russian Reconnaissance Fire Complex Comes of Age," U.S. Army Foreign Military Studies Office, (Fort Leavenworth, KS: May 2018).

16. Richard Mosier, "Breaking the Anti-Ship Missile Kill Chain," Center for International Maritime Security, (Washington, DC: February 2018).

17. Iain Thomson, "Smart Bombs, Smart Bullets, Now Guided Smart Artillery Shells, Thanks to DARPA Dosh," *The Register*, (London, UK: 2017).

18. Bernard Marr, "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," *Forbes*, (Jersey City, NJ: March 2019).

19. Mike Benitez, "It's About Time: The Pressing Need to Evolve the Kill Chain," *War on the Rocks*, (Online: May 2017), available at https://warontherocks.com.

20. Daniel Urchick, "Advanced ISR Sensors and Their Impact on 'Military Power'," *Defence IQ*, (Online: October 2018), available at https://defenceiq.com.

21. Sharon Shea, "Use Cases and Benefits of Smart Sensors for IoT," *IoT Agenda*, (Online), available at https://internetofthingsagenda.com.

22. Staff, "McAfee Labs 2016 Threats Predictions," McAfee Labs, (Santa Clara, CA: 2016).

23. Headquarters Marine Corps, *Marine Corps Operating Concept*, (Washington, DC: September 2016).