The Age of Chinese Espionage

Revamping Marine Corps intelligence

by 2ndLt Cybèle C. Greenberg, USMCR

"What is the quickest way you can destroy an organization? … Mistrust and discord." [1]

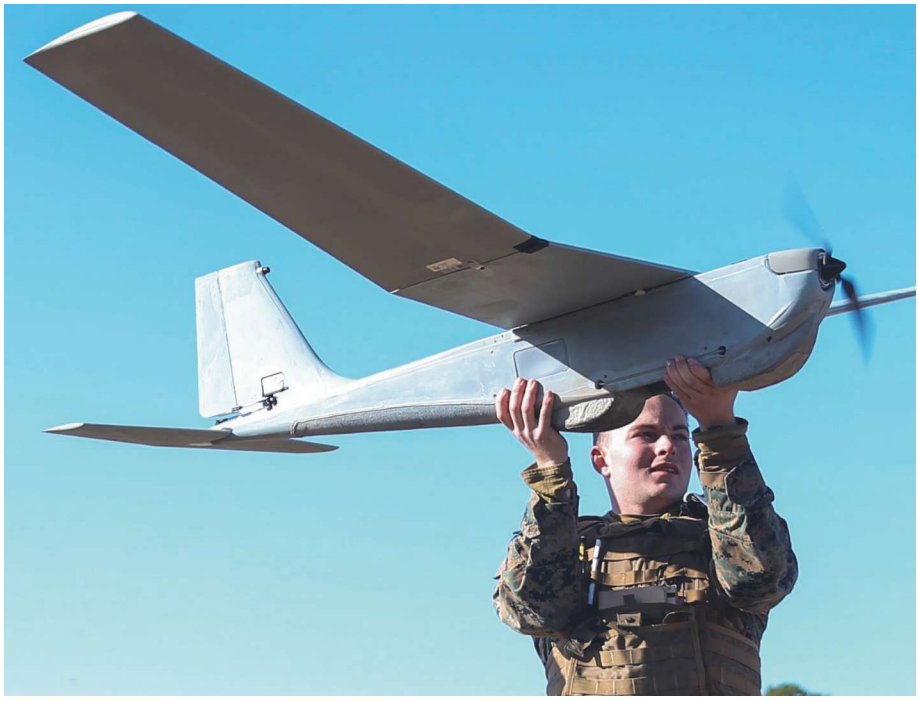
In January, the *New York Times* reported the expulsion of two Chinese Embassy officials accused of illegally gathering sensitive information on a special operations U.S. naval base in Norfolk, VA.[2] These expulsions are the first of this nature in 30 years; the last recorded incident occurred in 1987, when two Chinese Embassy employees with diplomatic cover were forced to leave the United States after getting caught accepting classified National Security Agency documents.[3]

According to the *Times*, the January expulsions "show the American government is now taking a harder line against suspected espionage by China."[4] Indeed, over the course of the last few years, a series of offensive actions by the United States' greatest strategic rival—including the Chinese cyber breach of the Office of Personnel Management (OPM) in 2015 and President Xi Jinping's ongoing revamping of the People's Liberation Army (PLA)'s intelligence networks—demonstrate the Marine Corps' dire need for a cutting-edge, updated intelligence program that both leverages and protects against modern technology.

MCDP 2, *Intelligence*, explains the importance of intelligence within the larger, overarching functions of tactical command and control.[5] Often, effective intelligence is "the critical factor […] in mission success or failure."[6] Within tactical planning, input from intelligence sources is what allows small unit commanders to anticipate the enemy's most likely course of action. This is one of the unique and most challenging aspects of intelligence: it "deals directly with an independent, hostile will personified by the enemy."[7] The influx of information from modern technology sources adds an additional layer of complexity to intelligence operations today. *MCDP 2* warns,

> [while] it is alluring to believe that the information revolution will solve the problems of uncertainty in dealing with the enemy, technology has its shortcomings as well.[8]

In this statement, "shortcomings" refers to the new vulnerabilities that inevitably complicate the movement of informa-



We need to invest in a superior force and equipment to support intelligence gathering. *(Photo by Cpl Tiana Boyd.)*

>2ndLt Greenberg is a provisional CI/HUMINT Intelligence Officer in the USMC Reserves. Upon graduating from MOS school, she has been assigned to join ISB in Brooklyn, NY.

tion from traditional paper sources to the cyber sphere.

One incident that clearly demonstrated some of these shortcomings was the Chinese cyber breach of the OPM in 2015: a breach in which hackers stole personally identifiable information from millions of U.S. Government employees. An article by Ian T. Brown published in the Fall 2019 issue of the *Marine Corps University Journal* explores how the Chinese government could potentially use the information gathered from this breach to mount a deliberate cyberattack against Americans at some point in the near future in retaliation for U.S. actions in the South China Sea. Brown makes the case for treating these cyberattacks with the upmost seriousness, arguing that certain unique aspects of the attacks—such as the fact that the hackers did not attempt to sell the information to third parties right away—suggest that "the hackers have plans for the data beyond a quick payday."[9] Indeed, Brown is convinced that the purpose of the attacks goes beyond "[disrupting] or [degrading] American military or intelligence systems" themselves to something more sinister. According to him, the goal is likely to target the very "cohesion of the organization [the U.S. Government]" by leveraging the information obtained from the online database to "spread fear, mistrust, and discord among the men and women in uniform who operate those [military and intelligence] systems."[10]

In addition to condoning cyberattacks—however implicitly—against the U.S. Government, President Xi Jinping is also leading the Chinese PLA through a systematic reform program. The goal: a military enterprise that can rival even that of the Americans. An anthology of essays on these PLA reforms, first written for the 2016 and 2017 PLA conference series co-sponsored by Taiwan's Council of Advanced Policy Studies, National Defense University, and the RAND Corporation, explores the implications of Xi's vision for what he has previously called "the great rejuvenation of the Chinese nation."[11] Most relevant to this paper was the creation in 2015 of a new independent military branch of the PLA called the strategic support force (SSF). In the anthology's introduction, the editors explain the SSF was meant to

> [consolidate] a variety of functions related to the information domain, including space and cyber operations, electronic warfare, and even some psychological warfare capabilities.[12]

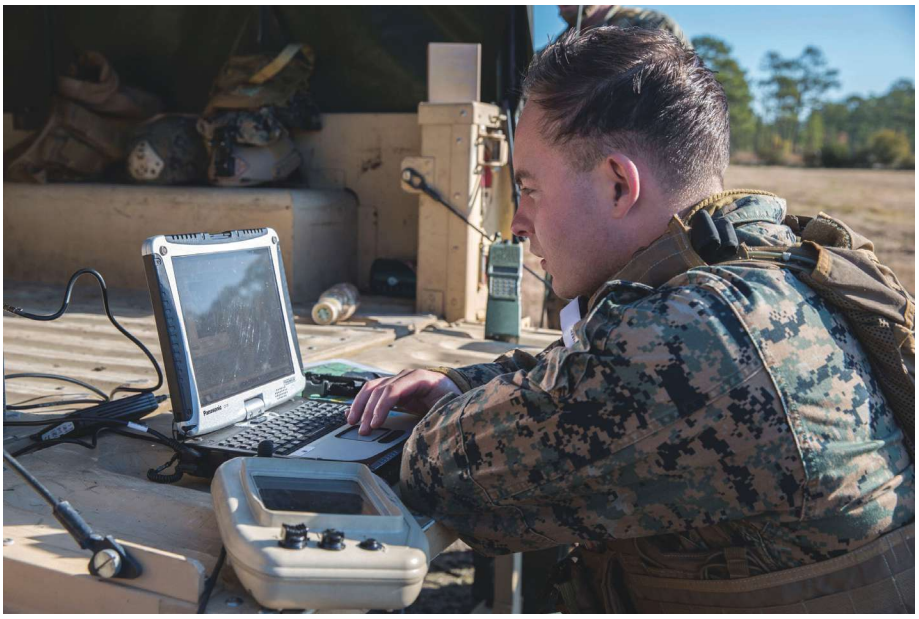
In one essay titled "Large and In Charge: Civil-Military Relations under Xi Jinping," Phillip C. Saunders and Joel Wuthnow argue the creation of the SSF was less about structural reform and more about centralizing control and command with regards to information flow.[13] With this new system of joint commands and one ultimate collection point for intelligence reports, it is easier for Xi and his senior military commanders to order and supervise offensive information gathering efforts on the United States and other key players in the southeastern region. The anthology editors explain that PLA strategists spent several years studying the structures of other successful military systems, including that of the United States and Russia, and subsequently decided to focus their reforms on "high-technology warfare," including "superior weapons technology; battlefield integration between air, land, and sea; high-speed, all-weather operations; new modes of long-range warfare, especially missile, electronic, and air warfare; and a premium on [command, control, communications, and intelligence] dominance."[14] The creation of the SSF, then, is "an intermediate step toward informationized war, using information systems and a defined degree of informationized weapons to carry out war."[15]

From both the OPM attack and the PLA reforms, we can draw several conclusions. First, these incidents and programs highlight the importance of continuously investing in a superior military intelligence force that can handle both offensive and defensive operations as information warfare becomes an increasingly large part of Marine Corps warfighting today. Second, however, we must be careful to heed the warning originally given in *MCDP 2* about a dangerous overreliance on technology. As we ensure our electronic and cyber intelligence capabilities always stay ahead of those of our peers, we must also bolster our more traditional intelligence gathering mechanisms, including investing time in culturally understanding our enemy and the local population within our area of operations.

The importance of human intelligence missions was clearly demonstrated by the Marine Corps' operations in Somalia in both Operation Restore Hope in 1992 and Operation United Shield in 1995.

The importance of human intelligence missions was clearly demonstrated by the Marine Corps' operations in Somalia in both Operation Restore Hope in 1992 and Operation United Shield in 1995. In 1992, when the first Marines landed in Mogadishu, they had only a very rudimentary and incomplete picture of the Somali culture and clan structure. Understanding the importance of cultural fluency, however, the Marines of Operation Restore Hope quickly established relationships with local leaders to gather information and garner strong local support. *MCDP 2* explains the larger implications of such efforts, and especially how they pertained to follow-on missions:

> This intelligence was used over the course of the campaign to plan and execute numerous successful tactical actions ... When the Marines of I Marine Expeditionary Force (MEF) returned in February of 1995 to assist in the final withdrawal of U.N. forces, they were able to draw on an extensive



Are we becoming too technologically dependent? ***(Photo by LCpl Larisa Chavez.)***

reservoir of intelligence to plan and execute Operation United Shield.[16]

Ultimately, 1 MEF was able to develop a playbook—completely independently of high technology resources—that helped anticipate Somali reactions to various U.S. operations, something that "contributed directly to the safe and effective accomplishment of the mission."[17]

Chinese intelligence agents have also recognized the importance of blending traditional human intelligence missions with modern technology. One recent execution of this two-pronged strategy was the recruiting of American and other foreign sources from LinkedIn profiles. William R. Evanina, the director of the National Counterintelligence and Security Center, explained the thought process behind these operations in a recent *New York Times* article: "Instead of dispatching spies to the U.S. to recruit a single target, it's more efficient to sit behind a computer in China and send out friend requests to thousands of targets using fake profiles."[18] By reaching out to Americans through LinkedIn, Chinese agents hope to leverage technology to gain a better understanding of our culture, needs, consumer desires, and tolerance for certain political actions. This is how Chinese agents start to form relationships with potential sources. As the article explains:

> Chinese agents often make offers over […] LinkedIn […] to bring the prospective recruit to China, sometimes through the guise of a corporate recruiting firm offering to pay them for speaking or consulting engagements or aid in research. From there, agents develop the relationship.[19]

Going forward, it is imperative that the Marine Corps continue to develop an intelligence plan fit for today's operations and able to counter our future enemies. Building up high technology to gather intelligence from the cyber sphere is important, but it can only supplement—and not replace—more traditional sources of intelligence, such as forming meaningful relationships with members of local groups and cultures. A well-developed yet simple intelligence program, hand-in-hand with sound infantry and combat arms tactics, will set us apart from peer competitors as well as enable us to fight and win wars against our enemies.

Notes

1. Col John Boyd, USAF(Ret), quoted in Ian Brown, *A New Conception of War,* (Quantico, VA: Marine Corps University Press, 2018).

2. Edward Wong and Julian E. Barnes, "U.S. Secretly Expelled Chinese Officials Suspected of Spying After Breach of Military Base," *New York Times,* (New York, NY: December 2019).

3. Edward Wong, "How China Uses LinkedIn to Recruit Spies Abroad," *New York Times,* (New York, NY: August 2019).

4. "U.S. Secretly Expelled Chinese Officials Suspected of Spying After Breach of Military Base."

5. Headquarters Marine Corps, *MCDP 2, Intelligence*, (Washington, DC: 1997).

6. Ibid.

7. Ibid.

8. Ibid.

9. Ian T. Brown, "Cyber's Cost: The Potential Price Tag of a Targeted 'Trust Attack,'" *MCU Journal: Economics of Defense*, (Quantico, VA: Marine Corps University Press, 2019).

10. Ibid.

11. Joel Wuthnow and Phillip C. Saunders, "Introduction: Chairman Xi Remakes the PLA," in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms,* (Washington, DC: National Defense University Press, 2019).

12. Ibid.

13. Phillip C. Saunders, and Joel Wuthnow, "Large and in Charge: Civil-Military Relations under Xi Jinping," in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms.*

14. John Chen, "Choosing the "Least Bad Option: Organizational Interests and Change in the PLA Ground Forces," in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*.

15. Ibid.

16. *MCDP 2, Intelligence*.

17. Ibid.

18. "How China Uses LinkedIn to Recruit Spies Abroad."

19. Ibid.