REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
	Master's of Military Studies	

4. TITLE AND SUBTITLE
U.S. Army Adaptation to the Information Collection Environment: 2018-2026

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Albert, John, L, Major, USA

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
Joyner, James PhD

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Adversary development of reconnaissance sensors, platforms, and networks has substantively increased U.S. Army difficulty in protecting critical information. Robust adversary reconnaissance systems have increased the accuracy and range of information collection while improving the speed of information dissemination. The Army Operating Concept and Army FM 3-0 Operations emphasize the need to adapt to the changing reality of technically sophisticated adversaries. In the near term, the Army organizes adapting to the current information collection environment by favoring active counterreconnaissance solutions. Active solutions are better suited to countering the advantages existing in adversary reconnaissance systems. Additionally, the Army adjusts its organization to enable high tempo counterreconnaissance to occur. Reducing organizational friction gives counterreconnaissance actions the opportunity to compete at the same tempo as adversary reconnaissance systems. Finally, the Army decentralizes and emphasizes deception operations. Doing so increases battlefield ambiguity and degrades adversary information collection in instances where the adversary reconnaissance system cannot be denied outright.

15. SUBJECT TERMS
counterreconnaissance; OPSEC, information collection, information protection, adaptation

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					USMC Command and Staff College
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU		**19b. TELEPHONE NUMBER** *(include area code)*
Unclass	Unclass	Unclass			(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

U.S. Army Adaptation to the Information Collection Environment, 2018-2025

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Major John Albert
United States Army

AY 17-18

Mentor and Oral Defense Committee Member: Dr. James H. Joyner
Approved: James H. Joyner
Date: 27 MAR 2018

Oral Defense Committee Member: LTC Paul Armstrong
Approved: Paul M Armstrong
Date: 27 MAR 2018

Executive Summary

Title: U.S. Army Adaptation to the Information Collection Environment: 2018-2025

Author: Major John Albert, United States Army

Thesis: The Army should adapt to the current information collection environment by favoring active and high tempo counterreconnaissance while decentralizing deception to deny adversary information collection.

Discussion: Adversary development of reconnaissance sensors, platforms, and networks has substantively increased U.S. Army difficulty in protecting critical information. Robust adversary reconnaissance systems have increased the accuracy and range of information collection while improving the speed of information dissemination. The Army Operating Concept and Army FM 3-0 Operations emphasize the need to adapt to the changing reality of technically sophisticated adversaries. In the near term, the Army should adapt to the current information collection environment by favoring active counterreconnaissance solutions. Active solutions are better suited to countering the advantages existing in adversary reconnaissance systems. Additionally, the Army should adjust its organization to enable high tempo counterreconnaissance to occur. Reducing organizational friction gives counterreconnaissance actions the opportunity to compete at the same tempo as adversary reconnaissance systems. Finally, the Army should decentralize and emphasize deception operations. Doing so increases battlefield ambiguity and degrades adversary information collection in instances where the adversary reconnaissance system cannot be denied outright.

Conclusion: Active and high tempo counterreconnaissance and deception operations represent a framework for successful adaption to the challenge of the current information collection environment.

DISCLAIMER

Table of Contents

Preface

This paper attempts to develop a framework for short-term Army adaptation to the increased threat extant in the current information collection environment. While technological development and organizational change are uneven and continuous processes, it is probable that the Army will enter combat with the forces and organizations currently existing in the near term. In this paper, I assume that the Army will not undertake major reorganizations before 2025 as service concepts such as the multi-domain battle concept are vetted, tested, funded, developed, and deployed. Further, in this paper, I present the information collection environment in stasis, that is, as a snapshot at this moment. In actuality, the constant struggle between reconnaissance and counterreconnaissance make the information collection environment dynamic and varying across operating environments. Finally, I have addressed counterreconnaissance from a unified perspective. It is obvious that protecting data on a computer in Kansas and a vehicle position in Poland require different protective techniques. However, I contend that the principles for protecting both are the same. It is the information that requires protection.

I would like to acknowledge the help of my advisor, Dr. James Joyner, for challenging my conclusions and helping me clarify and express my argument. Additionally, I would like to acknowledge the assistance of Major Marco Lyons in providing insight regarding U.S. Army future concepts.

"If we can make the enemy show his position…while concealing ours from him, we will be at full force where he is divided" – Sun Tzu[1]

In the early morning hours of July 11, 2014, massed precision rocket fire from pro-Russian separatists destroyed two Ukrainian mechanized battalions near the town of Zelenopillya, Ukraine. The barrage lasted all of three minutes.[2] Rather than relying on traditional ground scouts to gain the necessary targeting information, Ukrainian separatist forces instead used electronic warfare and cyber-attacks to force Ukrainian forces to employ easily intercepted cell phones for communication. The separatists were then able to use signals intelligence and unmanned aerial systems (UAS) to identify and confirm Ukrainian unit locations.[3] The brief, incredibly violent episode reinforces two important truths. First, inability to protect friendly information leads to losing the ability to maneuver and survive. Second, if relatively under-resourced forces such as these have such sophisticated capability, peer adversaries are fully capable of gathering critical friendly information and using it to decisive effect.

In response to the changed conditions, the United States Army has developed broad concepts that seek to drive doctrine, organization, training, material, leadership and education, personnel, and facilities (DOTMLPF) solutions. The 2014 *Army Operating Concept* offers mid and long-range solutions that seek to enable land forces to continue to project offensive land power into the middle of the century.[4] However, short term adaptations to the current environment have not been clearly established. Acknowledging the difficulty Army units will face in today's operating environment, *FM 3-0 Operations* opens with an admonition for Army and joint forces to adapt to the changed operating environment.[5] How does the Army approach adapting to deny enemy information collection efforts in the current operating environment? The Army should adapt to the current information collection environment by favoring active and

high tempo counterreconnaissance while decentralizing deception to deny adversary information collection.

This study examines how the Army can adapt to counter adversary information collection efforts. The Army term for measures taken to defy enemy reconnaissance and surveillance efforts is *counterreconnaissance*. These activities fall into two categories: passive and active.[6] The former involves activities taken on the friendly force to protect information, such as applying camouflage to vehicle positions, whereas the latter involves activities taken on enemy forces to protect information, such as fires to destroy an enemy observation post. This study will assess current threat information collection capabilities across sensors, platforms, and networks. Next, the paper will argue the Army should prioritize active counterreconnaissance adaptations in lieu of focusing primarily on passive measures. The study argues that in an environment of reconnaissance parity or deficit, the tempo of counterreconnaissance must be maximized through reorganization. Finally, the study argues the need for using and decentralizing deception measures to create counterreconnaissance effects.

Contemporary Information Collection Environment

Adversaries have developed robust, but uneven information collection abilities over the past two decades. While traditional ground reconnaissance remains a primary concern for the Army, new and improved sensor payloads, reconnaissance platforms, and communication methods have increased the range and accuracy of collection and the speed of information dissemination. Technologies previously reserved to a few great powers have diffused across nation states and nonstate actors. Additionally, information collection can now occur at significant range from the battlefield. The onward development of reconnaissance sensors, platforms, and networks has not been not uniform or ubiquitous. U.S. counteractions remain

effective in many cases. However, overall development of reconnaissance capability has eroded the ability of ground forces to avoid adversary contact and protect critical information.

Sensors

First, adversaries are employing sensor payloads with improved ability to collect critical friendly information while resisting friendly countermeasures. Except for acoustic sensors, most battlefield sensors focus on identifying changes in the electromagnetic spectrum across broad categories measuring radio, heat, and light emissions that signify the presence of enemy forces.[7] *ATTP 3-34.39 Camouflage, Concealment, and Decoys* lists nine categories of battlefield sensors: visual, near-infrared, infrared, ultraviolet, radar, acoustic, radio, multispectral, and hyperspectral.[8] Within each category, several sub-categories exist representing numerous vectors to collect battlefield information. An exhaustive survey of all types of sensor payloads would exceed the scope of this study. Further, states protect accurate information on the capability of sensors to limit an adversary's ability to develop countermeasures. To overcome this difficulty, a survey of one type of radar, the battlefield surveillance radar, will serve to demonstrate the capability change of sensor payloads across the spectrum of information collection. Because a competitive export market exists across a range of state actors for battlefield surveillance radars, capability information is publicly available as states attempt to generate sales.

Battlefield surveillance radars detect movement or electromagnetic signatures of people and equipment to identify enemy activity beyond visual range. The United States developed battlefield surveillance radar in its ongoing effort to improve early warning of Soviet ground formations massing along the central European border areas in the 1960s. Early battlefield surveillance radars had limited ranges and difficulty penetrating different types of terrain. A

1989 assessment of common U.S. and Russian ground-based surveillance radar highlighted the system limitations. The American AN/PPS-5B radar could detect personnel at five kilometers and vehicles at ten kilometers with an accuracy of twenty meters.[9] The common Soviet system, the PSNR-1, could detect personnel and vehicles at comparable ranges with an unknown degree of accuracy.[10] These battlefield surveillance radars increased ground early warning several times over traditional visual means. However, the radars still had to operate close to the forward edge of the battle area and within enemy tube artillery range. This fact made them targetable when either side employed the radars actively.

Modern battlefield surveillance radars have increased this capability significantly. The current common Russian battlefield surveillance radar available for export, the Kredo-1E model, can detect an individual human-sized target at fifteen kilometers and a tank at thirty-five kilometers with an accuracy of ten meters while simultaneously tracking twenty different targets.[11] As long ago as 2006, the Iranians operated two battlefield surveillance radars. The larger system, the 110-D, is able to detect an individual at eighteen kilometers and a heavy vehicle at forty kilometers with an accuracy of ten meters.[12] China's latest version of battlefield surveillance radar, the PL-02, is mounted on a wheeled vehicle platform and may be able to detect targets out to eighty kilometers under most weather conditions.[13] The improvement in range and accuracy of modern battlefield surveillance radar challenges the Army to counter effectively. The systems range limits the types of effects that can be brought against them and their accuracy undermines efforts at deception and dispersion.

Additionally, battlefield surveillance radar technology has diffused across more nation-states and threat actors. From its modest beginnings as a capability available only to the United States and the Union of Soviet Socialist Republics, eighteen countries were marketing some

forty-two types of battlefield surveillance radar for export by 2010.[14] Even non-peer state actors can purchase systems that achieve parity with US capabilities. Though figures from most sales are unavailable, U.S. and Dutch sales of battlefield surveillance radar show prices offered to allies between $300,000 and $500,000 per radar unit for older models.[15]

Platforms

In addition to sensor payloads, reconnaissance and surveillance platforms have increased in quantity and capability. Generally, they can be categorized along the domains of war in which they operate: air, sea, land, space, and cyberspace. The development of capabilities allows threat actors to act across domains in their reconnaissance efforts. The US was pioneering use of space reconnaissance satellites for tactical operations in support of Operation Desert Storm.[16] Today, many nations are space reconnaissance capable with Iran joining the club, having placed its fourth reconnaissance satellite into orbit in 2015.[17] Others can use commercially available imagery to supplant a dearth of space-based reconnaissance assets. An operational example can be seen in the public identification of an undisclosed US air base in the Jordanian desert. Using publicly available information including satellite imagery, logistic contracts, and public affairs statements, a non-state research team identified the base and its likely complement of air assets.[18] This low-end capability hardly existed two decades ago but holds tremendous promise as a platform for information collection today. As with sensor payloads, an exhaustive survey of all types of sensor platforms would exceed the scope of this study. Instead, a survey of developments in unmanned aerial systems (UAS) will serve to demonstrate the changes in sensor platforms. Unlike the case of battlefield surveillance radar in relation to the larger class of sensors, UAS development cannot be claimed as representative of all platforms. In comparison to cyber, UAS development has been mild, while in comparison with most ground platforms,

UAS development has been explosive. As such, the case of UAS falls about the median of cases regarding reconnaissance platform development.

As with battlefield surveillance radars, the US led experimentation with UAS, employing them for strategic reconnaissance missions with a variety of different sensor payloads during the Vietnam era.[19] However, it was Operation Desert Storm during which the US demonstrated the utility of UAS in support of tactical operations. UAS reconnaissance platforms so bedeviled Iraqi ground units that Iraqi soldiers surrendered on sight of the UAS rather than undergo the probable bombardment that would follow in one instance.[20] The RQ-2 Pioneer, the most common UAS employed for tactical reconnaissance at the time, could carry a variety of sensor payloads for five to six hours out to a radius of 100 nautical miles.[21] Additionally, the US was almost alone in the ability to employ UAS as a reconnaissance platform.

UAS platforms have matured considerably. The MQ-9 Reaper, a common US reconnaissance UAS capable of carrying armaments, has an endurance of twenty-nine hours and a radius of 4,000 nautical miles.[22] Capabilities previously held at the corps level, have been spread down the command structure. The Brigade Combat Team retains a platoon of RQ-7 Shadow UAS, roughly a RQ-2 Pioneer equivalent.[23] Adversary UAS development has increased dramatically. A 2015 RAND study of Chinese UAS development identified UASs in various stages of development and deployment from tactical to large, long-range reconnaissance systems.[24] China's UAS capability has reached a point of development allowing it to compete with the United States in the export market. For example, China has reached export agreements with several nations for its Pterodactyl-1 UAS, an equivalent to the Predator.[25] As our enemies in Iraq and Afghanistan have experienced, UAS development made protecting information more

difficult. The endurance and variety of payloads available to UAS erodes passive ability and require extensive active efforts to support offensive operations.

On the smaller end, UAS have become more capable. The non-state actor ISIS has most recently demonstrated this capability. During the operation to retake Mosul, Operation Eagle Strike, ISIS adapted small commercial-off-the-shelf UAS to act as reconnaissance and close air support platforms. ISIS managed over 300 sorties against coalition forces during one month of the Mosul operation with limited friendly success in defeating the reconnaissance effort.[26] Traditional active measures had difficulty defeating the small UAS.

As with battlefield surveillance radars UAS ability has diffused to other states and threat actors. A 2014 Rand study concluded over fifty countries managed UAS development programs while over seventy countries had acquired UAS.[27] In 2014, Russia alone activated fourteen companies of UAS, pairing them with mechanized brigades.[28] One assessment concluded that China funded research and development across seventy-five public-private companies developing UAS technologies.[29] Adversaries across the range of capability can be expected to effectively employ UAS as reconnaissance platforms.

Networks

Additionally, the explosive growth of effective communications has further complicated the information protection efforts. Networks can be thought of as interacting layers categorized as human, analog, and digital. Human networks represent the social quality of humans interacting directly with one another through verbal and non-verbal language. Next, analog networks include physical manipulations that convey information. Personal letters physically written between individuals represent a very simple analog network as information is translated from thought to letters through the physical medium of writing on paper. Manipulations of the

electromagnetic spectrum represent the high end of analog information network development. While analog networks remain important and voluminous in the world, changes to digital networks have catalyzed an adversary's ability to pass critical information rapidly. Digital networks employ non-physical manipulations to convey information. For example, computer hardware does not need to be changed to execute different sets of non-physically coded instructions. Digital networks enable fast and high-volume communications. Further, the low cost and integration of digital networks and devices into daily life and across the world has enabled their omnipresence. In addition to permitting increased reconnaissance as a platform in the cyber domain, "the speed, volume, and ubiquity" of digital networks enable reconnaissance assets to operate further from the traditional battlefield and to exist in areas not previously tapped for reconnaissance. [30]

The ability of a sensor or platform to collect critical information from a relatively great distance from the battlefield has been mitigated traditionally by the difficulty with which the collector must struggle to communicate the discovery to another element that can use the information to advantage. The pervasiveness of digital networks has eroded that mitigative characteristic. The US drove development and leads the world in the ability to pass large volume communications to and from tactical echelons, primarily through satellites employing a mix of analog and digital signal techniques.[31] As adversaries attempt to copy this high-end ability, the lower end of digital network power has opened for all to employ. In 2015, a US operation in Libya was revealed and pictures distributed worldwide minutes after contact by an individual with a camera phone and an internet connection.[32] With military operations likely to occur in and around populations, that occurrence is likely to increase. The volume of information that can be shared by non-combatants is alarming. A 2017 RAND study noted that Twitter followers

posted 500 million tweets every day.[33] In an interesting case, Libyan rebels executing an assault on a Libyan government artillery position retrieved technical information from refugees in Finland and England via a Skype conference call.[34] Speed, volume, and ubiquity of networks then, becomes a serious challenge to information protection efforts as traditionally non-military capabilities can be leveraged to reveal and distribute critical information.

Adaptation to the Current Information Collection Environment

The current information collection environment seriously challenges the ability of US land forces to protect critical information. In response, the Army must favor active counterreconnaissance, even at the expense of some passive measures. Concurrently, the Army must organize to maximize counterreconnaissance tempo. Both adaptations represent necessary symmetrical responses to improved adversary information collection. Additionally, however, the Army must respond asymmetrically, decentralizing and employing deception to increase situational ambiguity.

Favor Active Counterreconnaissance

In adapting to the current information collection environment, the Army should prioritize active measures above more familiar passive measures. However, the Army tends to think and act in terms of improving passive measures. General Mark Milley, the Army's Chief of Staff, concluded soldier's must, "employ every known technique of cover and concealment" to prevent being detected and killed in future conflicts.[35] The Army's focus on passive measures can be seen in adaptations already underway. Recently, 3rd Brigade Combat Team, 4th Infantry Division painted their tanks woodland green to better blend with the natural foliage during their deployment in eastern Europe.[36] Army units have also experimented heavily with managing electronic signatures. As one Army officer recently noted, understanding principles of antenna

theory, use of terrain masking, use of low power settings on radios, and understanding of radio procedures could yield significant improvement in information protection efforts.[37] All these recommendations are effective but passive measures.

Beyond these low hanging fruits, however, passive measures struggle in denying the robust reconnaissance systems of today. First, the increase in sensor capability challenge passive measures ability to retain concealment. For example, camouflage netting is a robust and common US passive capability. The Lightweight Camouflage Screen System (LCSS) breaks up visual signatures, reduces infrared signatures, and scatters radar returns when employed properly.[38] Doing so addresses four of the sensor categories defined above: visual, infrared, radar, and some multispectral. This is a robust passive capability. Alas, it counts for less in the current environment.

Multispectral sensors that can tease out subtle differences in the electromagnetic spectrum have become standard on the battlefield. Hyperspectral sensors that are capable of differentiating types of materiel are becoming available. China has deployed several hyperspectral sensors on satellites to overcome camouflage measures over the past decade.[39] Camouflage netting struggles to match the variety of urban and suburban environments, subtleties in changing vegetation, and loses much of its ability when movement is required.

Likewise, Chemical Agent Resistant Coating (CARC) paint provides a mobile passive capability. CARC limits visual, near-infrared, and infrared signatures of friendly vehicles and equipment.[40] Again, this represents an important multispectral capability, but other signatures of moving and operating equipment abound. Vehicles and generators create noise, show up on battlefield surveillance radar more easily, and leave imprints in the ground visible to aerial or satellite reconnaissance. This has always been so, but the ability of reconnaissance sensors to

detect this activity, with greater accuracy, and from greater distance has increased the likelihood of detection.

Further, passive adaptations struggle with the persistence of adversary information collection capabilities, which enables their intelligence personnel to closely refine analysis to the particulars of an environment. As seen in the example of the airbase in Jordan, a high intelligence skillset is not required when reconnaissance assets are able to persistently collect information in an area of interest. Eventually, the application of various reconnaissance sensors and platforms will overcome the narrow band of protection provided passively. Through the cyber reconnaissance platform, US Department of Defense information systems are scanned millions of times each day for vulnerabilities.[41] The asymmetry across cyber platforms is so unfavorable, the concept of security through obscurity, or hiding online has long been abandoned. In another example, the Iraqi Army attempted to address the dilemma presented by US Army multispectral sensors during Operation Iraqi Freedom by digging in and camouflaging their vehicles. This action reduced their infrared signature and allowed for application of visual camouflage.[42] The measure effectively fixed the Iraqis in place and still failed to work. Despite these passive measures, the dug-in forces were identified by persistent coalition aerial and ground reconnaissance and subsequently destroyed.[43]

Additionally, passive measures create a counter-intuitive effect on friendly forces. Because of the narrowness of passive measures, Army forces tend to layer them to create a greater overall protection effect but in a manner which interferes with the Army's preferred operating method. *FM 3-0 Operations* notes that Army forces conduct successful land operations when they, "seize, retain, and exploit the initiative by forcing an enemy to respond to friendly action."[44] To achieve this, Army commanders prefer high tempo operations that force

an adversary to react continuously from positions of disadvantage. Passive measures may cause the adversary to work harder to gain critical information, but also have a braking effect on friendly tempo. Passive measures do this by inhibiting the flow of friendly information as friendly forces take precautions to ensure the signature emitted does not give away critical information. For example, adjusting to burst radio transmissions from continuous transmissions, passively limits friendly radio traffic by consolidating all reporting and direction into short 'burst' windows. The technique frustrates signal intelligence gathering and reduces radio signatures. However, this passive measure limits information to and from command elements, slowing the tempo of operations.

Active measures face challenges too, but their effectiveness is less diminished by the development of reconnaissance systems. The primary challenge to active counterreconnaissance comes from requiring the use of rarer assets to be effective. As sensors and platforms move further from the battlefield, the ability to affect those systems is transferred from short range, common assets to long range, less common assets. For example, if the Chinese PL-02 battlefield surveillance radar is capable of an eighty-kilometer detection range, the counterreconnaissance agent shifts to long-range rocket, aviation, or cyber fires. The cold war era systems all fell well within tube artillery range. The responsibility for conducting the active measure shifts to higher echelons, but the effectiveness of the active method remains comparable.

Active measures have proved more effective in the current information collection environment. In invading Ukraine, Russian and proxy forces liberally employed electronic warfare and air defense to deny Ukrainian aerial platforms and disrupt radio reports. In so doing, the Russian and proxy forces acknowledged their inability to hide their forces passively and embraced the blinding effects gained from active measures. Similarly, the Israelis are suspected

of using cyber and electronic warfare assets successfully to disable Syrian air defenses during a raid to destroy alleged Syrian nuclear facilities.[45] Focusing on blinding Syrian radar reconnaissance assets, the Israelis acknowledged their inability to hide aerial platforms passively and employed the more effective active measures.

Beyond the generic application, active measures permit friendly forces to target vulnerabilities in an adversary's reconnaissance system, thus preventing collected information from reaching the end user without having to defeat the entire reconnaissance system. A friendly force need not smash every sensor, defeat every platform, or interrupt all networks if it can interdict a vulnerability in the interaction of all three. Not all elements of the reconnaissance system are equally robust. For example, most UAS models require active control from ground stations or via a data link.[46] This link may be attacked through electronic warfare, cyber, or direct means in an attempt to sever control of the UAS. Without the control, the UAS platform and sensor are denied the ability to collect critical information. In situations where the platform is hard to counter, the sensor may not be able to withstand direct effects. For example, China has been developing lasers since the early 2000s that blind friendly satellite optics without trying to blast the satellite out of orbit.[47] In the digital realm, the denial of service attack remains an effective tool at slowing or halting network communications with millions of short, efficient attacks occurring monthly.[48] If, joint and Army active air defense have difficulty, tracking and engaging small UAS, attacking the sensor or network is still a viable option.[49] The option to target a vulnerability in the adversary reconnaissance system comes as an advantage of active measures.

Further, active measures better address capability shortfalls of organization and equipping. As humans with access to digital networks crowd the battlespace, the difficulty in

protecting information passively increases. The US forces exposed by a camera phone and social media account in Libya had no means passively counter the exposure of their critical information. Active tactical cyber could have identified and possibly interdicted the dissemination of the collected information. The Army is working the issue programmatically but does not have solutions ready. In February 2018, the Army was training tactical cyber-electromagnetic activity teams at the National Training Center.[50] Called Expeditionary Cyber Teams, the cyber counterreconnaissance agents should be able to provide awareness and reach back for cyber capabilities to the tactical commander. In the meantime, units should move to become more active on their own. 1st Brigade Combat Team, 4th Infantry Division conducted an experiment by creating a small cyber cell from soldiers assigned to the unit. Across an 18-month period, the cell mined open source information on opposing force actors under simulation conditions. Using the rudimentary techniques of trolling and geolocation features resident in many software applications, the cell improved the brigade's reconnaissance efforts influencing a key maneuver decision and a counter-fire mission.[51] Though these measures were reconnaissance focused, application of active cyber measures in a counterreconnaissance role could provide a similar advantage in the fight to protect information. The Army will have to reflect this preference for active measures more generally to compete with the growth of reconnaissance systems.

Maximize Counterreconnaissance Tempo

The increased range, capability, and communication capacity of adversary reconnaissance systems do not present a dilemma to the Army in itself. Counterreconnaissance systems with comparable capabilities exist across echelons and through the joint force. For example, the PL-02 battlefield surveillance radar's eighty-kilometer range is still within that of

Army rocket artillery or joint fires. However, the changes to adversary reconnaissance ability do present a tempo dilemma for counterreconnaissance. Tactical information can be collected far from the battlefield, but protective measures capable of denying them may only exist at higher echelons. The PL-02 may concern the brigade combat team, but the brigade combat team is unlikely to have the fires or joint assets necessary to address the PL-02. The time taken to receive and employ the countering asset, whether Army rocket or joint fires, is much slower than that taken by the reconnaissance system to collect and disseminate friendly information. In the current environment, a tactical commander will require higher assets to counter adversary reconnaissance. LTG Gary Volesky, then Combined Joint Land Force Component Commander for Operation Inherent Resolve noted, "it was common practice in 2016 for action at the lowest tactical level to be directly supported by nationally and coalition sourced multi-domain capabilities (e.g., ISR, information operations [IO], cyber, electronic warfare [EW], military deception and others)".[52] The difference in tempo between reconnaissance collection and counterreconnaissance action compounds the challenge.

Additionally, counterreconnaissance systems begin with a tempo deficit. These systems consist of sensors, platforms, networks, command and control elements, and counterreconnaissance agents. A simple system could consist of a scout (platform) observing an enemy scout using binoculars (sensor) communicating through a radio (network) to a platoon leader (command and control) who directs a sniper (counterreconnaissance agent) to kill the enemy scout. Fortunately, the same technological factors that have driven the development of sensors, platforms, and networks for reconnaissance also help improve counterreconnaissance. Improvements to systems help detect adversaries at increased ranges and pass that information rapidly. Unfortunately, systems are rarely as simple as the example provided. The intervening

echelons of command and responsibility slow the ability of lower level commanders to employ assets. Thus, the counterreconnaissance tempo deficit is positively modified by technological changes but slowed by organizational factors.

Because protecting information is naturally and organizationally slower than reconnaissance systems, the Army should focus on maximizing the counterreconnaissance tempo. The rate at which information denial efforts can respond and deny adversary reconnaissance operations, more than demonstrating a bias for active measures, will determine how successful the Army is at protecting critical information. Symmetrically countering the improvements in sensors, platforms, and networks provides an opportunity for protective efforts to compete with, if not upend, the reconnaissance advantage. The Army must align authority to act, information, and the capability for counterreconnaissance systems to achieve a tempo advantage in relation to reconnaissance systems. Improving tempo will require reorganization. Army units at the division level and above should adapt two methods for increasing counterreconnaissance tempo: delegating and integrating.

Delegating capability and authority is the simpler and more effective technique to increase tempo. The idea of task-organization is a staple and common adaption to address various adversary capabilities. For example, task-organizing short-range air defense capabilities with tactical maneuver units increases tempo against small and medium aerial reconnaissance platforms. The information, authority, and capability exist at a common, low level permitting the protective activity to occur at the same or quicker tempo than the reconnaissance activity. Recently, the Russian battalion tactical group has proven effective at increasing the tempo of operations in the Ukraine by delegating previously centralized authority and capability to the relatively low control of a battalion commander.[53] By doing so, the Russian battalion tactical

groups have been able to rapidly exploit battlefield reconnaissance. The strike at Zelenopillya represents one such case. Delegating increases counterreconnaissance tempo to match the tempo of reconnaissance operations by aligning authority, ability, and information at the same level.

Integration is more difficult to achieve but allows greater control with a nominal loss of tempo. As opposed to delegation, integrated organizations may hold information, authority, and capability at different echelons, but optimize processes across echelons to achieve tempo enhancements. A good example comes from Operation Inherent Resolve. The Combined Joint Land Force Commander, Lieutenant General Volesky identified that his multinational headquarters would have to employ capabilities across the levels of warfare at the high tempo of ground tactical operations. His headquarters attempted an integrated solution by optimizing various staff functions across numerous echelons using federated trust mechanisms to integrate tactical actions with national assets and authorities.[54] This action increased the tempo of operations to match slow, national level capabilities and authorities with the much more rapid pace of tactical information. Integrating echelons for counterreconnaissance can have a similar boost to tempo but will always be slower than organizations adopting delegation.

In pursuing maximal tempo through delegation and integration, the Army incurs risk of overusing or misusing low provision assets. For example, cyber exploits are considered low provision assets as they are thought to be few in number and have limited utility beyond their initial use. Once the exploit is used, the adversary can study it and develop countermeasures. Additionally, cyber exploits are difficult to build and are expensive. In 2015, only fifty-four of 430 million recorded cyber-attacks involved a zero-day exploit.[55] Using a cyber exploit than, is held at high level of authority, rarely delegated, and poorly integrated. This avoids the risk of using the asset piecemeal for limited effect.

However, military operations sit at the edge of a large change in the character of war. Greater risk lies in tightly retaining control of counterreconnaissance measures for fear of their loss or mis-provision. For cyber alone, massive change is anticipated. The Defense Advanced Research Projects Agency has been working to develop artificial intelligence that detects vulnerabilities and rewrites code at the speed of computers, not humans.[56] One terrain feature further, quantum computing promises to make classical computing irrelevant. The exquisitely developed cyber exploit of today is heading the same direction as the horse cavalry. The risk then, is not in using the asset, but in sitting on it until it becomes irrelevant.

Decentralize and Lean on Deception

Finally, favoring active measures and increasing tempo cannot fully counter the ascendency of reconnaissance systems. Reconnaissance has a mass and price advantage. Though this is hardly a uniform prospect, reconnaissance systems are more numerous and cheaper than the information protection systems employed against them. The continued development of small UAS is one such instance. In the fight for Mosul, ISIS employed numerous small UAS at an estimated cost of $650 per unit.[57] Meanwhile, the Army's standard short-range air defense missile costs about $38,000 per unit.[58] While the Stinger may not be the ideal choice to counter small UAS, it is the counterreconnaissance tool available. Recently, the Russians claim to have used anti-aircraft missiles to defeat a swarm small UAS attack on one of their airbases in Syria.[59] As a solution, this is suboptimal and perhaps self-defeating to deploy relatively few $38,000 missiles against relatively many $650 small UAS. More importantly, even if active measures and high tempo can be achieved, reconnaissance systems will still retain a mass advantage over counterreconnaissance measures employed against them.

To accompany the symmetric responses above, the Army should lean on military deception (MILDEC) to assist symmetrical counterreconnaissance in protecting critical friendly information. A primary function of MILDEC is to assist information protection efforts. Deception in support of operations security (DISO), "conveys or denies selected information or signatures to a foreign intelligence entity (FIE) and limits the FIE's overall ability to collect or accurately analyze critical information about friendly operations, personnel, programs, equipment, and other assets." Famously, Operation Bodyguard, the Allied deception plan surrounding the Normandy invasion, successfully influenced Nazi perceptions causing the focusing of reconnaissance assets against the false invasion force. Thus, German reconnaissance and surveillance was denied through manipulation and ambiguity brought on by MILDEC activities. If reconnaissance cannot be denied through the symmetric application of counterreconnaissance in the current information collection environment, MILDEC can help the adversary deny his own effort through misapplication of the reconnaissance effort.

However, the ability of the Army to pull off a grand deception similar to Operation Bodyguard is challenged by the same growth of information collection capability that challenges information protection generally. The Marine Corps Operating Concept has noted that current friendly social media discipline and routine operating procedures undermine U.S. ability to shift adversary perceptions through deception.[60] The administrative, logistic, personal, and military signatures emanating in the buildup to a major operation would be nearly impossible to conceal. Using the Operation Bodyguard example, General Patton's fake army signature was sufficiently "loud" to crowd out counter-indicators gained from the real Allied force massing in south west England. Current reconnaissance systems are sufficiently robust to pick up the "noise" from the

real invasion force and provide to the enemy commander a more complete picture of what is really happening.

Instead of focusing on misleading the enemy to protect critical information, the Army should focus on the less decisive effect produced by MILDEC: ambiguity. Ambiguity does not rely on a single narrative that plays into an adversary's preconceptions leading to his selection of an incorrect course of action. Rather, using MILDEC for ambiguity locks the adversary into a period of uncertainty. The ambiguity type of MILDEC seeks to create a temporary cognitive advantage through confusion and distraction.[61] Egypt did this at a strategic level leading into the 1973 war with Israel by announcing the illness and exhaustion of President Sadat following an international conference. The act did not mislead Israeli leadership as to Egypt's intent but increased uncertainty and fed into Israel's fear of crying wolf over a false invasion threat .[62] At a lower tactical level the Army already employs MILDEC for ambiguity in the use of dummy fighting positions, phony military vehicles, and employment of false minefields.

If a misleading deception is possible, then information protection efforts can deny enemy collection efforts in the vein of Operation Bodyguard. However, as is more likely the case, if the best MILDEC can offer is ambiguity, adversary information collection efforts can still be denied in the aggregate. MILDEC depends on operations security (OPSEC) to help create cognitive effects.[63] When both components are present and effective, a rolling cognitive advantage is created. OPSEC permits MILDEC to position assets for employment, which deceives adversary reconnaissance, which assists further OPSEC, which assists further MILDEC. For example, Hezbollah effectively used dummy bunkers positions to draw Israeli reconnaissance focus leading up to the 2006 conflict between the parties. Effectively building a modern "Quaker Gun", the Hezbollah forces applied a simple deception scheme in the face of Israel's

overwhelming conventional reconnaissance dominance.[64] Israeli forces lost momentum after falling for the deception in initial tactical engagements. The ambiguity created by the dummy positions was insufficient to mislead Israel completely but did buy time and space for information protection efforts to be effective.

In maximizing the power of creating ambiguity through MILDEC, the Army must decentralize authority for execution. *FM 3-0 Operations* notes tactical deception activities work best when planned top down and should be executed by those echelons with significant resources available to assign a deceptive effort.[65] The manual designates the Corps as the most appropriate echelon for executing tactical deception activities and relegates lesser units to employing OPSEC measures including use of camouflage, concealment, and decoys. This is an accurate proposition if a grand misleading deception is necessary. Unsynchronized deception efforts can provide counter-indicators that awaken the adversary to the deception effort. However, if ambiguity is the goal, counter-indicators may be harmless or even desirable. To create the rolling protective effect desired, poorly synchronized, or unsynchronized efforts can create sufficient ambiguity to initiate the desired MILDEC-OPSEC reinforcing effect described in the paragraph above. The unsynchronized activities of Russian Internet trolls provide a non-military example. Russia pays some of its citizens to interact online with U.S. and other foreign citizens and agencies with the overall objective of increasing uncertainty within those nations.[66] However, it does not always try to synchronize the messaging of the multitude of real and fake online personas. Attempting to do so would slow the tempo of response and make it easier for foreign governments to clarify the purpose and method of Russian influence campaigns. The volume of "noise" created by the Russian Internet trolls, even when misaligned, is sufficient to create the necessary ambiguity. Just as friction develops inevitably from the levels of command

through which information must pass, so to can ambiguity be created by permitting a freer hand to all echelons to undertake deception in support of information protection.

Conclusion

The Army faces a steep challenge adapting to deny adversary information collection efforts given the capability of reconnaissance systems across sensors, platforms, and networks. Reconnaissance system advantage in range, accuracy, and dissemination speed require symmetric and asymmetric responses. In this competition between reconnaissance and counterreconnaissance, active measures will prove more useful than the passive measures that have borne fruit in the past. Additionally, the Army must organize to increase counterreconnaissance tempo to match that of reconnaissance systems. Aligning authority, capability, and information through delegation and integration can improve counterreconnaissance tempo to compete with the improved reconnaissance tempo. Still, military deception will be required to provide an asymmetric advantage for traditionally symmetric counterreconnaissance. Achieving ambiguity through MILDEC requires letting go of the tight control necessary for grand misleading deceptions. Overall, employing the framework will allow the Army to compete until long term technological, procedural, and organizational changes can be developed that restore U.S. counterreconnaissance parity or advantage.

[1] Roger Ames, *Sun-Tzu: The Art of Warfare* (New York: Random House, 1993), 62.
[2] Shawn Woodford, "The Russian Artillery Strike That Spooked The U.S. Army," *The Dupuy Institute* (blog), March 29, 2017, http://www.dupuyinstitute.org/blog/2017/03/29/the-russian-artillery-strike-that-spooked-the-u-s-army/
[3] Amos Fox, "Hybrid Warfare: the 21st Century Russian Way of Warfare," (master's thesis, U.S. Army Command and Staff College, 2017), 38, http://www.dtic.mil/dtic
[4] Headquarters, Department of the Army, *The Army Operating Concept: Win in a Complex World, 2020-2040*, TRADOC Pamphlet 525-3-1, Change 1, (Washington, DC: Headquarters Department of the Army, October 31, 2014), 34.
[5] Headquarters, Department of the Army, *Operations*, FM 3-0, Change 1, (Washington, DC: Headquarters Department of the Army, December 6, 2017), Foreward.
[6] Headquarters, Department of the Army, *Offense and Defense, Volume 1*, FM 3-90-1, Change 2(Washington, DC: Headquarters Department of the Army, April 13, 2015), B-5.
[7] Headquarters, Department of the Army, *Camouflage, Concealment, and Decoys*, ATTP 3-34.39, (Washington, DC: Headquarters Department of the Army, November 26, 2010), 2-2.
[8] Ibid, 2-4.
[9] Fred Bunn, *Early Warning and the Tank* (Aberdeen Proving Ground, MD: US Army Ballistic Research Laboratory, 1989), 19.
[10] Ibid, 19
[11] *Jane's*, "Details of upgraded SNAR-10 battlefield surveillance system emerge," August 10, 2015, https://janes-ihs-com.lomc.idm.oclc.org/Janes/Display/idr17885-idr-2015
[12] *Jane's*, "Iran markets battlefield radars," December 12, 2006, https://janes-ihs-com.lomc.idm.oclc.org/Janes/Display/jdw31276-jdw-2006
[13] Christopher Foss, "Precision Attack: China Aims for Greater Accuracy," *IHS Jane's International Defense Review* 48, no. 4 (April 2015).
[14] Defense Market Intelligence, "Battlefield Surveillance Radars, Global Sales Mapping," *Defense Market Intelligence*, accessed January 16, 2018, http://dmilt.com/docs/BSR.pdf
[15] Ibid, 5.
[16] Robert Butterworth, "Space and the Joint Fight," *INSS Strategic Forum*, (February 2012): 4.
[17] Stephen Clark, "Iranian Satellite Successfully Placed into Orbit," *Spaceflight Now*, February 2, 2015, https://spaceflightnow.com/2015/02/02/iranian-satellite-successfully-placed-in-orbit/
[18] George Kaplan, "We've Spotted a Secret American Drone Base in Jordan," *War is Boring*, July 3, 2017, https://warisboring.com/weve-spotted-a-secret-american-drone-base-in-jordan/
[19] John Blom, *Unmanned Aerial Systems: A Historical Perspective* (Fort Leavenworth, KS: Combat Studies Institute Press, 2010), 57.
[20] Ibid, 89.
[21] *Jane's*, "AAI/IAI RQ-2 Pioneer" February 5, 2010, https://janes-ihs-com.lomc.idm.oclc.org/Janes/Display/juav0725-juav
[22] *Jane's,* "GA-ASI Predator B/ MQ-9 Reaper/ MQ-9B," November 21, 2017, https://janes-ihs-com.lomc.idm.oclc.org/Janes/Display/juav9266-juav
[23] Headquarters, Department of the Army, *Brigade Combat Team,* FM 3-96, (Washington, DC: Headquarters Department of the Army, October 8, 2015), 1-24.
[24] Michael Chase, Kristen Gunness, Lyle Morris, Samuel Berkowitz, and Benjamin Purser III, *Emerging Trends in China's Development of Unmanned Systems*, RAND, 2015, https://www.rand.org/pubs/research_reports/RR990.html
[25] *Jane's*, "AVIC Wing Loong Series," January 9, 2018, https://janes-ihs-com.lomc.idm.oclc.org/Janes/Display/juava409-juav
[26] Mark Pomerleau, "How $650 drones are creating problems in Iraq and Syria," *C4ISRNET*, January 5, 2018, https://www.c4isrnet.com/unmanned/uas/2018/01/05/how-650-drones-are-creating-problems-in-iraq-and-syria/
[27] Lynn E. Davis, Michael J. McNerney, James Chow, Thomas Hamilton, Sarah Harting, and Daniel Byman, *Armed and Dangerous: UAVs and U.S. Security*, RAND, 2014, https://www.rand.org/pubs/research_reports/RR449.html
[28] Lester Grau and Charles Bartles, *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces* (Fort Leavenworth: Foreign Military Studies Office, 2016), 297.

[29] Adam Rawnsley, "Meet China's Killer Drones" *Foreign Policy* (January 14, 216), http://foreignpolicy.com/2096 16/01/14/meet-chinas-killer-drones/
[30] Michael Williams, "Speed, Volume, and Ubiquity," *RealClear Defense*, July 26, 2017, https://www.realcleardefense.com/articles/2017/07/26/speed_volume_and_ubiquity_111901.html
[31] Mak King and Michael Riccio, "Military Satellite Communications: Then and Now," *Aerospace*, April 1, 2010, www.aerospace.org/crosslinkmag/spring-2010/military-satellite-communications-then-and-now/
[32] Chris Stephen, "Secret US Mission in Libya Revealed after Air Force Posted Pictures," *The Guardian*, December 17, 2015, https://www.theguardian.com/us-news/2015/dec/17/secret-us-mission-in-libya-revealed-after-air-force-posted-pictures
[33] William Marcellino, Meagan L. Smith, Christopher Paul, and Lauren Skrabala, *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysts in Support of Information Operations*, RAND, 2017, https://www.rand.org/pubs/research_reports/RR1742.html
[34] John Pollock, "People Power 2.0" *MIT Technology Review,* April 20, 2012, https://www.technologyreview.com/s/427640/people-power-20/
[35] C. Todd Lopez, "Milley: Army on cusp of profound, fundamental change," October 6,2016, https://www.army.mil/article/176231/milley_army_on_cusp_of_profound_fundamental_change
[36] Christopher Woody, "US Tanks are Getting a Small Update That Signals a Big Shift to Defending Europe Against Russia," www.businessinsider.com/us-tanks-in-europe-painted-with-green-paint-for-camouflage-2017-4
[37] Joshua Christian, "Mastering the Fundamentals of Passive Counterreconnaissance to Survive against a Hybrid Threat," *Armor*, 2016, www.benning.army.mil/armor/eARMOR/content/issues/2016/JUL_SEP/3Christian16.pdf
[38] Headquarters, Department of the Army, *Camouflage, Concealment, and Decoys*, ATTP 3-34.39, (Washington, DC: Headquarters Department of the Army, November 26, 2010), C-1.
[39] Jeffrey Lin and P.W. Singer, "China To Launch Powerful Civilian Hyperspectral Satellite," *Popular Science*, January 25, 2016, https://www.popsci.com/china-to-launch-worlds-most-powerful-hyperspectral-satellite#page-3
[40] John Mort, "Modern CARCs for Military Protection," *Paint & Coating Industry Magazine*, October 1, 2007, https://www.pcimag.com/articles/95385-modern-carcs-for-military-protection
[41] Sean Lawson, "Just How Big Is The Cyber Threat To The Department Of Defense?," *Forbes*, June 4, 2010, https://www.forbes.com/sites/firewall/2010/06/04/just-how-big-is-the-cyber-threat-to-dod/#5f2de45746b3
[42] Michael Gordon and Bernard Trainor, *Cobra II: The Inside Story of the Invasion and Occupation of Iraq* (New York: Random House, 2006), 137.
[43] Ibid, 483.
[44] Headquarters, Department of the Army, *Operations*, FM 3-0, Change 1, (Washington, DC: Headquarters Department of the Army, December 6, 2017), 1-17.
[45] Shane Quinlan, "Jam. Bomb. Hack? New U.S. Cyber Capabilities and the Suppression of Enemy Air Defenses," *Georgetown Security Studies Review*, April 7, 2014, http://georgetownsecuritystudiesreview.org/2014/04/07/jam-bomb-hack-new-u-s-cyber-capabilities-and-the-suppression-of-enemy-air-defenses/
[46] Jason Yochim, "The Vulnerabilities of Unmanned Aircraft System Common Data Links to Electronic Attack," (master's thesis, U.S. Army Command and Staff College, 2017), http://www.dtic.mil/dtic
[47] Francis Harris, "Beijing secretly fires lasers to disable US satellites," *The Telegraph*, September 26, 2006, www.telegraph.co.uk/news/worldnews/1529864/Beijing-secretly-fires-lasers-to-disable-US-satellites.html
[48] Symantec, *Internet Security Threat Report Volume 21*, April 2016, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf , 67.
[49] Headquarters, Department of the Army, *Counter-Unmanned Aircraft System Techniques*, ATP 3-01.81, (Washington, DC: Headquarters Department of the Army, April 13, 2017), 1-1.
[50] Steven Stover, "Army Developing Expeditionary Cyber-electromagnetic Teams to Support Tactical Commanders," February 7, 2018, https://www.army.mil/article/200262/army_developing_expeditionary_cyber_electromagnetic_teams_to_support_tactical_commanders
[51] Curt Taylor and Joe Byerly, "Fighting for Information in a Complex World: Lessons from the Army's first Reconnaissance and Security Brigade Combat Team" 18 September 2017, Pg. 16
[52] Gary Volesky and Roger Noble, "Theater Land Operations: Relevant Observations and Lessons from the combined Joint Land Force Experience in Iraq," www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2017-Online-Exclusive-Articles/Theater-Land-Operations/
[53] Lester Grau and Chuck Bartles, "Integration of unmanned aerial systems within Russian artillery," *Fires*, May 2016, http://sill-www.army.mil/firesbulletin/, 34.

[54] Gary Volesky and Roger Noble, "Theater Land Operations: Relevant Observations and Lessons from the combined Joint Land Force Experience in Iraq," www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2017-Online-Exclusive-Articles/Theater-Land-Operations/
[55] Symantec, *Internet Security Threat Report Volume 21*, April 2016, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf ,5.
[56] https://www.darpa.mil/program/cyber-grand-challenge
[57] Mark Pomerleau, "How $650 drones are creating problems in Iraq and Syria," *C4ISRNET*, January 5, 2018, https://www.c4isrnet.com/unmanned/uas/2018/01/05/how-650-drones-are-creating-problems-in-iraq-and-syria/
[58] Franz-Stephan Gady, "India to Buy 245 US Stinger Air-to-Air Missiles," *The Diplomat*, April 1, 2016, https://thediplomat.com/2016/04/india-to-buy-245-us-stinger-air-to-air-missiles/
[59] Raf Sanchez, "Russia Uses Missiles and Cyber Warfare to Fight Off 'Swarm of Drones' Attacking Military Bases in Syria," *The Telegraph*, January 9, 2018, http://www.telegraph.co.uk/news/2018/01/09/russia-fought-swarm-drones-attacking-military-bases-syria/
[60] Headquarters, United States Marine Corps, *The Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*, (Washington, DC: Headquarters United States Marine Corps, September 2016), 6.
[61] Joseph Caddell, *Deception 101 – Primer on Deception* (Carlyle, PA: Strategic Studies Institute, 2004), 6.
[62] George Gawrych, *The 1973 Arab-Israeli War: The Albatross of Decisive Victory* (Leavenworth KS: Combat Studies Institute, 1996), 24.
[63] Headquarters, Department of Defense *Military Deception*, JP 3-13.4, (Washington, DC: Headquarters Department of Defense, February 14, 2017), II-3.
[64] David Acosta, "The Makara of Hizballah: Deception in the 2006Summer War," (master's thesis, Naval Postgraduate School, 2007), http://www.dtic.mil/dtic
[65] Headquarters, Department of the Army, *Operations*, FM 3-0, Change 1, (Washington, DC: Headquarters Department of the Army, December 6, 2017), 2-28.
[66] Krishnadev Calamur, "What is the Internet Research Agency," *The Atlantic*, February 16, 2018, https://www.theatlantic.com/international/archive/2018/02/russia-troll-farm/553616/

Bibliography

Acosta, David. "The Makara of Hizballah: Deception in the 2006 Summer War." Master's thesis, Naval Postgraduate School, 2007. http://www.dtic.mil/dtic

Ames, Roger. *Sun-Tzu: The Art of Warfare*. New York: Random House, 1993.

Blom, John. *Unmanned Aerial Systems: A Historical Perspective*. Fort Leavenworth: Combat Studies Institute Press, 2010.

Bolzak, Jerry. "Blinding the Enemy: Soviet Tactical Reconnaissance in the Rear Area." Master's thesis, U.S. Army Command and Staff College, 1989. http://www.dtic.mil/dtic

Bunn, Fred. *Early Warning and the Tank* (Aberdeen Proving Ground, MD: US Army Ballistic Research Laboratory, 1989), 19. http://www.dtic.mil/dtic

Butterworth, Robert. "Space and the Joint Fight." *INSS Strategic Forum* (February 2012).

Caddell, Joseph. *Deception 101 – Primer on Deception*. Carlyle, PA: Strategic Studies Institute, 2004.

Chase, Michael, Kristen Gunness, Lyle Morris, Samuel Berkowitz and Benjamin Purser III. *Emerging Trends in China's Development of Unmanned Systems*, RAND, 2015, https://www.rand.org/pubs/research_reports/RR990.html

Christian, Joshua. "Mastering the Fundamentals of Passive Counterreconnaissance to Survive against a Hybrid Threat." *Armor* (2016). www.benning.army.mil/armor/eARMOR/content/issues/2016/JUL_SEP/3Christian16.pdf

Davis, Lynn, Michael McNerney, James Chow, Thomas Hamilton, Sarah Harting, and Daniel Byman. *Armed and Dangerous: UAVs and U.S. Security*, RAND, 2014, https://www.rand.org/pubs/research_reports/RR449.html

Foss, Christopher. "Precision Attack: China Aims for Greater Accuracy," *IHS Jane's International Defense Review* 48, no. 4 (April 2015).

Fox, Amos. "Hybrid Warfare: the 21st Century Russian Way of Warfare." Master's thesis, U.S. Army Command and Staff College, 2017. http://www.dtic.mil/dtic

Gawrych, George. *The 1973 Arab-Israeli War: The Albatross of Decisive Victory*. Leavenworth KS: Combat Studies Institute, 1996.

Gordon, Michael and Bernard Trainor. *Cobra II: The Inside Story of the Invasion and Occupation of Iraq*. New York: Random House, 2006.

Grau, Lester and Charles Bartles. “Integration of Unmanned Aerial Systems Within Russian Artillery.” *Fires* (May 2016). http://sill-www.army.mil/firesbulletin/

Grau, Lester and Charles Bartles. *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces*. Fort Leavenworth: Foreign Military Studies Office, 2016.

Headquarters, Department of the Army. *Brigade Combat Team.* FM 3-96. Washington, DC: Headquarters Department of the Army, October 8, 2015.

Headquarters, Department of the Army. *C3CM: Multi-Service Procedures for Command, Control, and Communications Countermeasures*. FM 90-24. Washington, DC: Headquarters Department of the Army, May 17, 1991.

Headquarters, Department of the Army. *Camouflage, Concealment, and Decoys*. ATTP 3-34.39. Washington, DC: Headquarters Department of the Army, November 26, 2010.

Headquarters, Department of the Army. *Commander and Staff Organization and Operations*. FM 6-0, Change 2. Washington, DC: Headquarters Department of the Army, April 22, 2016.

Headquarters, Department of the Army. *Counter-Unmanned Aircraft System Techniques*. ATP 3-01.81. Washington, DC: Headquarters Department of the Army, April 13, 2017.

Headquarters, Department of the Army. *Information Operations*. FM 3-13. Washington, DC: Headquarters Department of the Army, December 6, 2016.

Headquarters, Department of the Army. *Mission Command*. ADRP 6-0, Change 2. Washington, DC: Headquarters Department of the Army, March 28, 2014.

Headquarters, Department of the Army. *Offense and Defense, Volume 1*. FM 3-90-1, Change 2. Washington, DC: Headquarters Department of the Army, April 13, 2015.

Headquarters, Department of the Army. *Operations*. ADRP 3-0. Washington, DC: Headquarters Department of the Army, October 6, 2017.

Headquarters, Department of the Army. *Operations*. FM 3-0, Change 1. Washington, DC: Headquarters Department of the Army, December 6, 2017.

Headquarters, Department of the Army. *The Army Operating Concept: Win in a Complex World, 2020-2040*. TRADOC Pamphlet 525-3-1, Change 1. Washington, DC: Headquarters Department of the Army, October 31, 2014.

Headquarters, Department of Defense. *Military Deception*. JP 3-13.4. Washington, DC: Headquarters Department of Defense, February 14, 2017.

Headquarters, United States Marine Corps. *The Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*. Washington, DC: Headquarters United States Marine Corps, September 2016.

Jane's. "AAI/IAI RQ-2 Pioneer," February 5, 2010. Jane's Information Group. https://janes-ihs-com.lomc.idm.oclc.org/Janes/Display/juav0725-juav

Jane's. "AVIC Wing Loong Series," January 9, 2018. Jane's Information Group. https://janes-ihs-com.lomc.idm.oclc.org/Janes/Display/juava409-juav

Jane's. "Details of upgraded SNAR-10 battlefield surveillance system emerge," August 10, 2015. Jane's Information Group. https://janes-ihs-com.lomc.idm.oclc.org/Janes/Display/idr17885-idr-2015

Jane's. "GA-ASI Predator B/ MQ-9 Reaper/ MQ-9B," November 21, 2017. Jane's Information Group. https://janes-ihs-com.lomc.idm.oclc.org/Janes/Display/juav9266-juav

Jane's. "Iran markets battlefield radars," December 12, 2006. Jane's Information Group. https://janes-ihs-com.lomc.idm.oclc.org/Janes/Display/jdw31276-jdw-2006

Littlebury, F. and D. Praeger. *Invisible Combat: C³CM: A Guide for the Tactical Commander.* Washington D.C.: AFCEA International Press, 1986.

Mission Command Training Program. *FY16 Key Observations*. Center for Army Lessons Learned Bulletin 17-05, February 2017. https://call2.army.mil

Marcellino, William, Meagan Smith, Christopher Paul and Lauren Skrabala. *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysts in Support of Information Operations*, RAND, 2017. https://www.rand.org/pubs/research_reports/RR1742.html

Pollock, John. "People Power 2.0." *MIT Technology Review* April 20, 2012. https://www.technologyreview.com/s/427640/people-power-20/

Rawnsley, Adam. "Meet China's Killer Drones." *Foreign Policy* January 14, 216). http://foreignpolicy.com/2096_16/01/14/meet-chinas-killer-drones/

Symantec. *Internet Security Threat Report, Volume 21*. (April 2016) https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Taylor, Curt and Joe Byerly. "Fighting for Information in a Complex World: Lessons from the Army's first Reconnaissance and Security Brigade Combat Team." White paper, 18 September 2017, 16.

Volesky, Gary and Roger Noble. "Theater Land Operations: Relevant Observations and Lessons from the combined Joint Land Force Experience in Iraq." *Military Review* June 2017.

www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2017-Online-Exclusive-Articles/Theater-Land-Operations/

Yochim, Jason. “The Vulnerabilities of Unmanned Aircraft System Common Data Links to Electronic Attack.” Master’s thesis, U.S. Army Command and Staff College, 2017. http://www.dtic.mil/dtic