REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 28-05-2019	**2. REPORT TYPE** Master's of Operational Studies	**3. DATES COVERED** *(From - To)* JUN 2018 - JUN 2019

4. TITLE AND SUBTITLE Artificial Intelligence (AI) enhanced systems to augment High-Value Target (HVT) location in Counterinsurgency (COIN)	**5a. CONTRACT NUMBER** N/A
	5b. GRANT NUMBER N/A
	5c. PROGRAM ELEMENT NUMBER N/A
6. AUTHOR(S) Al Nahyan, Mohammed, Major, UAE PGSOC	**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 School of Advanced Warfighting Marine Corps University 2044South Street Quantico, VA 22134	**8. PERFORMING ORGANIZATION REPORT NUMBER** N/A
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)** Dr. Benjamin Jensen
	11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The paper analyzes the F3EAD process to ascertain its current effectiveness in a COIN environment to precisely identify HVT for exploitation within the rules of engagement. Additionally, consideration is given to existing AI technology and AI apparatus that is readily obtainable to be adapted to or is currently in military use for incorporation. Furthermore, evaluation of which F3EAD elements will benefit from having AI enhanced systems incorporated into the targeting process, and theoretically will improve upon the current stratagem. In conclusion, the thesis presents the outcome of the research to establish if the incorporation of AI with the F3EAD process shall indeed become a force multiplier in a COIN environment.

15. SUBJECT TERMS
Counterinsurgency(COIN); Artificial Intelligence (AI); High Value Targets (HVT); Targeting; Find, Fix, Finish, Exploit, Analyze and Disseminate (F3EAD).

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** USMC School of Advanced Warfighting
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)*
Unclass	Unclass	Unclass	UU	42	(703) 432-5420 (Admin Office)

United States Marine Corps
School of Advanced Warfighting
Marine Corps University
3070 Moreell Avenue
Marine Corps Combat Development Command
Quantico VA 22134

FUTURE WAR PAPER

Artificial Intelligence (AI) enhanced systems to augment High-Value Target (HVT) location in Counterinsurgency (COIN)

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

Major Mohammed Al Nahyan

AY 2018-19

Mentor: Dr. Benjamin Jensen

Approved: ______________________

Date: 28 MAY 19

Disclaimer

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE SCHOOL OF ADVANCED WARFIGHTING OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT

“Whoever becomes the leader in this sphere (AI) will become the ruler of the world.”
Russian President Vladimir Putin.

1.0. Introduction.

Contemporary military organizations must act faster and with greater precision to outmaneuver their adversaries and avoid inaccuracies within a counterinsurgency (COIN) environment.[1] Moreover, this is a problematical task, founded on the complexities of COIN and the vast majority of insurgents have the advantage of operating within a familiar environment.

Insurgency and COIN are the two faces of an extremely multifaceted variety of warfare in which the violent option is selected to realize the political aspirations of the insurrectionary faction.[2] Adversaries perpetrate an amalgam of threats,[3] such as the employment of conventional weapons, irregular tactics, terrorism, and criminal behavior to simultaneously and adaptively obtain their political objectives.[4]

Counterinsurgents are required to focus on the insurgent network in order to achieve success, but if possible, must do so without inflicting harm on non-combatants. One solution to facilitating promptness and exactitude in targeting insurgent networks, and potentially reducing collateral damage, is examining the potential for employing Artificial Intelligence (AI) enhanced systems to augment High-Value Target (HVT) location in COIN.

In order to assess the theory set out above, the thesis will examine the six distinct steps of the Find, Fix, Finish, Exploit, Analyze, and Disseminate (F3EAD) targeting process, in turn, to establish which part or parts may benefit from having AI as a force multiplier contributing to the outcome. Additionally, in the course of examining the F3EAD process, the thesis will assess which stage in the cycle has the potential to cause the most significant level of collateral damage.

2.0. Counterinsurgency Warfare.

Insurgent networks accomplish their objectives by using subversion, by merging into the populace amid which the security forces operate, and by taking advantage of their most valuable weapon, the exploitation of any counterinsurgent miscalculations, which they can embellish through information operations or the media.[5] Insurgency and counterinsurgency must be considered as war amongst the people. Therefore their political and military aspects cannot be separated as clearly as those of conventional warfare.[6]

Political decisions will influence the planning and conduct of operations, and affect the behavior of the counterinsurgents. Military operations, whether successful or not will have serious political consequences on the political and legal environment. External powers may assist a host nation to focus its resources and capabilities on fighting a counterinsurgency, or they may deploy their forces to fight the insurgency directly. In either case, as examined in *Victory has a Thousand Fathers: Sources of Success in Counterinsurgency*,[7] the employment of certain principles of COIN will be requisite to a successful outcome.

Application of the principles of COIN warfare will mitigate the exploitation of regular forces by the insurgents. The United States of America (USA), the United Kingdom (UK) and the North Atlantic Treaty Organization (NATO) recognize the principles of COIN that the paper will cite. While semantics may vary, the fundamental recognized principles of COIN are, the primacy of political purpose, the unity of effort, understanding the human terrain, securing the population, neutralizing the insurgents, gaining and maintaining popular support, operating in accordance with the law, integrating intelligence, preparing for the long term, and learning and adapting.[8]

These principles must be applied to the accepted methodologies in countering an insurgency, which may be labeled as, Classic, Contemporary, and Insurgent COIN approaches. Classic and Contemporary techniques emphasize winning the support of the local population. Ideally, the government provides physical security, good governance, and economic opportunities, addresses the grievances that led to the insurgency, and thereby wins the population's support. These actions prevent or severely hamper insurgent recruitment among the population, and at the same time deprives the insurgents of their cause.[9]

Insurgent or enemy-centric COIN theory holds that the government's primary focus must be the destruction of the enemy. Once the insurgent forces have been eliminated, economic development and improvements in governance can proceed. In practice, elements of the three approaches are used together. Security must be established by defeating local insurgent forces before people-centric COIN policies can be put into effect. Conversely, even the most relentless enemy-centric COIN campaign will have population-centric elements.[10]

Furthering this strategy, some counterinsurgents, put tactics that seek to kill or capture HVT or the leadership of guerrilla organizations, at the forefront of their COIN efforts. However, some research shows that targeting insurgent leadership may be deemed counterproductive. Contrary to this, leadership targeting significantly increases the mortality rate of insurgent groups. Terrorist organizations are particularly vulnerable to leadership decapitation because of their organizational characteristics, which are brutal, secretive, and idealistic based, and magnify the difficulties of leadership succession.[11]

Classic and Contemporary COIN doctrines emphasize the population-centric aspects of COIN. Effective COIN operations along all the lines of effort are formed by timely, precise, and dependable intelligence, collected and analyzed at the tactical level and disseminated throughout the operational spectrum of the COIN campaign.[12] Due to the dispersed nature of COIN warfare and COIN operations being prime generators of intelligence this is considered necessary. A process develops where operations produce intelligence and that intelligence drives subsequent operations.[13]

Because COIN focuses so much on the population, through political and economic activities as well as conventional military actions, intelligence collection often has more in common with social analysis or anthropology than standard military intelligence. This requires learning new techniques of collecting and analyzing information and mastering new skills to utilize and apply the results in ways that enhance COIN campaigns.[14]

3.0. Targeting the Insurgency.

The contest between insurgents and counterinsurgents is typically a competition between human networks. Traditional relationships have been augmented by modern communications technologies that make networks more complex, faster reacting, and greatly empower those who use such media. Counterinsurgents have to understand how to find and exploit those enemy relationships while building and reinforcing their own.

This can be accomplished by employing the Find, Fix, Finish, Exploit, Analyze and Disseminate (F3EAD) targeting process. F3EAD facilitates a quick targeting process and is applicable for the delivery of both lethal and non-lethal capabilities to create physical and psychological effects.

F3EAD makes possible the targeting not only of individuals in time-sensitive targeting, but furthermore, and possibly of greater importance, the establishment of consequential targets through judicious exploitation and analysis. F3EAD facilitates the interaction between operations and intelligence as it filters the targeting process.[15]

F3EAD is a continuous process in which intelligence and operations nourish and sustain one another. The F3EAD process is configured to support the targeting of critical nodes by helping to analyze all characteristics of the threat network, identify the links between the critical nodes and focus dedicated intelligence collection assets. In turn, the resulting intelligence initiates kinetic strikes against the insurgent critical vulnerabilities, and provides an ability to visualize the operational environment.[16]

However, the F3EAD targeting process is as complicated as it is, unfortunately, occasionally imperfect and fails to achieve the hearts and minds principle, and it is these failings that are regularly manipulated by the insurgents. An enhanced F3EAD stratagem that engages positively identified legitimate targets, and avoids collateral damage to non-combatants and associated infrastructure, has the potential to eradicate what General Stanley. A. McChrystal referred to as counterinsurgency math.[17]

4.0. Artificial Intelligence.

AI is widely defined as the study of the calculations that formulate the ability to perceive, reason, and act.[18] However, in narrower terms, AI is characterized as non-human intelligence that is considered by its capability to reproduce human mental dexterity, such as pattern recognition, understanding of natural language, adaptive learning from experience, and strategizing or reasoning about others.[19]

Militaries have also considered AI in a functional context, along with others, one study on autonomy by the United States Defense Science Board (DSB), describes AI as the capability of computer systems to perform tasks that typically require human intelligence traits, such as perception, communication, and decision-making.[20] These traits are requisite in COIN targeting or the F3EAD process, which is an active data, focused procedure.

It is the data that requires rapid and accurate processing, and AI can provide these functions. AI systems employ algorithms, which are explained as the arrangement of commands and procedures that machines use to solve problems. They transmute data inputs into outputs and as such are the fundamental theoretical and scientific foundation of modern information technology (IT).

One aspect of algorithmic sequencing that must be measured as essential in COIN is the use of big data. Big data is described as, extensive data sets that may be analyzed computationally to reveal patterns, trends, and associations, primarily relating to human behavior and interactions.[21] Big data has been increasingly used in social and psychological examination to divulge individual divergences and group dynamics.[22]

The latter part of the big data explanation shows that AI employed algorithmic processing has the potential to become an exceptional force multiplier in future COIN warfighting. Before the current era, the decision-making process, inclusive of target selection (find, fix) and prosecution (finish), in warfare was always dependent on human reasoning.[23]

Excluding the fact that human decision-making is enormously persuasive, it also has its limitations regarding speed, attention, and thoroughness. However, there is also a biological threshold to how rapidly human analysts can conclude an evaluation, and there is no eschewing the cognitive load of formulating each momentous decision.[24]

Following a determinate quantity of processing information, all human specialists necessitate respite and sustenance to restore their multifaceted cognitive abilities. Fatigued human brains become lethargic and have the potential to cease being capable of analytical processing, degenerating instead to spontaneous quick thinking. Consequently, this generates the underlying conditions for miscalculation and generating the circumstances that may lead to collateral damage.

Machines enhanced with AI technology do not experience these restrictions. The brain of the AI technology is represented by conveniently duplicated software, which can run on hardware that is economical to produce, and can be positioned in amounts appropriate to fundamentally permit an endless source of tactical, operational, and strategic AI enhanced decision-making.

Moreover, several authorities on AI reason that, deep learning, a subtype of machine-learning that is based on artificial neural networks modeled after the human brain is seen as one of the significant technological revolutions that could be decisive in gaining tactical and, perhaps, strategic advantage on future battlefields.[25]

Hence, it is rational to assert that AI-enhanced systems will potentially make the F3EAD process further expedient, precise, and constructive in mitigating the risk from collateral damage.

5.0. F3EAD Analysis.

Cognizant of the preceding paragraph, and as stated in the introduction, the thesis will examine the six distinct steps of the F3EAD system, including, which phase in the targeting cycle has the potential to cause the most significant level of collateral damage.

This is seen as critical, given that the reduction of collateral damage is central to mitigating insurgent information operations (IO) that may result from inaccurate targeting. The assessment of the F3EAD methodology will assume that the cycle is beginning from a point where there is no information available to develop a legitimate target.

5.1. Find.

The find element of the F3EAD procedure ascertains a start point for intelligence gathering. Generally, the find portion comes in the form of HVT nominations, at which the full range intelligence gathering capabilities are employed to get a starting point for the rest of the process.[26] HVT targeting will most often be conducted in COIN operations where the enemy frequently hides among the civilian population.

Persistent and exact intelligence is often the key to defeating a threat whose primary strength is denying friendly forces access to a target. AI algorithmic processing or, more precisely, the appropriate form of machine learning provides added value to achieve the level of intelligence required.[27] In conjunction with Intelligence, Surveillance and Reconnaissance (ISR) platforms, machine learning can facilitate automation of one of the more time-consuming aspects of COIN, HVT positive identification.

ISR assets are most effective against evasive targets when employed en masse. This may have been achieved with the use of “off the shelf” equipment. However, there have been issues with this strategy recently.[28] The capacity for the insurgent’s to merge with civilians in the operational area (AO) requires tireless collection in order to locate and identify HVT.

Concerning the potential for collateral damage, this phase of the F3EAD cycle, if conducted accurately should limit or even eradicate any underlying effects. This will be due to the precise identification, not only of the HVT but of non-combatant individuals immediately located with them.

The enemy is remarkably well concealed and necessitates multiple sources of intelligence. Nevertheless, intelligence-gathering disciplines functioning together can find HVT that are concealed in the population of the AO.[29] Unfortunately, due to the fluidity of insurgent networks the time required by human analyses to process the data and positively identify HVT often allows the HVT to relocate before exploitation can be initiated.

Frequently this leads to the targeting process, mainly of insurgent leadership HVT, taking an inordinate amount of time.[30] It is anticipated that this is the juncture at which AI will become a force multiplier. The previously cited big data is gathered by the collection assets to be collated and processed by AI algorithmic computation.

Specifically, incorporating computer visualization and machine learning algorithms into COIN intelligence cell systems. These systems would analyze the collected data and automatically identify HVT for targeting.[31] This may be achieved by integrating an existing application programming interface (API) such as Amazon Rekognition or MarkLogic, packages that automatically perform detection and recognition analysis of images and videos to provide results.[32]

In this capacity, AI is intended to computerize and accelerate the work of the human analysts to produce accurate, actionable intelligence. Also, it may permit human analysts to formulate more critical and timely decisions based on the data produced. The find element of the F3EAD cycle should afford potential HVT to be nominated for further development, which moves into the next section of the F3EAD process, fix.

5.2. Fix.

Predominantly, fix is a continuation of the find piece of the targeting process. It develops the continuous information gathering effort that articulates the pattern of life of the HVT. The intelligence staff can formulate wide-ranging behavior models that will focus the specific collection requirements from analysis of the intelligence.[33]

As with the find portion of the process, fix will benefit from the AI enhancements or multipliers already cited. To that end, several intelligence agencies have some AI research projects in progress. The Central Intelligence Agency (CIA) has numerous projects in development that leverage AI in some faculty to undertake tasks such as multimedia recognition or labeling to predict future occurrences approximating terrorist attacks based on wide-ranging analysis of open source intelligence (OSINT).[34]

Intelligence Advanced Research Projects Activity (IARPA) is supporting numerous AI research projects intended to produce substantial apparatuses for the intelligence community.[35] Examples of its programs include developing algorithms to accomplish multilingual speech recognition and translation. Moreover and of note during the fix stage in targeting is a process of geo-location of images with no associated metadata.

Metadata is data that describes other data. Meta is a prefix that in the majority of information technology conventions denotes a fundamental characterization or description. Metadata recapitulates essential facts regarding information, this, in turn, facilitates discovering and working with particular examples of data uncomplicated. [36]

Examples of very basic document metadata might include, author, date created and date modified and file size. Having the capacity to filter through that metadata creates the environment that simplifies the location of a specific document. However, if coordinates of the location of HVT can be achieved without having to input associated metadata, a reasonable conclusion is that this will assist in the fix process being expedited.

Besides the potential geo-location improvements, there are also potential tools to conclude the purpose of a structure based on the pattern of life analysis. These examples and others are all requisites during the fix phase of the F3EAD process. Moreover, the expected amplification of precision in HVT fixing offered by the integration of AI-driven technology is expected to bring with it a decrease in the risk from collateral damage.

Collateral damage continues to be the source of disquiet, particularly for international Non-Governmental Organizations (NGO). The United Nations (UN) observes that the state of the protection of civilians is bleak, and the need for action to address it is urgent. As conflict [COIN] becomes increasingly urbanized, with the potential to affect tens of millions of people, the targeting of or failure to protect civilians cannot go unchallenged.[37]

5.3. Finish.

The addition of AI in the two previous steps of the targeting process is expected to increase the veracity and accuracy of HVT discovery, therefore acting as force multipliers for the finish stage. Importantly, the F3EAD process up to this point should have identified and nominated specific vulnerabilities that, if exploited, will accomplish the commander’s objective.

This intention will be achieved in the application of the finish phase by tasking actions such as capture, destruction, disruption, delay, degradation, neutralization or exploitation of enemy forces or resources critical to the enemy.[38]However, the nature of the finish phase in COIN brings with it definite complexities and generally requires a well trained and rehearsed finish force employing well-developed modes of operation to undertake the required action.[39]

As shown previously AI is anticipated to enhance the searching and detecting of targets. However, the decision to engage that target is still made by the human-machine interface. Occasionally, the weapon system is contained on a single platform, such as a drone. The weapon system consists of the aircraft, multimedia array, pilot, and missile. The multimedia array searches for and acquires the target, the human decides whether to engage, and the missile carries out the engagement.

All of these elements are necessary for the finish engagement to work. In addition to this, a weapon system should consist of all the components necessary to complete the entire combat observe, orient, decide and act (OODA) loop. If there is a human in the loop deciding which target to engage, even though AI may enhance the accuracy, time between target positive identification, and prosecution, it is still a semi-autonomous weapon system.[40]

At present, there is research and development, especially into how AI technology can be incorporated into equipment capable of accomplishing the finish segment of the F3EAD process, without human interaction in the decide part of the OODA loop.[41] Central to many of these projects are the Defense Advanced Research Projects Agency (DARPA).[42]

DARPA and other agencies are looking at the feasibility of fully autonomous operated weapons systems, employing weak and strong AI. In general, weak AI can be summed up as artificial intelligence up to, but short of, human-level intelligence, whereas strong AI is described as AI that is equivalent to human-level intelligence, potentially completing the finish portion of the F3EAD process without human interaction.[43]

However, the potential for exploitation of collateral damage by insurgents due to autonomous weapons systems engaging non-combatant targets is currently perceived as too high, as the AI weapons technology has not been developed to the necessary level of strong AI.[44] Irrespective of the methodology used to achieve the finish segment of the targeting cycle, by a human strike force or an autonomous AI driven engagement, if feasible, once the finish phase has been achieved, the HVT site must be secured and the position exploited.

5.4. Exploit.

Site exploitation is a systematic, comprehensive data gathering process to assemble potential intelligence.[45] Optimum HVT site exploitation necessitates a predetermined methodology and standard operating procedures (SOP) including tactics, techniques, and procedures (TTP) such as search plans, prepared site exploitation kits, and tactical questioning plans.[46] AI Biometric identification processing and AI, multimedia scanning technology, are examples of what AI enhanced technology can be employed here.

F3EAD varies from other targeting methodologies because of its stress on the exploit and analyze steps as the principal effort.[47] As for collateral damage potential during this phase, there is a low risk, as the HVT will have been secured by the counterinsurgent force and therefore will become a controlled environment, providing a semi-secure and safe environment for non-combatants.

Essentially, HVT and document exploitation help build the picture of the enemy as a system of systems, which is accomplished with in-depth analysis and application of lessons learned by the counterinsurgents about the insurgents.

5.5. Analyze.

The outcome of the analyze phase is to examine and evaluate information and swiftly process it into actionable intelligence that can be exploited to defeat the insurgent network. Specific information may be instantaneously actionable, such as information offering the position of another HVT. Additional information might require further analysis and corroboration.

The accumulation of information requires the counterinsurgents to rationalize operations to permit this data to be saved, examined, recalled and disseminated as necessary. New or additional HVT must be included in the collection and assessment process. Technical [AI] assets at all levels on the spectrum of conflict will also be significant, and apparatus to facilitate their incorporation must be expanded.

This will entail adaptation of current planning methodologies and procedures, and learning how to integrate new sources, a study by the DSB concluded that autonomy [AI] would deliver substantial operational value, in multiple dimensions, across an increasingly broad spectrum of missions.[48] Constant training for these type operations allows the progression and improvement of SOP, based on the application of lessons learned.

AI has the potential to speed this process up, by being integrated into the analysis procedure. Together with the counterinsurgents application of lessons learned, it is noticeable that the application of terror as a tactic has evolved and one theory that may be offered for this is the application of lessons learned within terrorist organizations, and indeed between groups. An example of this would be the so-called foreign fighters in various theatres of operation (TOO).[49]

Based on this theory, a reasonable statement is that insurgent groups apply organizational learning. Toft and Reynolds remark that there are three levels of organizational learning, organizational specific, isomorphic learning, and iconic learning.[50] These forms of organizational learning may shape the effectiveness of the counterinsurgents in the COIN campaign.

Counterinsurgent and insurgent elements make use of lessons drawn from practice within the organization to improve the effectiveness of their operations. Toft and Reynolds observe that all of the above levels of organizational learning are important, but offer that isomorphic lessons may be considered the most imperative.[51] Advancing the theory further, it may be assumed that transnational insurgent isomorphism is presently affecting the effectiveness of countering the insurgents.

AI may offer the solution to counterinsurgents in terms of accelerated machine learning systems that can decipher this form of this insurgent isomorphism. In combination with this, Toft and Reynolds continue to state that two types of learning take place in an organization. These being passive and active learning, the former being described as knowing about something, with the latter described as knowing about something and taking action to rectify the deficiencies that have been brought to light.[52]

Organizational learning is described in *Aptitude for Destruction Volume 1: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism*, as the process through which a group acquires new knowledge or technology [AI] that it then uses to make better strategic decisions, improve its ability to develop and apply specific tactics, and increase its chance of success in its operations.[53]All of the points here reiterate the evolution of insurgency previously shown.

Moreover, the study advances by characterizing learning as a four-part process comprising of, acquiring, interpreting, distributing, and storing information and knowledge.[54] Learning on the part of the counterinsurgents is imperative; currently, this is conducted predominately by human operators employing IT equipment, by introducing elements of the previously cited AI, this learning should advance exponentially.

Toft and Reynolds propose that lessons generated through isomorphic learning then leads to hindsight. The availability of hindsight allows foresight to be expanded depending upon the degree and form of organizational effect, foresight or prediction produces opportunities for potential active learning to take place.[55]

Furthermore, foresight or prediction is one of the aspects in the effective combating of extremism; this effectiveness to some extent revolves around being able to predict how groups are developing over time. This prediction will stem from information gleaned as to the modus operandi of any given insurgent group, which in itself is education based on lessons learned, in other words, organizational learning.[56]

This organizational learning only serves to reiterate the assertion that incorporating AI machine learning into identifying these factors will likely become a force multiplier to offer the required prediction in a manner that affords the counterinsurgent the advantage. [57] FM 3-24/MCWP 3-33.5 continues by stating, in COIN, the side that learns faster and adapts more rapidly, the better learning organization, usually wins. [58]

Incentives such as Project Maven, also known as the Algorithmic Warfare Cross-Function

Team are conducting research and development to this end.[59] Counterinsurgents have in place the mechanism for organizational learning. At all levels of the spectrum of conflict, the most common tools that may be employed to initiate isomorphism is the After Action Report (AAR) and mission debriefing reports, which are compiled and data based for retrieval.[60]

It is these databases and methods of retrieval that AI has the potential to expedite, processing the required information during the analyze phase. Given that counterinsurgents utilize publications such as FM 3-24/MCWP 3-33.5 as a guide in the operational execution of the transnational insurgency, it is evident that organizational learning is given a high priority.

Therefore any force multiplier that can enhance the ability of an organization to learn and adapt to an ever-evolving adversary rapidly must be regarded as essential. AI can hypothetically become this enlarger. As previously quoted, the side that learns quicker is the side that will claim eventual victory, to quote T.E Lawrence from Science of Guerrilla Warfare, "Guerrilla War is far more intellectual than a bayonet charge."[61]

The intention is to make intelligence, not information. To do this counterinsurgents have to invest resources and focus on preparation. The level of dedicated resources, mainly human, will have a direct correlation to the quality and quantity of developed intelligence. Too few resources result in the extrication of raw information effort, instead of an analytical and understanding effort, AI will fill any gaps left by the lack of human resources.

Ultimately, AI machine learning would enable machines to navigate and operate in highly complex environments and anticipate and quickly adapt to a variety of changing circumstances. These abilities are critical in situations where mere milliseconds in action-reaction dynamic can make a critical difference and any mistake, for example, in the selection and prosecution of human targets, where errors can have the severest consequences.

In this respect, the rapid analysis of large amounts of data, which far exceeds the abilities of human analysts, is of the most vital importance. Likewise, an integrated AI driven enterprise architecture[62] will allow for the timely (a principle of good intelligence) dissemination of the processed intelligence.[63]

5.6. Disseminate.

The disseminate step is straightforward but time-consuming. The goal is to ensure that all concerned elements are aware of the intelligence available within the COIN environment, and beyond if necessary. Although information may appear to be irrelevant, it may hold the key to revealing a network for flanking units. Fortunately, the various computer programs and IT networks greatly aid the dissemination process.

This can be further assisted by the introduction of the previously mentioned AI driven enterprise architecture, which is described as the fundamental organization of a system, embodied in its components, their relationships to each other and the environment, essentially a dissemination system.[64] Prioritizing the dissemination effort is essential.

Some information will answer priority intelligence requirement (PIR) and should be forwarded to the requesting agency immediately. Where AI enables correct judgments, this accumulation of processing power, disseminating intelligence that could perhaps even make attacks more discriminatory, thereby minimizing collateral damage in targeted killing campaigns.

The machine-learning algorithms that underlie such capabilities are trained through the consumption of large amounts of real-world training data and once deployed, through experience, could process the dissemination of intelligence autonomously. Further information may be essential based on the COIN operational setting, and this would be identified as such within the AI operational environment, flagged as such and disseminated accordingly.

6.0. Conclusion.

Algorithmic or AI warfare has become practical because of three key computing technology advances. First, is the exponential growth in computer processing power that has allowed implementing high-performance machine learning systems. Second is the sudden growth in big data, extensive datasets suitable to train learning capable machines. The third is the steady evolution of cloud technology allowing ready accessing of off-board processing and data.

Given the compressed decision-cycles of advanced AI systems in comparison with a human decision-maker, autonomous gathering and collation of battlefield intelligence, as well as algorithm-based data analysis, maneuver and target selection, could provide crucial tactical and, by extension, strategic advantages.

The thesis has shown that the combination of AI with the processes and associated technology of the F3EAD system will perform as a force multiplier. Inside the component parts of the F3EAD process, this will have the desired effect of increasing the counterinsurgents proficiency at various levels on the spectrum of conflict within a COIN environment.

Additionally, the areas with the potential likelihood of collateral damage occurring within the F3EAD process have been highlighted. Decisively, an algorithm-based analysis of COIN battlefield intelligence as a basis for targeting decisions could also potentially make strikes more accurate, thereby minimizing collateral damage and the ensuing public backlash and insurgent

IO retort, which would be a highly significant development in the context of targeted killings.

Guided by the Joint Capabilities Integration Development System (JCIDS) framework, the integration of future AI systems has the potential to permeate the entirety of military operations, from acquisition philosophies to human-AI team collaborations. Critical issues would include a possible need to develop clear categories of AI systems and applications. These categories must have rules-based and values-based decision processes clearly demarcated.

Machines by nature will abide by literal interpretations of policy, rules, and guidance, a review of their development should be performed to minimize unforeseen consequences. The thesis has established a coherent framework for prospective discussions regarding the integration of AI systems in future COIN operations. Ultimately, future examinations must seek to answer questions as to the suitability of entirely autonomous AI targeting and weapons systems in COIN warfare.

Endnotes

[1] Charles Cleveland, Benjamin Jensen, Arnel David, & Susan Bryant. *Military Strategy for the 21st Century: People, Connectivity, and Competition*. Cambria Press, Amherst, New York, 2018.pp.13-14; Christopher Paul, Colin P. Clarke, Beth Grill & Molly Dunigan. *Paths to Victory: Detailed Insurgency Case Studies*. RAND Corporation, 2013.pp. xi-xxix; David Galula. *Counterinsurgency Warfare: Theory and Practice*. Praeger Security International, 2006. pp.3-10; Murray Williamson. *America and the Future of War*. Stanford, CA: Hoover Institution Press, 2017.pp.24-43; Nick van der Bijl. *British Military Operations in Aden and Radfan*. Pen and Sword Military, 2014. pp.200-202.

[2] Joint Publication. *Joint Publication 3-24, Counter Insurgency*.25 April, 2018. pp.I-1 – I-10.

[3] United States Government. *Counterinsurgency Guide*. January, 2009. https://www.state.gov/documents/organization/119629.pdf

[4] David Galula. pp.11-28; Ian Beckett. *Modern Insurgencies and Counter-Insurgencies: Guerrillas and their Opponents since 1750*. London: Routledge, 2001.pp.1-24; Chaliand, Gérard & Arnaud Blin. *The History of Terrorism from Antiquity to Al Qaeda.* University of California Press, 2007.pp.12-4; Robert Taber. *War of the Flea: the Classic Study of Guerrilla Warfare*. New York: Brassey's Inc, 2002.pp.27-33.

[5] Alexander Spencer. *Lessons Learnt: Terrorism and the Media*. Arts and Humanities Research Council, March 2012. https://ahrc.ukri.org/documents/project-reports-and-reviews/ahrc-public-policy-series/terrorism-and-the-media/; Gabriel Weimann. *New Terrorism and New Media*. Commons Lab of the Woodrow Wilson International Center for Scholars, 2014. https://www.wilsoncenter.org/sites/default/files/STIP_140501_new_terrorism_F_0.pdf; United Nations Educational, Scientific and Cultural Organization. *Terrorism and the Media*. UNESCO 2017. http://unesdoc.unesco.org/images/0024/002470/247074E.pdf; United Nations Office on Drugs and Crime. *The use of the Internet for Terrorist Purposes*. United Nations New York, 2012. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[6] Joint Publication. *Joint Publication 3-24, Counter Insurgency*.25 April, 2018.pp.II 7-25; North Atlantic Treaty Organisation. *AJP-3.4.4, Allied Joint Doctrine for Counterinsurgency (COIN).* February, 2011.pp.1-4 – 1-5. United Kingdom-Ministry of Defence. *British Army Field Manual, Volume 1 Part 10, Countering Insurgency, Army Code 71876*. October 2009.2-1 – 2-8.

[7] Christopher Paul, Colin P. Clarke & Beth Grill. *Victory has a Thousand Fathers: Sources of Success in Counterinsurgency*. RAND Corporation, 2010. pp. xvii – xx.

[8] Christopher Paul. pp. 31-82. David Kilcullen. *Power Point Brief: Counterinsurgency in Iraq: Theory and Practice*. 2007. https://usacac.army.mil/cac2/AIWFC/COIN/repository/Dr_Kilcullen_COIN_Brief(Sep07).ppt; Joint Publication. *Joint Publication 3-24, Counter Insurgency*.25 April, 2018.pp. III – 7-16;

North Atlantic Treaty Organisation. *AJP-3.4.4, Allied Joint Doctrine for Counterinsurgency (COIN).* February, 2011.pp. 3-20 – 3-27. Steven Metz & Raymond Millen. *Insurgency and Counterinsurgency in the 21st Century: Reconceptualizing Threat and Response*. Strategic Studies Institute, November 2004.pp.14-25. United Kingdom-Ministry of Defence. *British Army Field Manual, Volume 1 Part 10, Countering Insurgency, Army Code 71876*. October 2009.pp. 3-1 – 3-2.

[9] Christopher Paul.pp.32. David Galula. pp.52-54.

[10] Ibid. pp.75-81. Ibid.

[11] Bryan C. Price. *Targeting Top Terrorists: How Leadership Decapitation Contributes to Counterterrorism*. International Security, Vol. 36, No. 4. Spring 2012.pp. 9–46. https://www.belfercenter.org/sites/default/files/files/publication/Price.pdf

[12] Department of the Army, Headquarters. Army Field Manual Interim. FMI 3-24.2. *Tactics in Counterinsurgency*. March 2009. pp.3-7 – 3-8.

[13] Joint Publication. *Joint Publication 3-24, Counter Insurgency*.25 April, 2018.pp. VII – 42; North Atlantic Treaty Organisation. *AJP-3.4.4, Allied Joint Doctrine for Counterinsurgency (COIN).* February, 2011.pp. 3-22 – 3-23; United Kingdom-Ministry of Defence. *British Army Field Manual, Volume 1 Part 10, Countering Insurgency, Army Code 71876*. October 2009.pp. 5-1.

[14] Joint Publication. *Joint Publication 3-24, Counter Insurgency*.25 April, 2018.pp. IV-4 – IV-7. United Kingdom-Ministry of Defence. *British Army Field Manual, Volume 1 Part 10, Countering Insurgency, Army Code 71876*. October 2009.pp. 3-5 – 3-7.

[15] Department of the Army, Headquarters. *Army Techniques Publication, Targeting, ATP 3-60 (FM 3-60).* 7 May, 2015.pp.B-1; Joint Publication 3-25. *Countering Threat Networks*. 21 December 2016.pp. V-12 – V-13; Joint Publication 3-60. *Joint Targeting*.31 January 2013.pp.II-3 – II-6; North Atlantic Treaty Organisation. *AJP-3.9, Allied Joint Doctrine for Joint Targeting, Edition A, Version 1***.** April 2016.pp.5-7. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/628215/20160505-nato_targeting_ajp_3_9.pdf

[16] Joint Publication 3-25.pp.V-12.

[17] Alexander Spencer; Gabriel Weimann; Human Rights Watch. *A Wedding That Became a Funeral: US Drone Attack on Marriage Procession in Yemen*.14-19. 2014. http://www.hrw.org; Paul Woodward. The National, United Arab Emirates, *General McChrystal's Afghan war*. September 29, 2009. https://www.thenational.ae/uae/general-mcchrystal-s-afghan-war-1.510904

[18] Stuart J Russell and Peter Norvig, ed. *Artificial Intelligence: A Modern Approach, Third Edition*. Prentice Hall, 2010. pp.1-3.

[19] Jeff Hawkins and Sandra Blakeslee. *On Intelligence: How a New Understanding of the Brain Will Lead to the Creation of Truly Intelligent Machines*. Owl Books, 2004.pp.9-18.
Stuart J Russell and Peter Norvig. pp.3-16.

[20] Andrew Ilachinski. *Artificial Intelligence & Autonomy: Opportunities and Challenges*. CAN Analysis and Solutions, October, 2017.pp.1-10; Cheryl Pellerin."Project Maven to Deploy Computer Algorithms to War Zone by Year's End," *Department of Defense*, 21 July 2017, https://www.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/; Daniel S Hoadley and Nathan J. Lucas. *Artificial Intelligence and National Security*. Congressional Research Service, April 26, 2018.pp.1-12. https://www.hsdl.org/?abstract&did=810166. Louise Amoore. *Algorithmic War: Everyday Geographies of the War on Terror*. Durham University, 03 May 2011. pp. 1-4. United States Deputy Secretary of Defense. Memorandum, *Establishment of the Joint Artificial Intelligence Center*. 27 June 2018.

[21] John Paul Mueller & Luca Massaron. *Artificial Intelligence for Dummies*. John Wiley & Sons, Inc., Hoboken, New Jersey, 2018.pp.5-55. Oxford English Dictionary. https://en.oxforddictionaries.com/definition/big_data

[22] Lin Qiu, Sarah Hian May Chan & David Chan. *Big Data In Social And Psychological Science: Theoretical And Methodological Issues*. Journal of Computational Social Science, 2017. pp.1:59-66.

[23] Charles Cleveland. pp. 217-225.

[24] Janice. H Laurence & Michael D. Matthews, ed. *The Oxford Handbook of Military Psychology*. Oxford University Press, Inc, 2012.pp.197-214; Science Direct. *Cognitive Load*. Psychology of Learning and Motivation, 2017. https://www.sciencedirect.com/topics/neuroscience/cognitive-load

[25] Greg Allen & Taniel Chan. *Artificial Intelligence and National Security*. Belfer Center Study, July 2017.pp.12-26. https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf; Michael Carl Haas and Sophie-Charlotte Fischer. *The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order*. Contemporary Security Policy, 38:2, 2017.pp.287. http://dx.doi.org/10.1080/13523260.2017.1336407

[26] Headquarters, Department of the Army. Army Techniques Publication, *Targeting, ATP 3-60 (FM 3-60)*. 7 May 2015. pp.B-3.

[27] Microsoft Azure. *Machine learning algorithm cheat sheet for Azure Machine Learning Studio*. 2018. https://docs.microsoft.com/en-us/azure/machine-learning/studio/algorithm-cheat-sheet; Stuart J Russell and Peter Norvig, ed. pp.693-758.

[28] Gary Mortimer. *US Army calls for units to discontinue use of DJI equipment*. 04 August 2017. https://www.suasnews.com/2017/08/us-army-calls-units-discontinue-use-dji-equipment/

[29] United Kingdom-Ministry of Defence. *British Army Field Manual, Volume 1 Part 10, Countering Insurgency, Army Code 71876*. October 2009.pp. 5-7 – 5-9.

[30] Peter Bergen. *Manhunt: The Ten Year Search for Bin Laden From 9/11 to Abbottabad*. Crown Publishing Group, May 2012.

[31] Abeer A. Mohamad AL-Shiha. *Biometric Face Recognition Using Multilinear Projection and Artificial Intelligence*. University of Newcastle, July 2013. pp.12-15, pp.159-162. https://pdfs.semanticscholar.org/2414/16b1249d2b71b373f8dcf054110d579a2148.pdf; AWS. *Amazon Rekognition Developer Guide.* 2018. https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf*;*

[32] AWS. *Easily add intelligent image and video analysis to your applications.*2018 https://aws.amazon.com/rekognition/; AWS. Amazon Rekognition Developer Guide. 2018. https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf; MarkLogic. *Enduring Intelligence Automation*. 2018. https://cdn1.marklogic.com/wp-content/uploads/resources/Enduring-Intelligence-Automation.pdf

[33] Headquarters, Department of the Army. Army Techniques Publication, *Targeting, ATP 3-60 (FM 3-60)*. 7 May 2015. pp.B-4.

[34] Daniel S Hoadley & Nathan J. Lucas. pp.9.

[35] IARPA. *Research Programs*. 10 December 2018. https://www.iarpa.gov/index.php/research-programs; Stephan De Spiegeleire, Matthijs Maas, Tim Sweijs. *Artificial Intelligence And The Future Of Defense: Strategic Implications For Small- And Medium-Sized Force Providers*. The Hague Centre for Strategic Studies, 2017.pp.87-98.

[36] Jenn Riley. *Understanding Metadata: What Is Metadata, And What Is It For?*. National Information Standards Organization (NISO), 2017.pp.6-9. www.niso.org; Margaret Rouse. WhatIs.com, *Definition: Metadata*. 13 December 2018. https://whatis.techtarget.com/definition/metadata; National Information Standards Organization. *Understanding Metadata*. NISO Press, 2004. pp.1. www.niso.org; Unknown. *Chapter 5. Geolocation.* 10 December 2018. https://docs.kde.org/trunk5/en/extragear-graphics/digikam/tool-geolocation.html

[37] Nigel Fisher. *93% of deaths and injuries in Yemen are civilian - this must change*. The Guardian, U.K, 27 October 2015. https://www.theguardian.com/global-development-professionals-network/2015/oct/27/yemen-deaths-93-civilian-this-must-change; United Nations Security Council. *Protection of civilians in armed conflict*. 14 May 2018.pp.2. https://reliefweb.int/sites/reliefweb.int/files/resources/N1812444.pdf

[38] Headquarters, Department of the Army. *ADRP 3-05: Special Operations*. 29 January 2018.pp.4-1.

[39] David Kilcullen. pp.13.

[40] Paul Scharre. *Army of None: Autonomous Weapons and the Future of War*. W. W. Norton & Company, New York, 2018.pp.34-50.

[41] Ibid. pp.52-65.

[42] Ibid. pp.66-73.

[43] Louis A Del Monte. *Genius Weapons: Artificial Intelligence, Autonomous Weaponry, and the Future of Warfare*. Prometheus Books, November 6, 2018.pp.98-112.

[44] Paul Scharre.pp. 148-152.

[45] Headquarters, Department of the Army. Army Techniques Publication, *Targeting, ATP 3-60 (FM 3-60)*. 7 May 2015.B-5.

[46] Center for Army Lessons Learned (CALL). *Tactical Site Exploitation Handbook*. May, 2007. http://call.army.mil; Headquarters, Department of the Army. Army Techniques Publication, *Site Exploitation*, ATP 3-90.15. July, 2015.

[47] Joint Publication 3-25.pp.V-3.

[48] Defense Science Board. Summer Study on Autonomy. June 2016.pp. 98-101.

[49] B.A.Jackson. *Counterinsurgency Intelligence in a "Long War": The British Experience in Northern Ireland*, Military Review. January-February 2007.pp.74-85; Klaus Jurgen Gantzel and Torsten Schwinghammer. *Warfare since the Second World War*. Transaction Publishing, 2000.pp.51-89; SENLIS. *Stumbling into Chaos: Afghanistan on the Brink*. SENLIS Afghanistan, November 2007.pp.38, 53. http://www.senliscouncil.net/modules/publications.

[50] B. Toft & S. Reynolds. Learning from Disasters: A Management Approach, third edition. Chippenham and Eastbourne, Palgrave Macmillan, 2005.pp. 42-64

[51] Ibid. pp. 42-64.

[52] Ibid. pp. 65-66.

[53] B.A. Jackson, J.C. Baker, K. Cragin, J. Parachini, H.R. Trujillo & P. Chalk. *Aptitude for Destruction, Volume 1: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism*.pp. 9. RAND Corporation, 2005. http://www.rand.org.

[54] Ibid.pp.10-16.

[55] B. Toft and S. Reynolds. pp. 69.

[56] B.A. Jackson et al.pp.10-16

[57] United States Department of Defense. *FM 3-24/MCWP 3-33.5 Insurgencies and Countering Insurgencies*. 13 May, 2014.pp.v.

[58] Ibid.pp.1-21.

[59] Deputy Secretary of Defense. *Memorandum: Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven).* 26 April, 2017.

[60] Headquarters, Department of the Army. Army Field Manual. FM 3-05.32.*Special Forces Group Intelligence Operations*. November 2004.pp.G-6; Headquarters, Department of the Army. TC 2-50.5, *Intelligence Officers Handbook*. 06 January 2010.pp. C – 2-4; United Kingdom, Ministry of Defence. *An Analysis of Military Operations in Northern Ireland*. 2006.pp.8-14.

[61] .J.D.Celeski. *Operationalizing COIN*, Joint Special Operations University Report, 05-2, 2005. http://jsoupublic.socom.mil/publications/jsou/JSOU05-2RceleskiOperationalizingCOIN_final.pdf.

[62] Charles Moller, ed. *Advances in Enterprise Information Systems*. CRC Press, 2014. pp.11-27. http://researchspace.csir.co.za/dspace/bitstream/handle/10204/6573/Kotze3_2012.pdf;jsessionid=EDA220C8CD93C64E76AF4661E206679D?sequence=1

[63] Joint Publication 2-01. *Joint and National Intelligence Support to Military Operations*. 05 July 2017.pp. III – 65-68.

[64] Charles Moller, ed. pp.16-23.

Bibliography

Allen, Greg and Taniel Chan. *Artificial Intelligence and National Security*. Belfer Center Study, July, 2017.

AL-Shiha, Abeer A. Mohamad. *Biometric Face Recognition Using Multilinear Projection and Artificial Intelligence*. University of Newcastle, July 2013. https://pdfs.semanticscholar.org/2414/16b1249d2b71b373f8dcf054110d579a2148.pdf

Amoore, Louise. *Algorithmic War: Everyday Geographies of the War on Terror*. Durham University, 03 May 2011.

AWS. *Amazon Rekognition Developer Guide*. 2018. https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf

AWS. *Easily add intelligent image and video analysis to your applications.* https://aws.amazon.com/rekognition/

Beckett, Ian. *Modern Insurgencies and Counter-Insurgencies: Guerrillas and their Opponents since 1750*. London: Routledge, 2001.

Bergen, Peter. *Manhunt: The Ten Year Search for Bin Laden From 9/11 to Abbottabad*. Crown Publishing Group, May 2012.

Celeski.J.D. *Operationalizing COIN*, Joint Special Operations University Report, 05-2, 2005. http://jsoupublic.socom.mil/publications/jsou/JSOU05-2RceleskiOperationalizingCOIN_final.pdf

Center for Army Lessons Learned(CALL). *Tactical Site Exploitation Handbook*. May,2007. http://call.army.mil

Chaliand, Gérard and Arnaud Blin. *The History of Terrorism from Antiquity to Al Qaeda.* University of California Press, 2007.

Cleveland Charles, Benjamin Jensen, Arnel David, and Susan Bryant. *Military Strategy for the 21st Century: People, Connectivity, and Competition*. Cambria Press, 2018.

Defense Science Board. *Summer Study on Autonomy*. June, 2016. https://www.hsdl.org/?abstract&did=794641

Del Monte, Louis A. *Genius Weapons: Artificial Intelligence, Autonomous Weaponry, and the Future of Warfare*. Prometheus Books, November 6, 2018.

Deputy Secretary of Defense. *Memorandum: Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven).* 26 April, 2017.

De Spiegeleire Stephan, Matthijs Maas, Tim Sweijs. *Artificial Intelligence And The Future Of Defense: Strategic Implications For Small- And Medium-Sized Force Providers*. The Hague Centre for Strategic Studies, 2017.

Galula, David. *Counterinsurgency Warfare: Theory and Practice*. Praeger Security International, 2006.

Gantzel, Klaus Jurgen and Torsten Schwinghammer. *Warfare since the Second World War*. Transaction Publishing, 2000.

Fisher, Nigel. *93% of deaths and injuries in Yemen are civilian - this must change*. The Guardian, U.K, 27 October 2015. https://www.theguardian.com/global-development-professionals-network/2015/oct/27/yemen-deaths-93-civilian-this-must-change

Haas, Michael Carl and Sophie-Charlotte Fischer. *The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order.* Contemporary Security Policy, 38:2, 2017.281-306. http://dx.doi.org/10.1080/13523260.2017.1336407

Hawkins, Jeff and Sandra Blakeslee. *On Intelligence: How a New Understanding of the Brain Will Lead to the Creation of Truly Intelligent Machines*. Owl Books, 2004.

Headquarters, Department of the Army. *ADRP 3-05: Special Operations*. 29 January 2018.

Headquarters, Department of the Army. Army Field Manual. FM 3-05.32.*Special Forces Group Intelligence Operations*. November 2004.

Headquarters, Department of the Army. Army Field Manual Interim. FMI 3-24.2. *Tactics in Counterinsurgency*. March 2009.

Headquarters, Department of the Army. Army Techniques Publication, *Site Exploitation*, ATP 3-90.15. July, 2015.

Headquarters, Department of the Army. Army Techniques Publication, *Targeting*, ATP 3-60 (FM 3-60). 7 May, 2015.

Headquarters, Department of the Army. TC 2-50.5, *Intelligence Officers Handbook*. 06 January 2010.

Hoadley, Daniel S. and Nathan J. Lucas. *Artificial Intelligence and National Security*. Congressional Research Service, April 26, 2018.

Human Rights Watch. *A Wedding That Became a Funeral: US Drone Attack on Marriage Procession in Yemen*. 2014. http://www.hrw.org.

IARPA. Research Programs. 10 December 2018. https://www.iarpa.gov/index.php/research-programs

Ilachinski, Andrew. *Artificial Intelligence & Autonomy: Opportunities and Challenges*. CAN Analysis and Solutions, October, 2017.

Jackson B.A. *Counterinsurgency Intelligence in a "Long War": The British Experience in Northern Ireland*, Military Review. January-February 2007.

Jackson.B.A, Baker.J.C , Cragin.K , Parachini. J, Trujillo. H. R, Chalk P. *Aptitude for Destruction, Volume 1: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism*. RAND Corporation, 2005. http://www.rand.org.

Joint Publication 2-01. *Joint and National Intelligence Support to Military Operations.* 05 July 2017.

Joint Publication 3-24. *Counter Insurgency*.25 April 2018.

Joint Publication 3-25. *Countering Threat Networks*. 21 December 2016.

David Kilcullen. *Power Point Brief: Counterinsurgency in Iraq: Theory and Practice*. 2007. https://usacac.army.mil/cac2/AIWFC/COIN/repository/Dr_Kilcullen_COIN_Brief(Sep07).ppt

Laurence, Janice. H and Michael D. Matthews, ed. *The Oxford Handbook of Military Psychology*. Oxford University Press, Inc, 2012.

MarkLogic. *Enduring Intelligence Automation*. 2018. https://cdn1.marklogic.com/wp-content/uploads/resources/Enduring-Intelligence-Automation.pdf

Metz, Steven & Raymond Millen. *Insurgency and Counterinsurgency in the 21st Century: Reconceptualizing Threat and Response*. Strategic Studies Institute, November 2004

Microsoft Azure. *Machine learning algorithm cheat sheet for Azure Machine Learning Studio*. 2018. https://docs.microsoft.com/en-us/azure/machine-learning/studio/algorithm-cheat-sheet

Moller, Charles, ed. *Advances in Enterprise Information Systems*. CRC Press, 2014. pp. http://researchspace.csir.co.za/dspace/bitstream/handle/10204/6573/Kotze3_2012.pdf;jsessionid=EDA220C8CD93C64E76AF4661E206679D?sequence=1

Mortimer, Gary. US Army calls for units to discontinue use of DJI equipment. 04 August 2017. https://www.suasnews.com/2017/08/us-army-calls-units-discontinue-use-dji-equipment/

Mueller, John Paul and Luca Massaron. *Artificial Intelligence for Dummies*. John Wiley & Sons, Inc., Hoboken, New Jersey, 2018.

North Atlantic Treaty Organisation. *AJP-3.4.4, Allied Joint Doctrine for Counterinsurgency (COIN).* February, 2011. https://info.publicintelligence.net/NATO-Counterinsurgency.pdf

North Atlantic Treaty Organisation. *AJP-3.9, Allied Joint Doctrine for Joint Targeting, Edition A, Version 1***.** April 2016.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/628215/20160505-nato_targeting_ajp_3_9.pdf

Oxford English Dictionary. https://en.oxforddictionaries.com/definition/big_data

Paul, Christopher, Colin P. Clarke & Beth Grill. *Victory has a Thousand Fathers: Sources of Success in Counterinsurgency*. RAND Corporation, 2010.

Paul, Christopher, Colin P. Clarke, Beth Grill and Molly Dunigan. *Paths to Victory: Detailed Insurgency Case Studies*. RAND Corporation, 2013.

Pellerin, Cheryl. "Project Maven to Deploy Computer Algorithms to War Zone by Year's End." *Department of Defense*, 21 July 2017. https://www.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/

Price, Bryan C. *Targeting Top Terrorists: How Leadership Decapitation Contributes to Counterterrorism*. International Security, Vol. 36, No. 4. Spring 2012. https://www.belfercenter.org/sites/default/files/files/publication/Price.pdf

Qiu, Lin, Sarah Hian May Chan and David Chan. *Big Data In Social And Psychological Science: Theoretical And Methodological Issues*. Journal of Computational Social Science, 2017.

Riley, Jenn. *Understanding Metadata: What Is Metadata, And What Is It For?*. National Information Standards Organization (NISO), 2017. www.niso.org

Rouse, Margaret. WhatIs.com, *Definition: Metadata*. 13 December 2018. https://whatis.techtarget.com/definition/metadata; National Information Standards Organization. *Understanding Metadata*. NISO Press, 2004. www.niso.org

Russell, Stuart J. and Peter Norvig, ed. *Artificial Intelligence: A Modern Approach, Third Edition*. Prentice Hall, 2010.

Scharre, Paul. *Army of None: Autonomous Weapons and the Future of War*. W. W. Norton & Company, New York, 2018.

Science Direct. *Cognitive Load*. Psychology of Learning and Motivation, 2017. https://www.sciencedirect.com/topics/neuroscience/cognitive-load

SENLIS. *Stumbling into Chaos: Afghanistan on the Brink*. SENLIS Afghanistan, November 2007.pp. http://www.senliscouncil.net/modules/publications.

Spencer, Alexander. *Lessons Learnt: Terrorism and the Media*. Arts and Humanities Research Council, March 2012. https://ahrc.ukri.org/documents/project-reports-and-reviews/ahrc-public-policy-series/terrorism-and-the-media/

Taber, Robert. *War of the Flea: the Classic Study of Guerrilla Warfare*. New York: Brassey's Inc, 2002.

The National, United Arab Emirates, *General McChrystal's Afghan war*. September 29, 2009. https://www.thenational.ae/uae/general-mcchrystal-s-afghan-war-1.510904;

Toft.B, Reynolds.S, (2005). *Learning from Disasters: A Management Approach, third edition,* Chippenham and Eastbourne, Palgrave Macmillan.

Townsend, Charles, ed. *The Oxford History of Modern War*. Oxford University Press, 2000.

United Kingdom, Ministry of Defence. *An Analysis of Military Operations in Northern Ireland*. 2006.

United Kingdom, Ministry of Defence. *British Army Field Manual, Volume 1 Part 10, Countering Insurgency, Army Code 71876*. October 2009.

United Nations Educational, Scientific and Cultural Organization. *Terrorism and the Media*. UNESCO 2017. http://unesdoc.unesco.org/images/0024/002470/247074E.pdf

United Nations Office on Drugs and Crime. *The use of the Internet for Terrorist Purposes*. United Nations New York, 2012. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

United Nations Security Council. Protection of civilians in armed conflict. 14 May 2018. https://reliefweb.int/sites/reliefweb.int/files/resources/N1812444.pdf

United States Government. *Counterinsurgency Guide*. January, 2009. https://www.state.gov/documents/organization/119629.pdf

United States Department of Defense. *FM 3-24/MCWP 3-33.5 Insurgencies and Countering Insurgencies*. 13 May,2014.

United States Deputy Secretary of Defense. Memorandum, *Establishment of the Joint Artificial Intelligence Center*. 27 June 2018.

Unknown. *Chapter 5. Geolocation.* 10 December 2018. https://docs.kde.org/trunk5/en/extragear-graphics/digikam/tool-geolocation.html

van der Bijl, Nick. *British Military Operations in Aden and Radfan*. Pen and Sword Military, 2014.

Weimann, Gabriel. *New Terrorism and New Media*. Commons Lab of the Woodrow Wilson International Center for Scholars, 2014. https://www.wilsoncenter.org/sites/default/files/STIP_140501_new_terrorism_F_0.pdf

Williamson Murray. *America and the Future of War*. Stanford, CA: Hoover Institution Press, 2017.